Vehicular Security Through Reputation and Plausibility Checks

Sanjay K. Dhurandher, Mohammad S. Obaidat, *Fellow, IEEE,* Amrit Jaiswal, Akanksha Tiwari, and Ankur Tyagi

***Abstract*—Vehicular ad hoc networks (VANETs) are essentially used to communicate real-time traffic and safety information. In this paper, we present vehicular security through reputation and plausibility checks to address the most important issue of security in VANETs. The algorithm provides security against the attacks of event modification, false event generation, data aggregation and data dropping. It performs not only detection but also the isolation of malicious nodes in the network. It employs sensors in a reputation-based system and presents a very robust yet cost efficient approach as it utilizes just vehicle to vehicle communication, thereby reducing the security issues and cost associated with the roadside infrastructure. The algorithm has been simulated and tested on various scenarios and has been observed to be very effective and efficient in terms of the percentage of malicious nodes detected, number of control packets sent after detection of malicious nodes, average time taken to detect nodes which are generating false information, number of packets dropped, and the number of packets received by malicious nodes.**

***Index Terms*—Geocasting systems, malicious attacks, plausibility checks, security through reputation, vehicular ad hoc networks (VANETs).**

I. Introduction

WITH THE INCREASE in the number of vehicles in the world, the transportation system has become inefficient. Increasing accidents and traffic jams are leading to loss of millions of lives, money, and time, year after year. This is one of the major problems being faced by the society today. Vehicular ad hoc networks (VANETs) [1] can be used to alleviate the problems of vehicle safety as well as the traffic control and optimization. VANET as proposed consists of mobile hosts equipped with wireless communication devices and road side units (RSUs) and in it both vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure (V2I) Communication is possible. Dedicated RSUs, because of their required investment in purchase, installation, and maintenance at least for developing economies, have not been seen as an appropriate possible solution and thus work is still in progress that looks into implementing only V2V without infrastructure to reduce the implementation cost. A robust V2V communication system can help us create a network where one vehicle can inform other vehicles about various existing conditions like traffic jams, accidents, and implementation of brakes.

The security in VANETs is of primary concern since an attacker may try to insert or modify life-critical information. The major attacks [1] in VANETs are message forging, impersonation, packet dropping, black hole, gray hole, worm hole, on-board tampering, and in-transit traffic tampering. Infrastructure-based VANET uses majorly infrastructure for handling Security [1] by providing private keys to vehicles at real time. These keys can work well but need full infrastructure support. Storing keys in the vehicles can also not be a solution as it is totally open to attackers of the network. In this paper we propose secured VANET data transfer protocol, which allows vehicles in VANET to communicate important information related to traffic jams, accidents, and brake implementation to other nodes, with feature to detect as well as isolate the different malicious nodes which may be present in the network.

A. VANETs Challenges and Unique Characteristics

VANETs have certain differences with mobile ad hoc networks (MANETS). Consequently, most of the work done on MANETS cannot be directly applied to vehicular networks. Some of the challenges [4], [19], [20] are network dynamics, resource constraints, high application requirements on data delivery, no confidentiality for safety information, infrastructure access, central registration and periodic technical inspection, liability identification, and security issues.

VANETs have tremendous potential and scalability and therefore a successful attack by an adversary might have disastrous effects leading to huge loss of life. Thus, security in VANETs is of primary concern since an attacker may try to insert or modify life-critical information. The major attacks [4] in VANETs are message forging, impersonation, packet dropping, gray hole, worm hole, on-board tampering, and in-transit traffic tampering.

VANETS are designed to cater to a number of applications pertaining to passenger safety, ease, and comfort. However, the most important application envisioned for VANETS is to

Manuscript received April 21, 2011; revised November 30, 2011, August 14, 2012; accepted January 14, 2013. Date of publication March 7, 2013; date of current version May 22, 2014.

S. K. Dhurandher, A. Jaiswal, and A. Tiwari are with the Center for Application of IT in Financial Systems, Division of Information Technology, Netaji Subhas Institute of Technology, University of Delhi, New Delhi 110078, India (e-mail: dhurandher@rediffmail.com; jaiswal_amrit@yahoo.com; akankshaa89@gmail.com).

M. S. Obaidat is with the Department of Computer Science and Software Engineering, Monmouth University, West Long Branch, NJ 07764-1898 USA, and also with the Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi 127788, United Arab Emirates (e-mail: msobaidat@gmail).

A. Tyagi is with Eigen Technologies Pvt. Ltd., New Delhi 110058, India (e-mail: ankur@eigen.in).

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

Digital Object Identifier 10.1109/JSYST.2013.2245971

provide safe and secure driving conditions to the passengers [5]. Some other applications for VANETs are safety-related applications, traffic optimization, infotainment, electronic toll collection, and roadside service finder.

However, the main challenge in VANETs remains security. The possible misuse of VANETs can create a lot of problems and difficulties especially in situations where life critical information is involved. In this paper we propose a novel way of incorporating security in VANETs through a trust-based algorithm based on reputation using sensors.

II. Related Work

Establishing security in VANETS is dependent on a number of parameters that include minimum delay, trust, cost, and gradual deployment. A lot of effort has been put into research in this area that focuses on secure protocols for routing as well as one-hop communication. A number of methods have been proposed [2]–[6] to achieve security in VANETs such as cryptographic schemes [2], reputation-based systems [3], and plausibility and sensor-driven techniques [4].

As security being a major concern in VANETs, researchers have proposed a number of secure protocols [2]–[4], [7], [11]–[13] that are based on either one of the above mentioned schemes or a combination of them. There have also been some new methods as proposed in [18] and [21]. Samara *et al.* [18] propose a framework that provides security based on hardware that uses symmetric as well as asymmetric cryptography for message exchange. Here, the trust between the nodes is obtained using a trusted platform module and group communication. However, a security model through the use of position detectors such as eye-devices and ear-devices has been proposed by Gongjun *et al*. [21]. In this the data of neighboring vehicles captured with the help of these devices are matched and the final decision in order to achieve security is taken based on it. Furthermore, the authors in this work [21] have assumed that majority of the vehicles are not misbehaving. The sections to follow discuss some of these protocols in detail.

A. Secure Vehicular Communications Systems: Design and Architecture

The authors in [10] have proposed a secure architecture. The architecture consists of the certification authority (CA) where each authority is responsible for a region. Each authority provides certificates to nodes registered with it as well as foreigner certificates to nodes registered with other CAs when these nodes enter its geographical boundary.

The RSUs as well as the vehicles are equipped with an hardware security module that is used to physically store and protect the private keys for signature generation. It is used as a tamper resistant solution to prevent against physical on-board tampering.

Each node utilizes a number of short term public–private key pairs (called pseudonyms that do not reveal the identity of the node) instead of using just one long term public–private key pair. Each node uses a pseudonym for a short period of time and then switches over to another. This provides the required privacy. The list of the mapping between the short term and long term key pairs is maintained by the node's CA.

Certificate revocation is performed by the CA to handle malicious nodes. This is done by issuing certificate revocation lists that are distributed to vehicles with the help of RSUs. Two localized schemes—misbehavior detection system and local eviction of attackers by voting evaluators—have been incorporated to detect and eliminate faulty nodes locally. Secure communication in the architecture involves:

a) S*ecure beaconing:* Before being broadcast, the beacon messages are signed using a private key corresponding to a particular pseudonym. A geostamp is also attached that includes the geographic coordinates along with the time instant of transmission. A certificate is also attached to verify the signature.

b) S*ecure neighbor discovery:* Each node maintains a neighbor table that includes its communication neighbors. A node estimates the sender–receiver distance using its own coordinates, the location in the received message and the time of flight.

c) S*ecure geocasting:* The authors have proposed a position verification approach, based on plausibility heuristics, which is capable of detecting position falsifications [8]. Also pseudonyms changing leads to instability in nodes' neighbor tables which can lead to transmission faults in the next hop. To handle this, callback media access control (MAC) layer mechanism is used where the MAC layer notifies the routing layer about missed neighbors.

B. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications

This protocol [9] caters to the two issues, efficient authentication of anonymous safety messages and efficient tracking on the source of a disputed safety message, but makes use of infrastructure. It focuses on location privacy [14]–[16].The network architecture consists of the top trusted authority (TA), the immobile RSUs at the road side, and the mobile on-board units (OBUs) equipped on the running vehicles. *TA:* TA is responsible for registration of immobile RSUs at the road side and mobile OBUs equipped on the vehicles, and for the identification of OBU corresponding to a safety message. The RSUs have storage units for storing information coming from the TA and the OBUs. The OBUs are integrated with the running vehicles and share local traffic information among themselves and with RSUs to request for keys. The protocol is divided into four parts: system initialization, OBU short-time anonymous key generation, OBU safety message generation and sending, and OBU fast tracking algorithm, with each having a separate algorithm [9]. Anonymous keys are generated dynamically between the RSUs and the OBUs enabling quick tracking and authentication accomplished by the request-response protocol between the OBU and the RSU thus reducing the storage space required. Level-3 privacy security is provided to the OBUs as no OBUs can reveal the real identity or launch moving track attack. The safety message is level 1 secure to the TA as it can reveal the real OBU identity. With all its merits, the question remains that of the infrastructure which involves implementation cost.

C. Secure Position-Based Routing (PBR) for VANETs

This protocol [2] relies on asymmetric cryptography and digital signatures. When one hop communication is taken into account, only the source is required to sign the packet. However, when dealing with multihop communication, there are two schemes proposed—source signature and sender signature. Source signature is signed by the source on the immutable fields whereas the sender signature is signed over the immutable fields by each node that is involved in multihop communication.

Before a node accepts a packet, it performs a series of plausibility checks to ensure the correctness of information. In order to verify that the message is neither too old nor meant for the future, a timestamp field is used. This timestamp is then checked to ensure that it lies in a time window. Further checks are performed by assuming a maximum transmission range of the nodes in the network. A neighboring node cannot lie beyond this maximum range. Checks have also been proposed based on the velocity of the nodes. These checks are performed by calculating the time difference between any two successive position updates and multiplying it with the maximum velocity of the nodes. The maximum velocity of the nodes is assumed and any position update should lie within a space window to be valid.

The protocol proposes rate-limiting mechanisms to take into account false broadcast floods that could be injected by a malicious node and that could lead to lot of overheads and resource wastage in the network. This is achieved by setting a limit on the rate of data that can originate from a node and by providing private vehicles a much lower rate of data transmission as well as a smaller transmission area as compared to RSUs and emergency vehicles.

D. VARS: A Vehicle Ad Hoc Network Reputation System

VARS [3] is a reputation-based system which uses modules for direct and indirect reputation handling, opinion generation and confidence decision (message handling) and situation recognition. VARS defines three areas: the event area within which an event can be recognized, the decision area where the trustworthiness of event messages have to be decided upon and the distribution area which specifies how far those messages are distributed.

1) *Direct and Indirect Reputation Handling:* The term direct trust is used for reputation information that is derived from experience that an announced event can be verified if recognized by a node. indirect trust is transitive second-hand reputation provided by nodes of which reputation information is already known. Depending on the kind of reputation information a source is attributed with a sender-based reputation level. The thresholds for the confidence decision are adjusted in relation to the relative position of the sender compared to the position of the deciding node.

2) *Message Handling:* It consists of two parts.

a) O*pinion generation::* 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, 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. This process is called opinion generation. Before the message is transmitted, every forwarding node appends its own opinion about the trust of the message to the message through a mechanism called opinion piggybacking [3].

b) C*onfidence decision::* A node within a decision area has to evaluate all messages related to the distinct event. If the event is thought to be prevalent, the trust-opinion generator announces this event to the applications. It is at the discretion of the application to inform the user or take actions. Messages might be kept for repeated decision on reception of further messages.

3) *Situation Recognition:* The situations are categorized with respect to the availability and quality of reputation information as well as familiarity of the area, i.e., rural/unknown or metropolitan/well-known areas. These levels are called geo-/situation-oriented reputation levels.

Thus, VARS uses redundancy within the reputation system and high mobility in order to tackle the attacks. Simulations have proven it usable in face of fake events, up to some satisfying degree of malicious nodes. However sophisticated attacks, such as collusion attacks, cannot be handled because the situation-oriented reputation level allows long-lasting groups of attackers to manipulate a node's reputation database.

E. Illusion Attack on VANET Applications: A Message Plausibility Problem

In this paper [4], a new attack that is specific to VANETs, called Illusion attack is described and a possible solution to address this attack is proposed through a plausibility mechanism. This attack is a type of false message generation attack where the malicious node deceives the sensors in its own car to create the illusion of a false attack. Using this attack a malicious node can cause traffic jams and accidents with ease. Two conditions have been proposed that a malicious node has to fulfill to launch a successful illusion attack. The first condition involves the creation of a suitable traffic situation as referred in [4] on the road and the second is the dissemination of false traffic messages in the network.

A plausibility validation model [4] has been proposed to secure vehicular networks. The input data is obtained by a node either through wireless antenna or through data reported by sensors. The input message is verified through a predefined rule set that is dependent on the type of messages. A number of rules have been proposed to check the plausibility of messages. These include dropping of duplicate messages. The broadcast range of messages is defined based on the type of event and this has been used to calculate the plausibility of the hop count field in a message. The timestamp of the message is checked to ensure that the message is not too old. The velocity field is checked by assuming a maximum permissible velocity. Also, the location is verified by ensuring that the distance covered by the message is greater than or equal to the distance between the positions from where the message was initiated and the current position of the receiving vehicle. If all the fields in

the message pass the validation check then the message is accepted else it is discarded.

III. Proposed Technique: VSRP

A. Proposed Algorithm

The proposed algorithm establishes security in a VANET through accomplishment of trust levels for nodes in the network using reputation and plausibility checks. The algorithm has been designed primarily for safety related information that are broadcasted in single hop and relayed in multihop through intermediate nodes. The packets to be sent will always be broadcasted and a unicasted packet will be taken as malicious information.

The algorithm follows an event oriented approach, that is, a node initiates the communication when it observes an event through its sensors. The types of events have been classified as follows.

(a) *Single-hop:* Information about the events such as application of brakes needs to be communicated by a node only in its one hop neighborhood.

(b) *Multihop:* Information about the events such as traffic jams and accidents is to be communicated by a node in its one hop neighborhood which is to be further relayed by the intermediate nodes to a threshold range, where this is the range up to which the packet can be relayed.

(c) *Malicious-intent:* When a node detects malicious behavior either through the information gained through its own sensors or through checks performed by it after a packet has been forwarded, it communicates this information to its neighbors.

The proposed algorithm in the case of traffic jams and accidents is divided into four phases: neighbor discovery, data dispatching, decision making and trust updating, and neighbor monitoring. In the case of information related to brakes the algorithm is divided into three phases: data dispatching, decision making and trust updating, and neighbor monitoring.

1) *Neighbor Discovery:* Whenever a node needs to forward some event which is either sensed through its own sensors or is forwarded by some trusted node, it initiates the neighbor discovery phase. In this phase, the sensing node broadcasts a N*eighborreq* packet and waits for the *Neighborrep* packets with which it recognizes its neighbors.

In this phase, on receiving a *Neighborreq* packet a node checks in its trust table for that particular node. If the sending node is present and its trust value is 0, the node discards that packet. If the sending node is present and its trust value is not 0, the node accepts the packet and updates its *Reqseentable*. If on updating the *Reqseentable* the sending node is found guilty of data aggregation then its trust value is set to 0 and a malicious-intent message is broadcasted to all the nodes.

If however the node is not present in the *Trust Table* it is inserted in the *Trust Table* with a trust rating of 2 and the node also inserts the request into the *Reqseentable*. The request packet is accepted only if the node is either not in the Trust Table or is present with a trust value not equal to zero.

When the initiator of the request receives *Neighborrep* it scans its *Neighbor Table* and Trust Table to check if the entry already exists for that node. If the entry does not already exist in the Neighbor Table then the initiator inserts it in the Neighbor Table and if it does not exist in the Trust Table then it is inserted in it with a trust value of 2 and counter value of 0.

2) *Data Dispatching:* Once a node has identified its neighbors it broadcasts the data packet and inserts this event in its event table to keep record of the fact that this event had been dispatched.

3) *Decision Making and Trust Updating:* When a node receives a data packet it performs the following checks on it.

STEP 1: If the packet is received from outside the threshold range that means it is pertaining to an event that is far away then the packet is dropped. If the action has already been taken on that event then also the packet is dropped.

STEP 2: If the above two criteria are not met then the node checks whether the event is in its detection range or not where detection range is the range of the node within which the node can detect an event. If the node is itself in the detection range and it has no information about the event then the event is possibly false and it decreases the trust value of the sending node and broadcasts a malicious intent control packet. If the node is itself in the detection range and it has information about the event then the event is genuine and it increases the trust value of the sending node.

STEP 3: If the receiving node however is not in the detection range then it starts a timer and collects the responses from the other nodes in the temptable. If after the expiry of the timer the number of responses collected exceeds the threshold value say $\Delta 2$, the event is considered to be genuine and the trust values of all the sending nodes are incremented.

If however the responses so collected do not exceed the threshold value then the responses are evaluated in accordance with the trust value of the sending nodes as

$$\text{Nresponse} = \sum(\text{Trust value of sending nodes}) \quad (\text{no. of responses of same trust}) \tag{1}$$

If the value of *Nresponse* exceeds the threshold value, the event is considered to be genuine and the trust values of all the sending nodes are incremented.

STEP 4: If however still the threshold is not exceeded the receiving node increases its detection range to maximum in order to collect the responses from the other nodes and performs Steps 2 and 3 again.

Even if after performing these steps the node receives responses less than the above said threshold value it then takes a decision based on the previous trust value of the sending node for which it consults its trust table.

4) *Neighbor Monitoring:* Each node keeps track of all the data that it receives from other nodes. Based on the information that is available with the node and the information that it receives, it is able to identify, whether the data received by it, is from a malicious node or not. Through event classification, we have considered that a genuine packet will always be broadcasted and a unicasted packet will be taken as malicious information.

B. Implementation and Handling of Attacks

The algorithm is meant for four types of attacks, namely, false event generation, data modification, data aggregation and data dropping. The implementation and handling of the attacks is as described below.

False event generation is a type of attack in which a vehicle generates information about an event that actually does not exists. This can be detected with the help of sensors. If a node in the detection range of an event has no information about the event then the event is definitely not genuine. Thus a false event generation can be easily detected.

Data modification is a type of attack in which a vehicle purposely modifies the type of event that is a traffic jam to an accident or vice versa. For this a vehicle changes the type of event field in the data packet. In our algorithm an event is taken to be genuine only if either a required number of nodes generate that information or the information is received from a required number of trusted nodes such that a minimum threshold is exceeded. This feature helps to detect data modification.

Data dropping is a type of attack in which a vehicle does not forward the information it is supposed to forward. In our algorithm neighbor monitoring is a continuous feature in which the nodes simultaneously monitor their neighbor nodes. Thus, if a node has received a packet but is not forwarding it the neighbor nodes can safely assume it to be a data dropping node.

Data aggregation is a type of attack in which a vehicle continuously sends or rather floods packets in the network. In order to handle this, whenever a Neighborreq packet is received from the same node, the counter maintained is incremented by one. This counter is checked at every pre-specified interval of time and if the counter value is found to exceed the threshold value, data aggregation by the malicious node is detected.

Once an attack is detected, the algorithm isolates the malicious node in the network by generating a malicious-intent packet that informs the neighbor nodes about the malicious node. However, this malicious-intent packet is only accepted by the nodes, if it is generated by a trusted node thus imparting reliability to the algorithm.

C. Comparison of the Proposed Algorithm With Existing Approaches

1) *VARS Versus VSRP:* 1) VARS defines the decision area where the trustworthiness of event messages has to be decided upon. Until now these areas are proposed to be of circular shape. Further development should map those areas to the layout of the streets. The algorithm proposed by us makes no such assumptions. The trustworthiness of the messages are decided upon using sensors, decision making phase and the previous trust value of the node.

2) In VARS, depending upon the kind of reputation information a source is attributed with a sender-based reputation level. The thresholds for the confidence decision are adjusted in relation to the relative position of the sender compared to the position of the deciding node. The proposed algorithm improves on the confidence decision making phase as it is independent of the relative position of sender compared to the position of the sending node. First a node checks whether the event is in its own detection range. If not the decision is made on either the rule of majority or on the trust levels already assigned to the nodes.

3) VARS distinguish between situations with respect to availability and quality of reputation in formation as well as familiarity of the area, i.e., rural/unknown or metropolitan/well-known areas. These levels are called geo/situation-oriented reputation levels. Moreover, no parameters have been defined in order to clearly identify these areas. No such Reputation levels are there in the proposed algorithm. All the areas are of equal importance and the reputation levels are assigned on the basis of the number of good or malicious behaviors performed by a node previously.

4) Only if the event is thought to be prevalent, the trust-opinion generator announces this event to the applications. In case the event is not prevalent the proposed algorithm also sends a malicious intent information packet in order to inform the neighbor nodes about the detection of a malicious activity.

5) The proposed system is likely to be susceptible to more sophisticated attacks, such as collusion attacks, because the situation-oriented reputation level allows long-lasting groups of attackers to manipulate a node's reputation database. The proposed algorithm is better equipped to handle such attacks. It can detect at least such attacks if the node is itself in the detection range.

2) *Secure PBR Versus VSRP:* Secure PBR utilizes asymmetric cryptography and digital signatures to achieve security. Incorporating cryptographic mechanisms in the protocol poses challenges of efficient key distribution and management. This would require additional infrastructure. Moreover, manufacture of vehicles is done by different companies and this would require the difficult task of coordination and cooperation of different manufacturers. Plus, cryptography requires high processing time. VSRP which is based on the trust assigned to nodes will perform better in terms of deployment as no additional infrastructure is needed and the calculation time will also be reduced as no cryptographic schemes are employed.

False location generation in secure PBR is handled through plausibility checks. However, there exist possibilities of attack of false information generation under plausibility checks by adjusting the position with respect to the position of neighboring nodes. VSRP eliminates attacks pertaining to false event generation completely by utilizing the plausibility of data collected through sensors as well as the trust value of the sending nodes.

The problem of packet dropping is not addressed in secure PBR, whereas this problem has been effectively handled in VSRP.

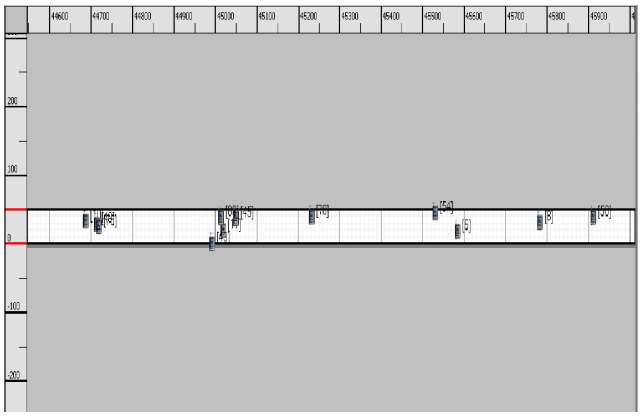

Fig. 1. Simulation topology.

3) *Illusion Attack Versus VSRP:* VSRP can handle illusion attack as it accepts an event as valid only if majority of the trusted nodes agree to its occurrence. Hence, VSRP not only handles illusion attack but a number of other attacks which include message forging, data dropping and data aggregation. Whereas, the solution proposed in the paper on illusion attacks does not handle either of these possible attacks in vehicular networks.

The paper on illusion attacks can detect a false event generated by a malicious node. However, VSRP not only identifies a false event and the corresponding malicious node but also provides a way to eliminate malicious nodes from the network.

IV. Simulation and Results

The proposed VSRP technique has been simulated using the Qualnet Simulator 5.0 [8], [17]. Fig. 1 below provides the simulation topology used to carry out the simulation. A stretch of 12.5 km of a 50 m wide road is taken, on which the nodes are dispersed. The nodes have random speeds and move in a particular direction.

For providing random mobility, the random mobility model available in [8] is modified such that the node only moves in a particular direction. The network is simulated for 10 min.

The values used for the simulation are as follows.

The threshold range for accidents is 4 km, traffic jams is 2 km, and application of Brakes is 400 m. The detection range for accidents is 50 m, traffic jams is 40 m, and application of Brakes is 15 m. Value of $\Delta 1 = 2$ and $\Delta 2 = 10$. Three different cases have been simulated.

Threshold range represents the distance a packet of a particular kind must travel before which nodes will stop relaying it. As per this experiment, information related to accidents is sent to the maximum distance such that other cars on the road could get that information a lot earlier so as to have all the time to take appropriate decision. Already occurring traffic jam information is given medium (still high) threshold distance. This distance is assumed such that it is appropriate enough for a car to take a direction change decision on time. Detection range is the range in which a particular kind of event could be detected. It is assumed to be highest for accidents and minimum for brakes.

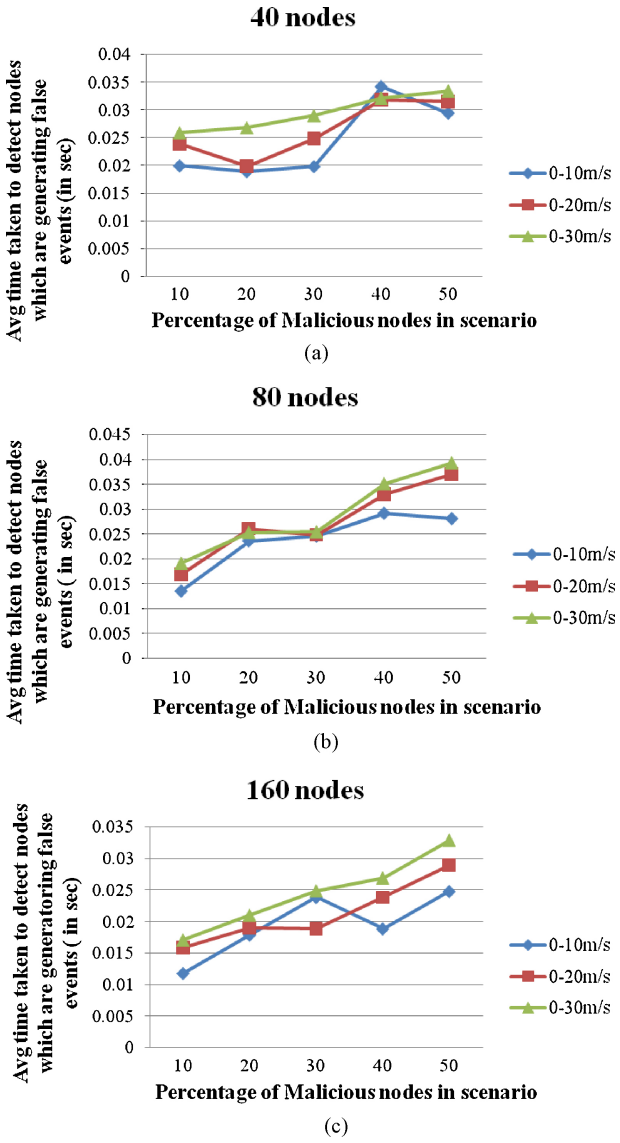

Fig. 2. Average time taken to detect nodes which are generating false information for 40, 80, and 160 nodes, respectively. (a) Mean: 0.02682, Standard Deviation: 0.005407. (b) Mean: 0.026823, Standard Deviation: 0.007233. (c) Mean: 0.021834, Standard Deviation: 0.005526.

In order to increase or decrease the trust value of a node, a single event is not made the basis. In order to double check, we set $\Delta 1=2$. $\Delta 2$ is set to a higher value, which in this case it is set to 10, so as to make sure that a lot of cars are detecting the same thing which provides proper conformity of the information being received with large number of packets.

Analysis: In the above graphs, we can see that in general the time taken to detect malicious nodes which generate false events in the network increases as the percentage of malicious nodes in the network is increased except for some specific cases like speed 0–20 m/s. This is because a false event generating node can be detected with the help of sensors or when a threshold is not exceeded and the greater the number of such nodes greater number of malicious intent packets are needed to be generated in order to isolate them. Also in general at higher speeds time taken to detect such nodes is comparatively higher due to the frequent change in the

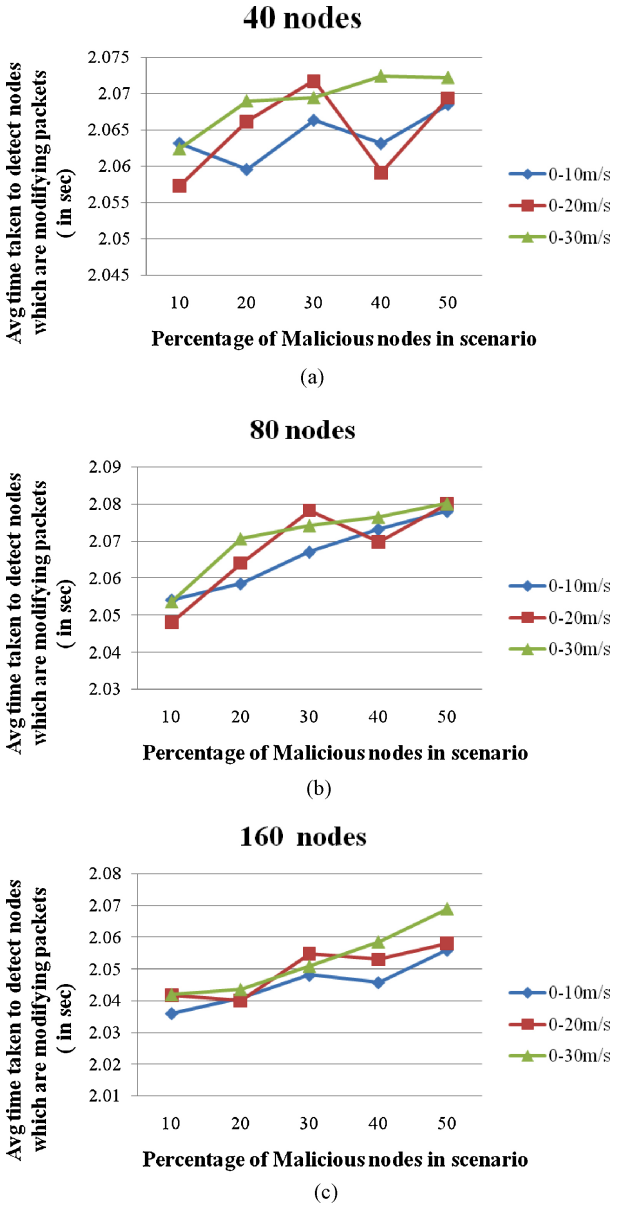

Fig. 3. Average time taken to detect nodes which are modifying packets for 40, 80, and 160 nodes, respectively. (a) Mean: 2.066075, Standard Deviation: 0.004972. (b) Mean: 2.068538, Standard Deviation: 0.010544. (c) Mean: 2.049375, Standard Deviation: 0.008972.

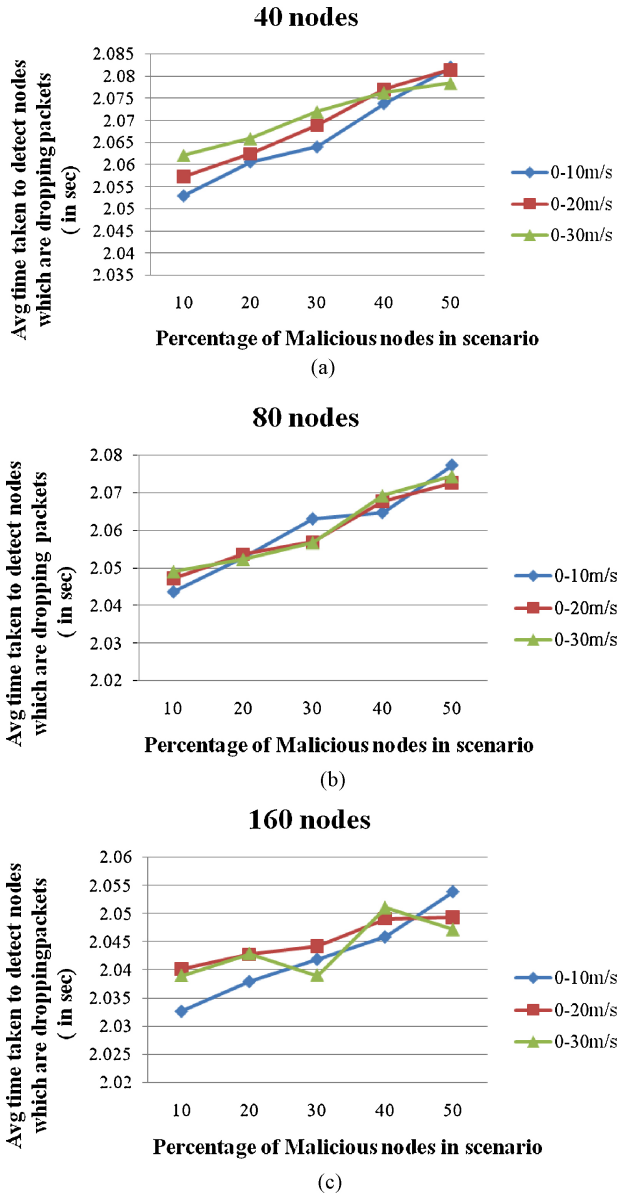

Fig. 4. Average time taken to detect nodes which are dropping packet for 40, 80, and 160 nodes, respectively. (a) Mean: 2.069106, Standard Deviation: 0.0091. (b) Mean: 2.06022, Standard Deviation: 0.010577. (c) Mean: 2.043837, Standard Deviation: 0.005665.

topology and less number of nodes is in the detection range of each other. Also, as we move from 40 nodes to 80 nodes and then to 160 nodes we see that the time taken to detect data modifying nodes decreases (for the same speed and percentage of malicious nodes). This can be attributed to the fact that as the density of nodes increases there are more number of nodes to identify the malicious behavior and hence it happens faster, i.e., since this algorithm is peer to peer so the higher the number of peers, the better the performance.

Analysis: In the graphs below, we can see that the time taken to detect malicious nodes which modify packets in the network increases as the percentage of malicious nodes in the network is increased. This is because a data modifying node can be detected with the help of sensors or when a threshold is not exceeded and the greater the number of such nodes greater number of malicious intent packets are needed to be generated in order to isolate them. Also in general at higher speeds time taken to detect such nodes is comparatively higher due to the frequent change in the topology and less number of nodes is in the detection range of each other. Also, as we move from 40 nodes to 80 nodes and then to 160 nodes we see that the time taken to detect data modifying nodes decreases (for the same speed and percentage of malicious nodes). This can be attributed to the fact that as the density of nodes increases there are more number of nodes to identify the malicious behavior and hence it happens faster, i.e., since this algorithm is peer to peer so the higher the number of peers, the better the performance.

Analysis: In the above graphs we can see that, in general, the time taken to detect malicious nodes which are dropping

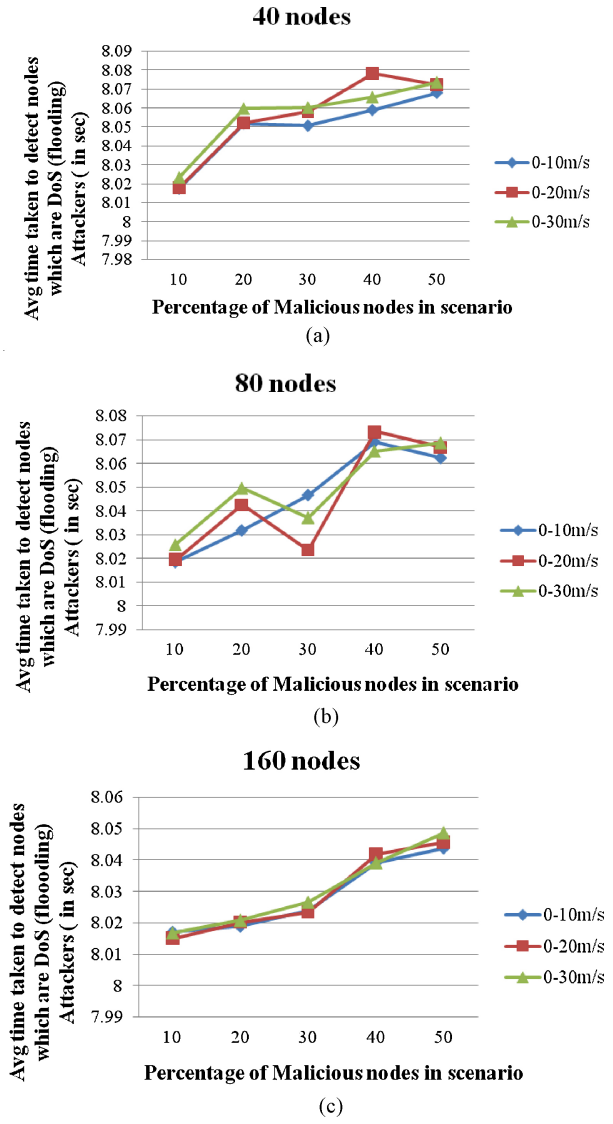

Fig. 5. Average time taken to detect nodes which are dropping packet for 40, 80, and 160 nodes, respectively. (a): Mean: 8.054051, Standard Deviation: 0.019586. (b) Mean: 8.046857, Standard Deviation: 0.019895. (c) Mean: 8.029525, Standard Deviation: 0.012115.

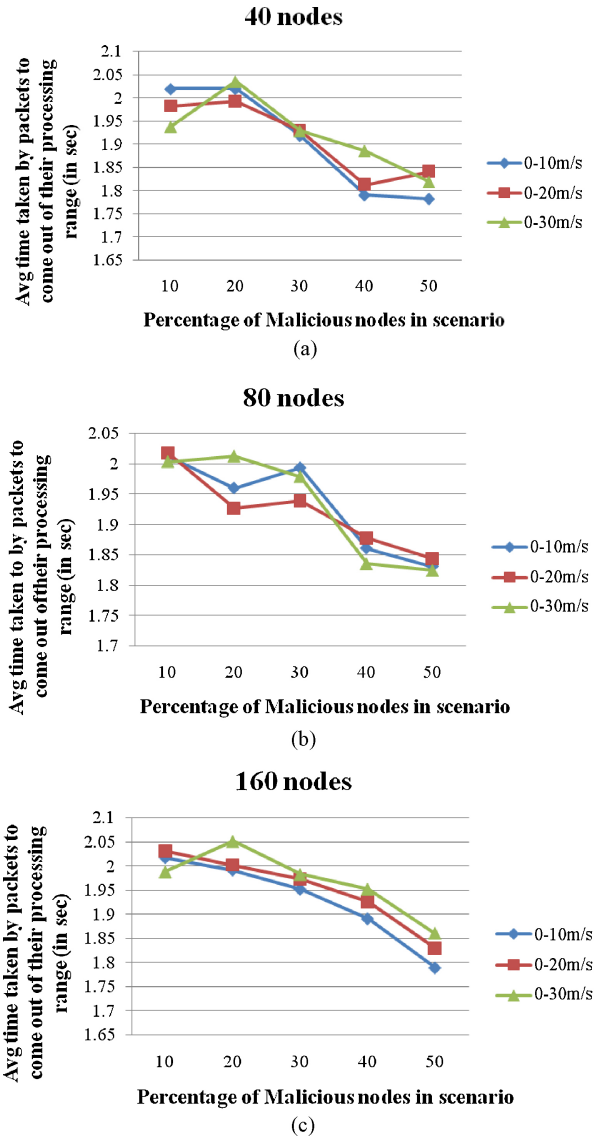

Fig. 6. Average time taken by packets to come out of their detection range for 40, 80, and 160 nodes, respectively. (a) Mean: 1.913733, Standard Deviation 0.087303. (b) Mean: 1.928311, Standard Deviation: 0.074997. (c) Mean: 1.95001, Standard Deviation: 0.07625.

packets increases as the percentage of malicious nodes in the network is increased. This is because a data dropping node can be detected only with the help of neighbor monitoring and the greater the number of such nodes greater number of malicious intent packets are needed to be generated in order to isolate them. Also at higher speeds time taken to detect such nodes is comparatively higher due to the frequent change in the topology. The time taken is almost same as in the 40 nodes scenario indicating the efficiency of the algorithm. As we move from 40 nodes to 80 nodes to 160 nodes we see that the time to detect nodes which are dropping packets decreases because as the density of the nodes increases the number of neighbors which can detect a malicious node will increase and hence the time taken to detect nodes which are dropping packets will reduce.

Analysis: In the above graph, we can see that, in general, the time taken to detect malicious nodes which are flooding packets in the network increases as the percentage of malicious nodes in the network is increased. This is because a flooding node can be detected only when a threshold is exceeded and the greater the number of such nodes greater number of malicious intent packets are needed to be generated in order to isolate them. Also in general at higher speeds time taken to detect such nodes is comparatively higher due to the frequent change in the topology in which the links between the nodes break often. Also, as we move from 40 nodes to 80 nodes and then to 160 nodes we see that the time taken to detect data modifying nodes decreases (for the same speed and percentage of malicious nodes). This can be attributed to the fact that as the density of nodes increases there is more number of nodes to identify the malicious behavior and hence it happens faster, i.e., since this algorithm is peer to peer so the higher the number of peers, the better the performance.

Analysis: In the above graphs, we can see that, in general, the time taken by the packets to come out of their transmission

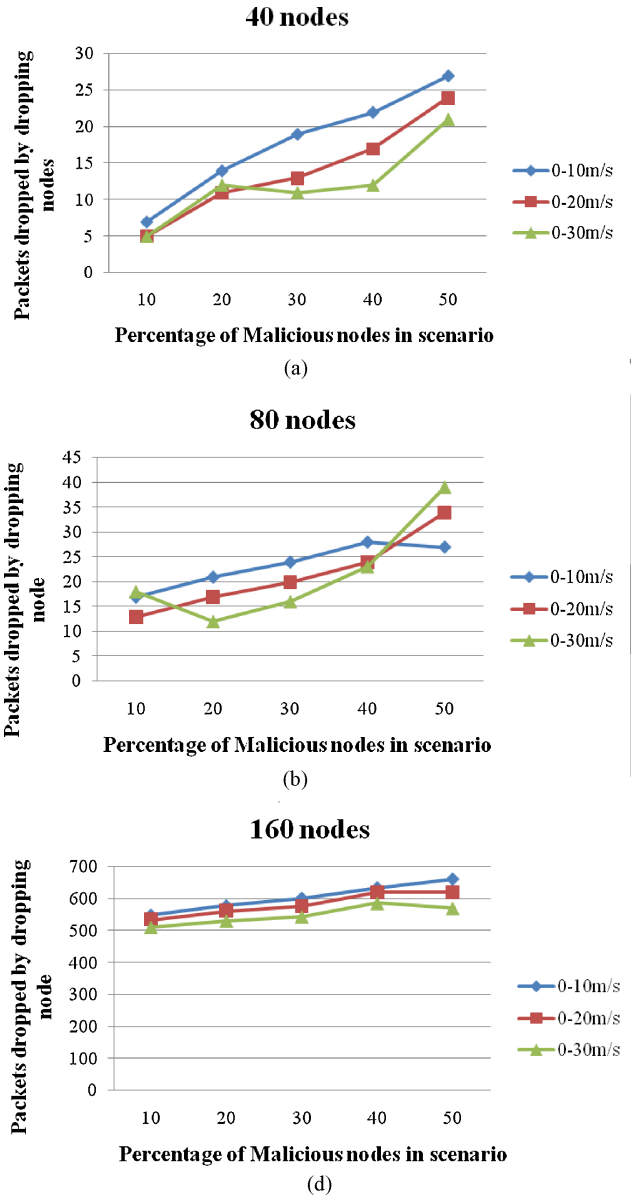

Fig. 7. Number of packets dropped by dropping nodes for 40, 80, and 160 nodes, respectively. (a) Mean: 14.666, Standard Deviation: 6.79986. (b) Mean: 22.2, Standard Deviation: 7.513797. (c) Mean: 579.3333, Standard Deviation: 42.39216.

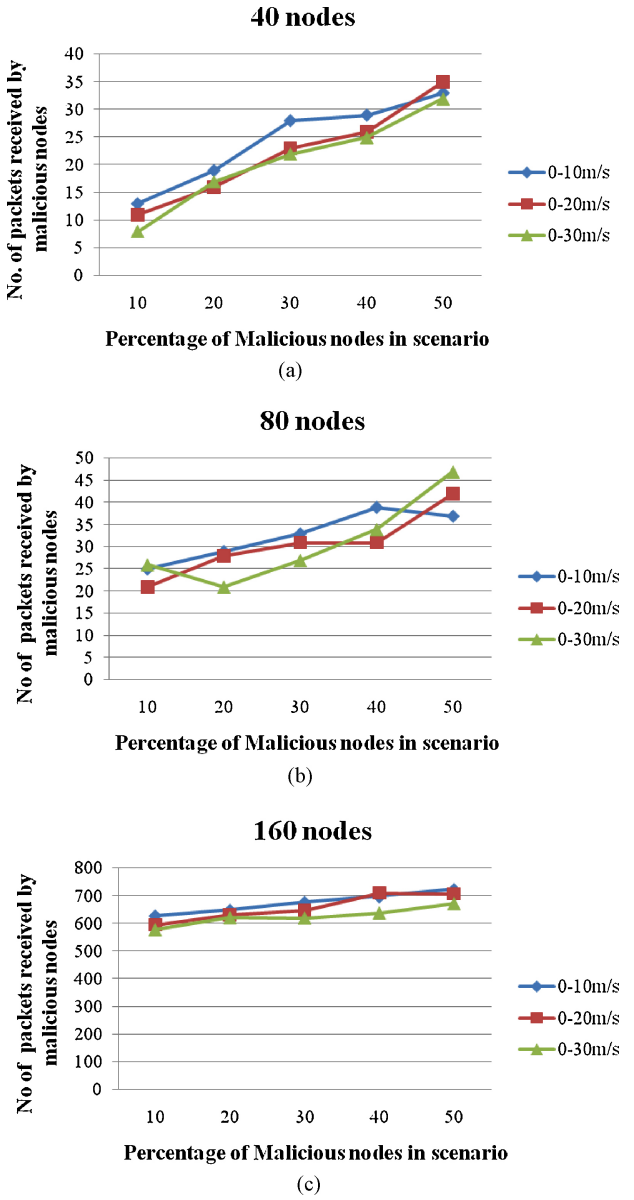

Fig. 8. Number of packets received by malicious nodes for 40, 80, and 160 nodes, respectively. (a) Mean: 22.46667, Standard Deviation: 8.305477. (b) Mean: 31.4, Standard Deviation: 7.452708. (c) Mean: 653.8, Standard Deviation: 43.45309.

range in the network decreases as the percentage of malicious nodes in the network is increased. This is because the algorithm isolates the malicious nodes in the nodes in the network such that a packet is not transmitted through them and the total processing time is reduced. As we move from 40 nodes to 80 nodes to 160 nodes we see that the time taken by the packet to come out of the transmission range increases but only by an extremely small amount which can be accrued to the increase in the number of nodes. This shows the efficiency of the algorithm, i.e., even though the number of nodes is doubling the taken by the packet to come out of its transmission range changes only slightly.

For Figs. 2–6, the anomalies can be explained by the fact that the number and presence of non-malicious nodes which can actually detect the malicious activity where the malicious event might have taken place vary which in turn affect the average calculated.

Analysis: In the above graph, we can see that the number of packets dropped by dropping nodes increase as the percentage of malicious nodes in the network is increased. This is because the larger the number of malicious nodes in the network, the greater the time needed to detect them. Also, at higher speeds less number of packets is dropped by the dropping nodes due to the frequent change in the topology. When we move from 40 nodes to 80 nodes to 160 nodes we see that the number of packets dropped also increases as there is an increase in the absolute number of nodes (see Fig. 7).

Anomalies here can be explained by considering the effect of topology for a particular speed present at the time when malicious event took place, which may result in lesser dropping nodes in range of a node where an actual event occurs.

Analysis: In the above graph, we can see that the number of packets received by malicious nodes increase as the percentage of malicious nodes in the network is increased. This is because the larger the number of malicious nodes in the network, the greater the time needed to detect them. Also at higher speeds less number of packets is received by the malicious nodes due to the frequent change in the topology. As we move from 40 nodes to 80 nodes to 160 nodes there is an increase in the number of packets received because the number of nodes in the network increases (see Fig. 8).

Anomalies here can be explained by considering the effect of topology for a particular speed present at the time when malicious event took place, which may result in lesser dropping nodes in range of a node where an actual event occurs.

V. Conclusion and Future Work

In this paper, we have proposed VSRP which provides robust communication in the case of life threatening events such as accidents as well as traffic jams. It is an event oriented approach that uses reputation-based systems that also utilize sensors attached to vehicles. It is a secure algorithm that can handle a number attacks that include data modification, data aggregation, data dropping and false event generation. Simulation results have shown that VSRP can efficiently handle these attacks and can detect up to 85% malicious nodes in most of the cases.

The timely identification of malicious nodes is very critical in vehicular networks as even a very slight delay could lead to loss of life and property. The average time taken by VSRP to detect malicious nodes that perform false event generation is 0.025 s, data dropping is 2.06 s, packet modification is 2.06 s, DOS (flooding) attacks is 8.04 s. It can be seen that the time taken by VSRP for the detection of various malicious nodes is suitable for securing real time traffic information. Also, the average time taken for a packet to come out of its processing range is 1.95 s which shows that the nodes receive real time traffic information in a timely manner giving the drivers adequate time to decide their course of action.

While most of the algorithms just detect the malicious nodes, VSRP not only detects malicious activity but also eliminates the malicious nodes. VSRP is also the ideal solution to the vehicular problems of developing countries as it is infrastructure less. Since it is infrastructure less, it is more cost efficient and also does not pose the problems associated with RSUs such as the RSU becoming a bottleneck. The control overheads in VSRP are also reduced as each node forwards the data intelligently and does not work in a brute force manner by forwarding the same information from different neighbor nodes a number of times.

The simulation results show that VSRP provides an efficient and robust method to secure vehicular networks without using any infrastructure.

In future work, we plan to extend VSRP to provide information to a particular region that is geocasting. We intend to study the possible use of vehicle to vehicle communication without using any infrastructure for the purpose of providing traffic information such as velocity and density on a particular road to other vehicles in the network. VSRP could be suitably extended and modified to secure such applications. We also plan to study other applications of VANETs such as entertainment, automatic toll collection, and location-based services and to extend VSRP to handle these applications.

References

[1] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETs," NEC Network Laboratories, Heidelberg, Germany, NEC Tech. Rep. NLE-PR-2006-19, Version 1.1, Mar. 2006.

[2] C. Harsch, A. Festag, and P. Papadimitratos, "Secure position-based routing for VANETs," in *Proc. Veh. Technol. Conf.*, 2007, pp. 26–30.

[3] F. Dotzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad-hoc network reputation system," in *Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw.*, Jun. 2005, pp. 454–456.

[4] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET applications—A message plausibility problem," in *Proc. 2nd IEEE Workshop Autom. Netw. Appl.*, Nov. 2007, pp. 1–8.

[5] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2003, pp. 1510–1515.

[6] G. Philippe, G. Dan, and S. Jessica, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, 2004, pp. 29–37.

[7] [Online]. Available: http://www.scalable-networks.com/

[8] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP : Efficient condition privacy preservation protocol for secure vehicular communication," in *Proc. IEEE 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1229–1237.

[9] P. Papadimitrators, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communications systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

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

[11] Y. Peng, Z. Abichar, and J. M. Chang, "Roadside-aided routing (RAR)in vehicular networks," in *Proc. IEEE Int. Conf. Commun.*, vol. 8. Jun. 2006, pp. 3602–3607.

[12] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int Workshop Veh. Ad Hoc Netw.*, Oct. 2004, pp. 29–37.

[13] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.

[14] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. 3rd Eur. Workshop. Security Privacy Ad Hoc Sens. Netw.*, vol. 4572. Jul. 2007, pp. 129–141.

[15] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in Proc. 1st Int. Workshop Wireless Netw. Intell. Transp. Syst., Aug. 2007.

[16] *QualNet User's Manual*, version 3.6, Scalable Network Technologies, Inc., Los Angeles, CA, USA, 2003.

[17] A. A. Wagan, B. M. Mughal, and H. Hasbullah, "VANET security framework for trusted grouping using TPM hardware," in *Proc. 2nd Int. Conf. Commun. Softw. Netw.*, Feb. 2010, pp. 309–312.

[18] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security issues and challenges of vehicular Ad Hoc networks (VANET)," in *Proc. 4th Int. Conf. New Trends Inf. Sci. Service Sci.*, May 2010, pp. 393–398.

[19] V. Paruchuri, "Inter-vehicular communications: Security and reliability issues," in *Proc. Int. Conf. ICT Convergence*, Sep. 28–30, 2011, pp. 737–741.

[20] A. Wasef, L. Rongxing, L. Xiaodong, and S. Xuemin, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 22–28, Oct. 2010.

[21] Y. Gongjun, B. B. Bista, D. B. Rawat, and E. F. Shaner, "General active position detectors protect VANET security," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Oct. 26–28, 2011, pp. 11–17.

Sanjay K. Dhurandher received the M.Tech. and Ph.D. degrees in computer science from the Jawaharlal Nehru University, New Delhi, India.

He is currently an Associate Professor in the Division of Information Technology, Netaji Subhas Institute of Technology (NSIT), University of Delhi, New Delhi, where he is also the Head of the Advanced Centre of IT in Financial Systems. From 1995 to 2000, he was a Scientist/Engineer at the Institute for Plasma Research, Department of Atomic Energy, Gujarat, India. His current research interests include wireless ad hoc networks, sensor networks, computer networks, opportunistic networks, network security, and underwater sensor networks.

Dr. Dhurandher currently serves as the Associate Editor of Wiley's *International Journal of Communication Systems*.

Mohammad S. Obaidat (F'05) received the M.S. and Ph.D. degrees in computer engineering with a minor in computer science from Ohio State University, Columbus.

He is an internationally well-known academic/researcher/scientist. He is currently a Full Professor of computer science at Monmouth University, West Long Branch, NJ, USA, where he was the Chair of the Department of Computer Science and the Director of the Graduate Program. He is also with the Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, United Arab Emirates. He was an Advisor to the President of Philadelphia University. He has received extensive research funding and has published more than ten books and more than 550 refereed technical articles. He has chaired numerous international conferences and given numerous keynote speeches all over the world.

Dr. Obaidat is the Editor-in-Chief of three scholarly journals and also the Editor and Advisory Editor of numerous international journals and transactions including IEEE journals/transactions. He was the President of the IEEE Solid-State Circuits Society (SCS). He is a Fellow of the SCS.

Amrit Jaiswal received the Graduate degree in information technology from the Netaji Subhas Institute of Technology, University of Delhi, New Delhi, India. He is currently working toward the Postgraduate degree in finance from the Indian Institute of Management Indore, Indore, India.

His current research interests include computer networks, network security, and vehicular/mobile ad hoc networks.

Akanksha Tiwari received the B.E. degree in information technology from the Netaji Subhas Institute of Technology, University of Delhi, New Delhi, India, in 2011.

She is currently a Software Developer at Adobe India, Noida, India. Her current research interests include collective information, information management, and ad hoc networks.

Ankur Tyagi received the B.Tech. degree in electronics and communication engineering from the Technological Institute of Textile and Sciences, Bhiwani, India, in 2008.

He is currently a Senior Application Engineer at Eigen Technologies Pvt. Ltd., New Delhi, India. His current research interests include network and media access control layer design and implementation for vehicular/mobile ad hoc networks and wireless sensor networks.