Hindawi
Journal of Sensors
Volume 2018, Article ID 6576841, 17 pages
https://doi.org/10.1155/2018/6576841

Research Article

VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead

Sheeraz Ahmed,[1,2] **Mujeeb Ur Rehman**,[2] **Atif Ishtiaq**,[1] **Sarmadullah Khan**,[3] **Armughan Ali**,[4] **and Shabana Begum**[5]

[1]*Iqra National University, Peshawar, Pakistan*
[2]*Career Dynamics Research Centre, Peshawar, Pakistan*
[3]*School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK*
[4]*COMSATS Institute of Information Technology, Attock, Pakistan*
[5]*Islamia College University, Peshawar, Pakistan*

Correspondence should be addressed to Sheeraz Ahmed; sheerazahmed306@gmail.com

Received 23 February 2018; Revised 15 May 2018; Accepted 4 June 2018; Published 16 July 2018

Academic Editor: Almudena Rivadeneyra

VANET is an application and subclass of MANETs, a quickly maturing, promising, and emerging technology these days. VANETs establish communication among vehicles (V2V) and roadside infrastructure (V2I). As vehicles move with high speed, hence environment and topology change with time. There is no optimum routing protocol which ensures full-pledge on-time delivery of data to destination nodes, and an absolutely optimum scheme design for flawless packet exchange is still a challenging task. In VANETs, accurate and on-time delivery of fundamental safety alert messages (FSAMs) is highly important to withstand against maliciously inserted security threats affectively. In this paper, we have presented a new security-aware routing technique called VANSec. The presented scheme is more immune and resistive against different kinds of attacks and thwarts malicious node penetration attempts to the entire network. It is basically based on trust management approach. The aim of the scheme is to identify malicious data and false nodes. The simulation results of VANSec are compared with already existing techniques called trust and LT in terms of trust computation error (TCE), end-to-end delay (EED), average link duration (ALD), and normalized routing overhead (NRO). In terms of TCE, VANSec is 11.6% and 7.3% efficient than LT and trust, respectively, while from EED comparison we found VANSec to be 57.6% more efficient than trust and 5.2% more efficient than LT. Similarly, in terms of ALD, VANSec provides 29.7% and 7.8% more stable link duration than trust and LT do, respectively, and in terms of NRO, VANSec protocol has 27.5% and 14% lesser load than that of trust and LT, respectively.

1. Introduction

Communication remains a main focus of interest in human beings. Hence, in results of continuous struggle, it became possible to replace one communication medium by other fastest communication means for sending and receiving information. Computer networks are a bunch of networked computing hardware devices interchanging data to the communicating networked devices through a data link. The link between nodes is fixed, that is, wired or with wireless media. The Internet is a prominent computer network. Wireless technology does not provide full security of information because the medium is open. To ensure security, encryption/decryption techniques are used to identify the authorized users. Table 1 shows different types of wireless networks.

The wireless sensor network (WSN) is a self-organizing, infrastructureless network. WSN is an example of wireless networks using IEEE 802.15.4 protocol designed for low-rate WPANs and also for sensor networks. WSN consists of numerous small sensors with low cost, low battery power, and limited computational capabilities and low communication bandwidth. These sensor nodes are used to collect information as well as integrate and transmit data in a wireless fashion and handover it to the base station (BS) via a gateway node [1]. WSN is comprised of power components, radio transceiver, and computing and sensing devices. Sensors are

Table 1: Different types of wireless networks.

Type	Applications	Range	Standards
Personal area network (PAN)	Cable replacement for peripherals	Within reach of a person	Bluetooth, ZigBee, NFC IEEE 802.15
Local area network (LAN)	Wireless extension of wired network	Within a building or campus	IEEE 802.11 (Wi-Fi)
Metropolitan area network (MAN)	Wireless internetwork connectivity	Within a city	IEEE 802.16 (WiMAX)
Wide area network (WAN)	Wireless network access	Worldwide	Cellular (UMTS, LTE, etc.)

hundreds and thousands in number, communicating with each other through radio communication over an industrial, scientific, and medical (ISM) radio band.

To obtain information on location and positioning, local positioning algorithms and the global positioning system (GPS) can be employed [2]. The IEEE 802.11p standard known as wireless access in vehicular environments (WAVE) is a specially developed version to adapt vehicular ad hoc network (VANET) requirements and support intelligent transport systems (ITS). IEEE 802.11p is one of the fresh sanctioned amendments to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). In this sense, IEEE 802.11p is denoted as WAVE.

Information and communication technology (ICT) plays a vital role in making the cities smarter in the future through intervehicle communication (IVC), using an infrastructure of Car4ICT using IEEE 802.11p based on dedicated short-range communication (DSRC) protocol [3]. Car4ICT infrastructure is a future technology which will facilitate users by easily accessing different applications like routing, uploading, and downloading data. It also provides data processing and storage facilities for the users. Such services are complex and require detailed knowledge to constitute it in big cities [3]. IEEE 802.11 is an accumulation of physical layer (PHY) specifications and media access control (MAC) for implementing WLAN in the 2.4, 3.6, 5, and 60 GHz frequency bands, maintained by the IEEE 802 LAN Standards Committee in 1997.

A mobile ad hoc network (MANET) is a network which has many autonomous mobile nodes which are free to move in any direction, also continuously modifying their locations in a self-configurable manner. It is an infrastructureless network; these nodes have the capacity to connect with Wi-Fi or any cellular infrastructure. VANET is an application of MANETs. VANET is a wireless ad hoc network, in which moving vehicles behave like mobile nodes and allow them to connect with each other via DSRC, and a protocol proposed for WAVEs is IEEE 802.11p for IVC. VANETs enable infrastructure-to-vehicle (I2V), or vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V) communication system [4, 5].

V2I communication is a wireless exchange of safety messages and access to the Internet between vehicles and roadway side units. A major concern of VANETs is to avoid vehicle collisions and get updates about road condition, weather information, traffic jam situation, and so on. In V2V infrastructure, when vehicles come in the communication range, it results in an automatic connection and establishes an ad hoc network. This enables sharing of position, speed, and direction data; again, DSRC connects with the global positioning system (GPS) resulting in a V2V communication system which provides a 360° view of vehicles within the communication range.

VANETs utilize movable vehicles and establish a wireless link among vehicles with features such as rapid changing topology, high computational ability, predictable mobility, and variable network density. VANET architecture consists of three parts: (i) an on-board unit (OBU) which is built in the vehicles or vehicles itself, (ii) an application unit (AU) person set in the car, that is, driver, and (iii) a roadside unit (RSU) installed on highways which constitutes the VANET system and provides a basis for an intelligent transportation system (ITS) [4, 5]. The researchers successfully advent a network with the collaboration of WSNs and VANETs named as vehicular sensor networks (VASNETs). Vehicles are mobile nodes in VASNET, and an important application for vehicular networks is cooperative collision warning (CCW) message disseminations, which uses V2V communication and hence achieves safety [6]. The basic VANET structure is shown in Figure 1.

VANET is an application of mobile ad hoc networks (MANETs) which differs from MANETs in a few ways like the following. (i) Power is a constraint in MANETs, but in the case of VANETs, power is not due to tremendous installed battery. (ii) Moving pattern: in VANETs, nodes move coherently, while in MANETs node moments are random. (iii) Mobility: the mobility ratio in VANETs is bigger than in MANETs [6]. VANETs have three main architectural categories, which are as follows. (i) Pure ad hoc mode: in this mode, only V2V communication exists and no other infrastructure takes part. (ii) Pure cellular or WLAN mode: in this mode, vehicles can easily access information from cellular towers and access points (APs). (iii) Hybrid mode: this mode can use and access data from cellular/WLANs as well as from pure ad hoc mode depending upon the information capacity and route congestions [4, 5].

VANETs have different characteristics, summarized as follows:

(i) *High mobility*: in VANETs, vehicles move at high velocity which causes the contraction of the mesh network. So, in such case, vehicle position identification is difficult and it also leads to poor security provision to node privacy.

(ii) *Rapidly changing network topology*: in VANETs, vehicles move randomly with high speed, so evidently

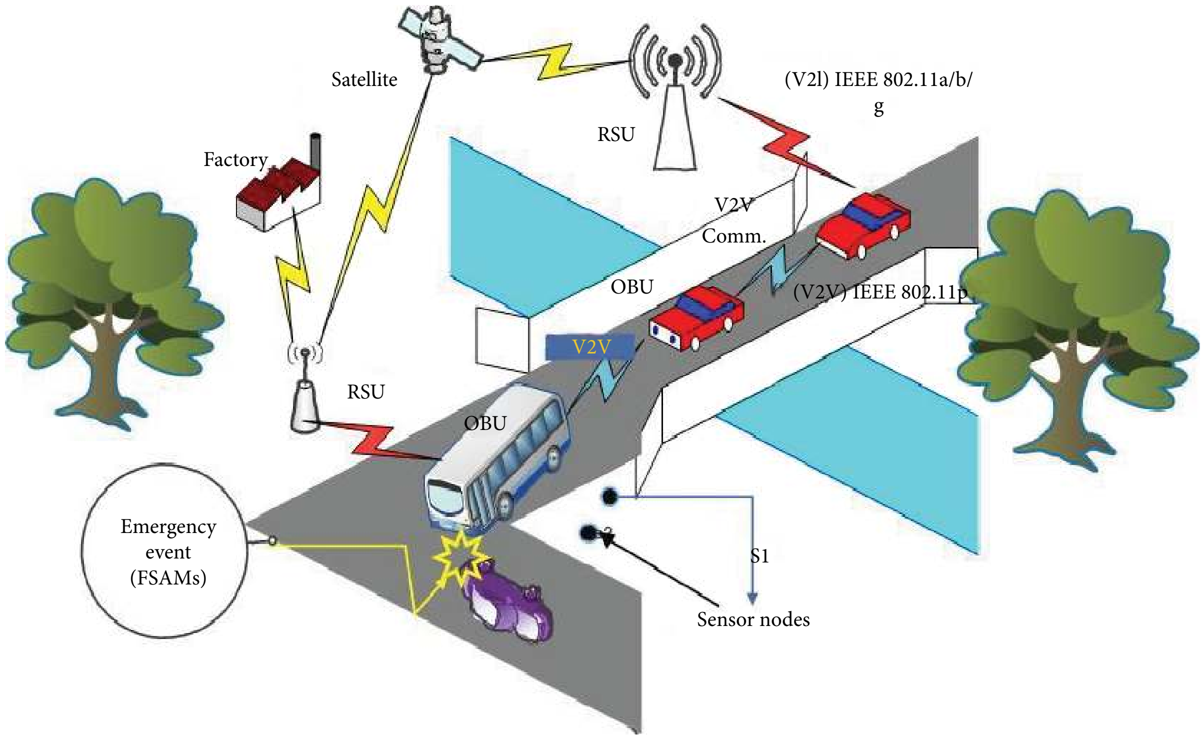


Figure 1: Basic VANET structure.

the position of vehicles will change most oftenly. The topology is dynamic and irregular. It encourages attacks in the network and makes it difficult to sort out misbehavior/attacks in the network [7].

(iii) *Availability of the transmission medium*: VANET size in the geographical point of view is boundless. VANET infrastructure can be designed for a city, cities, or as a whole for a country. The wireless medium is a universally available transmission medium, which is a big reward in IVC.

(iv) *Frequent exchange of information*: the VANET network is ad hoc in nature. In VANETS, nodes gather information from the neighbor vehicular nodes and also from RSUs. So, in this way, nodes exchange their information.

(v) *Attenuations*: DSRC is a digital transmission band facing problems in transmission frequencies; these are reflection, diffraction, and dispersion, various kinds of fading phenomena, and Doppler effect losses. Due to multipath padding propagation, delays occur [7].

(vi) *Time critical*: in VANETs, time period management is absolutely needed; it should be ensured that information reaches to the exact accurate node in the specified time, to enable the node for decision and execute action accordingly.

(vii) *Limited bandwidth*: VANETs use the DSRC band with a limited bandwidth of 27 MHz; the theoretical data rate is 27 Mbps.

(viii) *Energy storage and computing*: VANET is rich in energy, computing capability, and storage.

(ix) *Limited transmission power*: in a WAVE scenario, the transmission power is up to 1000 m and ensures data reachability to nodes. In congestion or accident situation, transmission power can be maximizes [7].

Security of VANETs is an important factor which protects information related to the driver and vehicle from unauthorized access and ensures privacy of the driver and vehicle. In VANET scenario, nodes are highly dynamic; in such networks, information security is a very tough job.

1.1. Security Requirements in VANETs. To ensure information security, different security goals should be fulfilled; the most common security requirements are confidentiality, data integrity, and availability. In addition, other security requirements are authentication, data check, and nonrepudiation [8]. So, collectively in VANETs, six security goals should be fulfilled. Keeping information hidden from unauthorized access is called *confidentiality*, protecting information from unauthorized changes is called *integrity*, and accessibility to the required information by an authorized user is called *availability* [7]. The process which belongs to the verification of information generated by the sanctioned user is called *authentication*. The transmitted message is confirmed and checked by the receiving node/vehicle; whether the received data is correct or having some false information is called *data check*. *Nonrepudiation* is the process in which the sender of a message cannot disown himself from the communication at the end of the communication session [8]. Data correlation can also be considered a security requirement which easily finds out bogus data, by correlation to finger out the similarity between the data received and the data transmitted. Making secure the position of vehicle and BS is also a concern with VANET security [7]. Entities that are involved in VANET security are drivers, OBUs, RSUs, and attackers. The driver is a key part of the VANET system taking decision in emergency situations providing safety to the vehicle and comfort to passengers.

Vehicle OBU may be a normal automated system or may be an attacker impersonating himself as a normal node, and similarly RSUs can be normal or may be a malicious node and can disrupt the normal network activities for the attacker's own benefits. Attackers can launch different kinds of techniques to interrupt normal network functions; attackers can be internal or external, and they have only one motive to benefit themselves [7]. Attackers can be of two types; they may be rational and irrational and can do active or passive attacks. Active attacks are detectable while passive attacks are not. The third party should be a trusted or semitrusted authority, or it may be a manufacturer of the vehicles which is also a key entity of the VANET system [8].

1.2. Possible Attacks that Are Vulnerable to VANET Security

(i) Attacks on availability: in such attacks, the attacker shuts down the entire network and the node has no access to the information.

(ii) Attacks on authentication: identification of vehicles is mandatory to rectify the genuine sender and receiver, confirm identity first to kick out intruders, and reduce the chance of information loss.

(iii) Attacks on confidentiality: the information should be confidential between the authorized users and kept hidden or encrypted from the intruders to avoid traffic analysis or snooping attacks.

(iv) Attacks on integrity: the intruder should change the data by deletion, insertion, and modification of data according to his requirements and benefits. Data integrity keeps away repudiation and replaying attacks.

(v) Attacks on nonrepudiation: the ability to confirm that the sender and receiver of the message are authentic users and at the end they cannot refuse to acknowledge [7, 9].

(vi) Another attack known as denial of service (DOS) or distributed denial of service (DDOS): it hijacks the network totally, slows down the entire process and interrupts the services of network. The intruders send many fake or bogus requests, reply to the network, and impersonate themselves as a normal vehicle OBU or RSU, and the network seems busy or out of reach, not responding to the genuine vehicles [10].

(vii) Identity revealing: disclosing details of the individual vehicle can put security at danger. Later character revealing must be avoided.

The various other types of attacks are like broadcast tampering, Sybil attacks, message suppression attacks, alteration attack, and wormhole attack [11]. Lots of research work are done on ITS, and nodes are equipped with communication technology. Messages are exchanged between nodes containing information regarding their current location and its surroundings. Different techniques are used in the VANET system to enhance its security. To reduce the accident ratios and ensure safe transportation, different approaches are used to identify the causes of traffic accidents in ITS.

National Databank Wegverkeer (NDW) is a database containing real-time data about the traffic network of the Netherlands. When a crash occurs, the factor can be easily found out from NDW. Another technique is event data recorder (EDR), a device built in the vehicle which collects violent information regarding the vehicle's speed, heading, and engine accelerator. The main aim of EDR is to get information about the event when the crash is faced by the vehicle system, that is, EDR provides postaccident information and causes of the accident can be easily investigated. EDR can also collect other kinds of data if appropriate sensor nodes are used [12].

IEEE 802.11p is a standard protocol for WAVE. In VANETs, vehicles are equipped with DSRC to broadcast messages to neighbor nodes. Neighbor nodes/vehicles are also equipped with DSRC or stationary stations located at the roadside. These messages contain information, like safety warnings and traffic information. IEEE 802.11p determines a set of two types of messages: cooperative awareness message (CAM) and decentralized environmental notification message (DENM) used in ITS [12]. CAM is broadcast and replicated again and again to all nodes in the neighborhood. CAM shows positioning and other basic status-related information of the communicating entities in the ITS system [12]. DENM is the second message presented by 802.11p. The message is also broadcasted to other ITS stations when a particular incident occurs to inform other vehicles. Wrong way driving, accident, and roadwork are the examples of such incidents.

On detection of hazardous events by the ITS station, it starts broadcasting without any delay a DENM message to other ITS stations in the region (a specific geographical area) which can be affected by the event. The message is continuously broadcasting repeatedly, till the event is over. When the specified event is over, a special DENM message is circulated to inform all nodes about the disappearance of the event [12].

An autonomous traffic management scheme which enables the vehicular network, to exchange data between vehicles, should be about the change of route in case of congestion, traffic jam condition, or any other emergency situation. The network is called VANET-based autonomous management (VAM) scheme.

In the presence of traffic light, VAM establishes coordination between vehicles and the light controller to overcome congestion [13].

To keep information security in VANETs, different approaches are used. Public key cryptography (PKC) is an asymmetric key algorithm, in which a key used for encryption of a message is not used for the decryption of that message. Encryption and decryption are done with two separate keys. In such algorithms, each node has a pair of cryptographic keys: one is public encryption key (PEK) and the other is private decryption key (PDK). The pair of cryptographic keys is generated by the real time application (RTA) technique periodically. Public keys are reached to each and every RSU in its operation area via a secure medium/channel.

Traditional wired networks are protected by several lines of defense such as firewalls and gateways. Security attacks on such networks may come from any direction and target all nodes. VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and centralized administration. The main challenge facing VANETs is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are, and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in a privacy-vital environment [14].

2. Literature Review

ITS and VANETs have been under research for many years. But with the advancement in generation of communication technology, there is a need to refine the information exchange process and come up with better security and more fulfilling solutions against threats that meet the demands of the day. With the world moving steadily towards WAVE, there is a need to refigure the entire ITS system security and ensure that the VANET security process does not prove to be a bottleneck in the advancement of the ITS technology. We shall have a look at some of the earlier works done in the field of VANET security in order to eliminate or reduce the frequency of attacks in VANETs by malicious nodes.

In paper [15], researchers proposed a novel authentication mechanism for secure message transmission in a VANET scenario. The author has shown that an already existing technique of message authentication was based on a combined signature technique, in which the forwarding node used a combined signature algorithm via RSU and results in a huge transmission overhead message. Due to a combined signature scheme, RSU sometimes transmits fake authenticated messages toward nodes. To avoid such issues, the authors proposed an aggregate message authentication code technique which verifies the integrity and authenticity of messages and thinned communication overhead.

Pseudo-RSUs were installed in the neighborhood of RSU to stop false information dissemination, to ensure exchange of rectified authenticated messages. The authors proposed a technique based on results obtained from simulations and security parameters which reduced considerably the communication overhead and enhanced the validity of disseminated information, which validated the authors' suggested technique. In [16], the authors fabricated a technique which has studied security aspects of V2V communication utilizing a radiofrequency (RF) transceiver. The main part of the VANET environment is position-based information of the vehicular node. The use of an RF transceiver improved the trust on received data about the vehicle's location. The suggested model of authors followed the rule of "Trust on what you observed, confirm what you listen." The basic motive of the scheme was to find a vehicular communication system best suited in minimum cost and more effective in data distribution, as well as to ensure passengers' safety, security, and comfortability.

The RF transceivers verify reported data in the network and approve the position of the neighbor's vehicles and that of the malicious vehicle too and hence ensured the security of the network. The authors suggested a scheme which enhanced VANET security through precluding malicious entities from penetration into the network, hence reducing the chances of putting invalid data about the position information of vehicles.

In paper [17], researchers designed a novel technique of detection, named greedy detection for VANETs (GDVANs); it was for the purpose of reducing greedy behavior frequency in VANETs. VANETs' basic motive was to assure road passengers' safety and enhance transportation quality. Multiple attacks were launched in VANETs; among them, one was denial of service (DOS) attack, which interrupted authorized clients from available information.

The authors proposed a technique incorporating two phases: suspicious phase and decision phase. The suspicious phase followed the concept of linear mathematical regression, where a fuzzy logic decision scheme was followed by a decision phase. The advantage of the designed scheme was that the network nodes had the capacity of execution and no change was required in the standard IEEE 802.11p protocols at any stage. Moreover, the technique had the ability of greedy behavior-type threat detection and found a potentially compromised node list, utilizing three newly defined metrics. The authors justified and validated their proposed scheme from results obtained from experiments or simulation.

In [18], the authors demonstrated that VANETs basically had the opportunity of safe wireless communications with threat avoidance capability, but still, security threats in VANETs are a disputing task, like access control, integrity of data, confidentiality, nonrepudiation, availability, and data privacy. The paper suggested a model which was about VANETs protecting against threats, labeled as an attack-resistant trust (ART) management algorithm. ART had not only detection capability of malicious data and node but also the ability to deal with malicious attacks. In VANETs, ART judged the trustworthiness of both data and mobile nodes. Especially, assessment of data trust was done on the basis of sensed and collected data from various vehicles; judgment of node trust was done in two ways, that is, functional trust and recommendation trust, which reveal how probably a node could accomplish its functionality and how trustworthy the recommendations from a node for other nodes would be, respectively. The authors validated their proposed scheme ART, via experimental data they analyzed. Moreover, the scheme ART had broad applications in VANET background, to enhance traffic experimentation in terms of secure mobility, with reinforced reliance. Agarwal et al. [19] developed a theory to assure security inside educational institutions, medical institution/health care centers, residential places, and so on, through conversion of stodgy vehicles into connected vehicles to prevent careless driving. In the designed model, entry and exit points (gates) were defined. Authors suggested wireless hardware-type "GPS" arrangement to supervise moving vehicles, velocity, and region of entry. At the entryway, orthodox vehicles obtain a device from guards on duty and return the device back upon exiting to authorized guards on duty.

When the devices were activated, a communication mean/path is set up among security depots and drivers inside the specified region to avoid rule violation. For vehicles inside that particular region which have a speed threshold, on crossing the threshold value warning messages were disseminated between the vehicle operator and the system. In the depot, receiving unit holds previous record of each individual drive separately; in terms of any misconduct penalizing action taken versus the handed driver. The scheme proposed by authors was judged on trial bases and, over race, was cut down up to sixty percent securing residential human areas; these characteristics validated the scheme efficacy.

In [20], researchers had considered VANET a complicated network, in which all vehicular node moments were in random manner. In VANETs, the node position changes, so data dissemination was a problem; also, creation of new links took place each time for data packet transmission. So, in such scenario, an attack could wind up all communications running among vehicular nodes. According to authors' conclusion, the Sybil attack was one among other different attacks in VANETs, due to which packet loss occurred. In this paper, the authors discuss impacts of Sybil attempts on VANET communication protocols. Further, researchers examined and scrutinized the verity of VANET routing hierarchies and found the AODV routing scheme to be more efficient in terms of attacks launched in VANET fencing. In the existence of attack in VANETs, the AODV algorithm used simulator QualNet 5, whose output results were satisfactory, but more advancement in routing hierarchy was still required.

Researchers in [21] exhibited that VANET security was the most research-adopted area due to its quality of providing better protection to drivers, vehicles, and so on. Vehicles in VANETs move with maximum acceleration, and also network topology dynamically changes which makes it hard to wipe out false invalid nodes totally and ensure dispersion of data among nodes safely. Hence, in the authors' view, information privacy and security in VANETs were the most vital research-inquired tasks.

In the paper, the authors exemplified different security threats to VANETs and pointed out possible remedy algorithms to mitigate those attacks. The authors had categorized those defensive mechanisms and analyzed them on a dissimilar performance point of view. Eventually, research workers found different research subjects based upon VANET security threats and incited scientists to work on these topics and discover an efficient method to resolve threats and attacks in VANETs.

Research work in [22] presented a detection problem of DOS attacks happening in VANETs. The authors' primary contribution was to conceptualize a new security model based on a game pattern for DOS attacks in VANETs. Secondly, researchers expressed two conditions about game theory, strategic-type game, and extensive-type game. Thirdly, authors had studied DOS attacks on the basis of practical suppositions, utilizing the actual mobility models based on an actual map. Finally, authors analyzed their designed model and validated it through a simulation process. Moreover, authors stated about their contribution in research that no such type of game-related model was designed earlier. Researchers concluded their research work analysis that they will solve DOS attack problems arising in VANETs.

In [23], researchers showed that with the growth of security techniques in VANETs, threats also grow relatively. Authors proposed a trust-based management algorithm called threshold adaptive control technique; the technique was mainly used to detect malicious and selfish nodes, and they fixed themselves inside the network intelligently. Authors showed that previous detection techniques failed up to some extent in detecting these intelligent malicious nodes. Authors have designed an adaptive detection threshold technique, which motivates the attackers to act well, and finally, the designed technique catches the malicious behavior and hence was able to detect the malicious nodes immediately.

From their simulation results, authors concluded that their designed technique had best detection ratio more than 80% even in high ratio of attackers present inside the network. Also it handovers high data packets among nodes even when VANETs are dense.

In [24], the authors proposed a trust-based framework for communication in VANETs that is capable of accommodating traffic from different applications. Their scheme assigned a trust value to each road segment and one to each neighborhood, instead of each car. It scaled up easily and was completely distributed. Experimental results demonstrated that their framework outperformed other well-known routing protocols since it routed the messages via trusted vehicles.

In [25], authors showed that only authentication of nodes was not enough for secure data transmission in the VANET network, because sometimes even authentic nodes disseminated fake information and on/off attacks lead network application to threats of various attacks. To avoid such threats and attacks, authors proposed a technique called logistic trust mechanism, which has the ability to detect and identify malicious false messages and nodes. According to authors, to detect an attack, the first correct event should be identified as data depends on the events. The proposed scheme identifies the correct event first through information collected from trusted sources and also from the receiver observation itself. On the basis of this information, in logistic trust algorithm, the behavior of the nodes was identified through the receiver's own observation which was complemented by the opinions of other nodes. Authors proposed a scheme which had 99% accuracy in detection of malicious nodes and messages, which shows the efficacy of their proposed technique.

VANET security-oriented schemes are summarized in Table 2 given below with various parameters addressed in schemes, area of applications, techniques utilized, and deficiencies or research gaps present in these schemes.

3. Objectives of Research

In our research work, we proved our proposals with the assistance of a mathematical model and a flow chart. Our mathematical model and designed flow charts evidently validated our research. In our research work, we evaluate the performance of our design scheme VANSEC to trust [24] and logistic trust (LT) [25] schemes with respect to vehicle density using a MATLAB simulator to model all the driving environment and networking details of VANETs.

In the last phase of our research, we conducted a relative comparison. We compared our suggested VANSEC protocol with existing VANET algorithms, and comparative investigations are made and presented. The parameters we choose for our research work are TCE, EED, ALD, and NRO. In our presented scheme, the latency and TCE are dragged to minimal values and show enhanced efficacy with respect to other algorithms in terms of compared parameters.

The main objectives of our research work are as follows:

(i) To propose a protocol that can work efficiently, ensuring improvement in VANET security, and which should be scalable for the network in the future

(ii) Ensure data confidentiality, data integrity, and data availability for the clients in a VANET scenario

(iii) Propose an efficient technique to make the intruders' attempts thwart against data modification through data an insertion or deletion process

(iv) Adopting/applying different security mechanisms/ protocols through which the VANET system becomes much secure as well as provides better performance in terms of delay, higher PDR, small packet loss ratio, and efficient utilization of energy resources

4. Research Methodology

The process we implemented includes three vehicles and RSUs communicating with each other via IEEE 802.11p and IEEE 802.11 a/b/g. The scenario we put in our design is a hidden node for some other nodes moving towards each other. V3 and V1 are unaware of each other, because vehicle V3 is out of range to vehicle V1, that is, V1 and V3 are not in range of each other. Both vehicles are hidden from each other. Vehicle V2 is in range of V3 as well as of V1 via DSRC. However, there is also an RSU in access of all the vehicles.

In a narrow road scenario, V3 broadcasts an alert about its speed and position to inform nearby vehicles through DSRC and sends an alert towards the RSU. Vehicle V2 received the alert and propagated the alert to its nearby vehicles as shown in Figure 2.

On reception of alert by V1 from V2 and also from RSU, V1 goes for registration or authentication verification process, to make sure that the message was issued from an authentic source or from a malicious node. From Figure 2, there is communication among vehicles which is called ad hoc mode, while with the addition of an infrastructure it is switched into infrastructure mode. The VANET security model is confined and explained with the help of a flow chart shown in Figure 3.

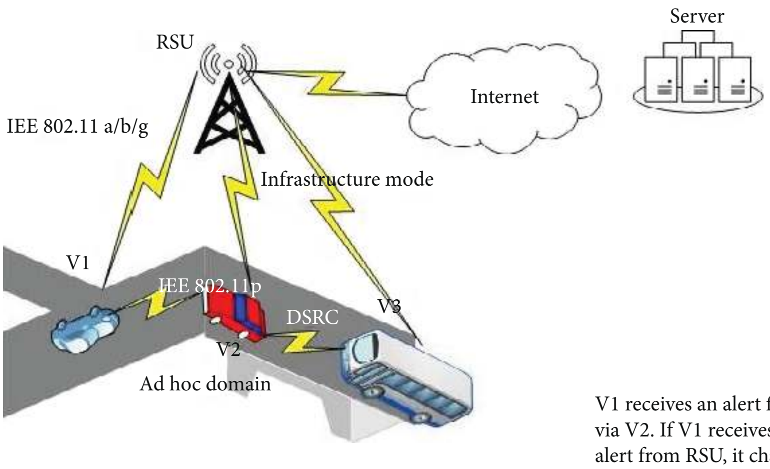
In the initialization process, vehicles and RSU register themselves to a registration server. The registration server verifies its authentication from a verification server to avoid penetration of malicious node and make the system secure at the primary level. There are three vehicles (V1, V2, and V3) and an RSU participating in the session; V1 receives a FSAM from V3 through V2. V1 inquired the same alert message FSAMs from RSU to confirm whether the received FSAM from V3 is correct. The decision-making block will check the similarity index. If the alert FSAMs received from both entities are the same, then it will inform the driver about the validity of node V3 also informing *ConVai* (confirm validity) message exchange about the validity of node V3 correctness, where *ConVai* exchange confirms the confidentiality of FSAMs to avoid snooping and traffic analysis. Integrity of FSAMs is checked to handle modification, masquerading, repudiation, and replay of attempts of false nodes. Also, it ensures on-time availability of FSAMs for requesting vehicles. After meeting the minimum acceptable threshold value of *ConVai* exchange, node 3 and other nodes meet the same criteria and are declared valid. These valid nodes are enlisted in the list of correct true nodes and allowed for communication or broadcasting FSAMs in the network.

If received FSAMs from RSU and V3 do not match and decision is blocked, then it is switched into another block for further verification about V3. This helps to look over node V3 position availability or unidentified position. If the position is identified, then FSAM is forwarded to the next block, to check FSAM confidentiality and for further investigation about FSAMs which is confirmed by *ConVai* exchange. After position validity and FSAM correctness, node V3 validity is endorsed and allowed for broadcasting FSAMs in the network. If node V3 position is invalid, then FSAM is discarded; again if the position of the node is valid but FSAM does not hold confidentiality check properly, FSAM is pumped into the discard bin.

Sensor nodes are also dispersed on highways which also gather data about events; Cluster Head (CH) forwards FSAMs towards *ConVai* exchange which are filtered here. If the received FSAMs from CH and RSUs are same notifying V3, then V3 and other nodes are assumed valid and are allowed for broadcasting. In case of any dissimilarity among the received FSAMs from different entities, they are pushed towards the discard bin which is shown in the flowchart diagram. All of these FSMs received from different sources alerts

Table 2: Summery of related work on VANET security.

Scheme	Technique	Area of applications	Parameters addressed	Deficiencies
Secure message delivery and authentication [15]	Aggregate message authentication code (MAC)	VANET security	Reduced communication overhead, improved authenticity	Packet loss End-to-end delay
Believe what you see, verify what you hear [16]	Detection and correction of error	VANET security	False position information detection, quick and fast data dissemination	Safety warnings, electronic toll collection, blind curve problem, etc.
Greedy detection for VANETs (GDVANs) [17]	Linear regression, mathematical concept, and fuzzy logic	VANET security	Prevention of DOS attack, no modification in IEEE 802.11p, greedy behavior detection	Duration between two successive transmission, transmission time, connection attempts made by node
Attack-resistant trust (ART) management [18]	Two separate metrics: data trust and node trust	VANET security	Ensure trustworthiness of data and node, cost effective in terms of comm. overhead	Misbehavior detection and trust management
GPS-based wireless hardware system [19]	Conversion of conventional vehicles into connected vehicles	VANET security	Limited speed threshold, effective in terms of safety, avoids accident	Cloud computing, advanced features needed to make the system smart and more realistic
AODV [20]	Routing protocol	VANET security	Sybil attack in VANETs	AODV with features of anti-Sybil attack
Various security threats and possible defensive mechanisms [21]	Threat investigation	VANET security	False info. dissemination, black hole attack, impersonation, man in the middle attacks, etc.	Security check when changing RSU by vehicles, secure private data like e-mail, IP address changed to pseudonym, etc.
Game theory model [22]	Reaction game mechanism	VANET security	DOS attack reaction problem	Costly and complex
Detection of intelligent malicious behavior [23]	Adaptive detection threshold	VANET security	High detection ratio, high packet delivery ratio, etc.	Investigates other adversaries, mobile certification authority
Trust [24]	Trust value assignment	VANET security	Routed the messages via trusted vehicles	Misbehavior detection and trust management
Logistic trust (LT) [25]	Authenticated node, correct event detection	VANET security	90% accurate with 2% error possibility in information	No specified attacks, that is, ballot stuffing and bad mouth attack.



V1 receives an alert from V3
via V2. If V1 receives the same
alert from RSU, it changes
its status according to the
alert received. Else
discard the alert.

Figure 2: Vehicle-to-vehicle communication.

are forwarded to *ConVai* exchange for judgment, to check whether these alerts satisfy the *ConVai* exchange minimum accepted threshold value.

If it holds, it enhances V3's trustiness. If the received FSAMs satisfies the *ConVai* exchange minimum acceptable threshold value, then the exchange notifies and informs the driver, neighbor RSU, and CH if anything about FSAM's validity ensures V3 trustiness and accuracy. However, if the *ConVai* exchange threshold value does not meet the required criteria (certain mathematical value), then it alerts all RSU, CH, and vehicular nodes participating in the current communication session that the given FSAMs broadcast by V3 are invalid.

The alert is also forwarded to drivers to make them sure about the malicious node penetration. All these node CH and vehicles held for next FSAMs alert the message, and fake formulated FSAMs are moved toward the discard block. This reduces the level of V3 trustiness and enables other nodes to be aware about the falsehood of received FSAMs from V3 and ensures to remember the bad experience for a long time. Moreover, vehicle V3 is forbidden to pump any alert in the network because the system declares it invalid and a fake node. However, if node V3 is declared a true one, the experience of validity is also remembered for long time and enhances V3 trustiness in the entire network. It is a brief description of our flowchart shown in Figure 3 which made our efforts of the VANSEC model for VANET security useful. In the future much, work is also possible in the area of VANET security in routing protocols and thwarting different attack launches by attackers for their own benefits.

4.1. Algorithm of VANSEC Communication Model. The algorithm below exhibits that input nodes will broadcast or issue an alert message received by output nodes and act according to the received alert messages if found authentically verified through *ConVai* exchange.

5. Mathematical Modelling of VANSec Protocol

As mentioned earlier, the VANET system is a threat from various attacks. Here, we will study them mathematically and understand how they work. In the VANSec security model on reception of any consequences from the source node, the destination nodes have different ways of confirmation about the validity of received FSAMs. Two verification techniques are listed below.

In the first technique, the receiver node checks the status of the sender/source node and verifies the status of the received FSAM's validity. Secondly, the receiver goes through a comparison phase where the receiver relates and compares the results collected from the source node and neighbor nodes of the source; if both have the same opinion about the received FSAMs, then the sender is considered a valid/true node. Our designed VANSec model comprises multiple events, so the occurrence of incorrect events should also be possible. The result reported from a source needs to be confirmed before exchanging information in the network. About the event accuracy, the VANSec model collects enough evidence to list the event valid/invalid and correct false information to avoid nodes from misguidance.

Our work provides a basis for all kinds of trust models, and we also used this idea in our proposed model. The accuracy of any occurred phenomenon is recorded and based on the observation of participating nodes (from event occurrence to the reported event). So a valid node forwards a valid event towards the receiving node, and with the passage of time, more nodes are also aware about the event to occur. However, the trustiness of the discussed technique may face failure when a valid node in the VANSec model furbishes invalid/fake information. To avoid fake information dissemination, a mass metric procedure (MMP) is used to confirm actual true or valid report and contradicting report. Mass is used to measure the weight of an object. For example, you are measuring the mass of your body when you step on to a

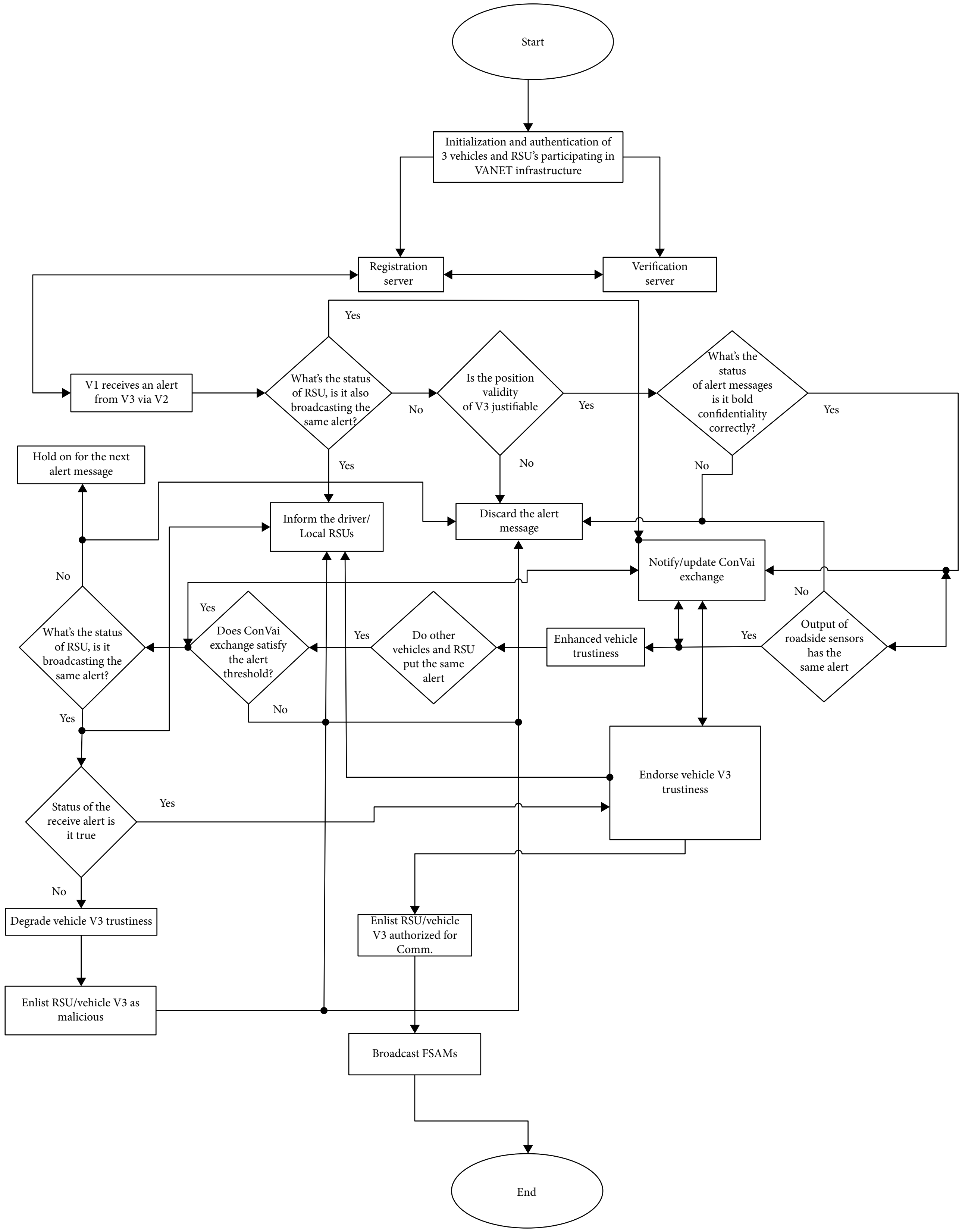

Start
Initialization and authentication of 3 vehicles and RSU's participating in VANET infrastructure
Registration server
Verification server
Yes
V1 receives an alert from V3 via V2
What's the status of RSU, is it also broadcasting the same alert?
No
Is the position validity of V3 justifiable
Yes
What's the status of alert messages is it bold confidentiality correctly?
Yes
Hold on for the next alert message
Yes
No
No
Inform the driver/ Local RSUs
Discard the alert message
Notify/update ConVai exchange
No
No
Yes
What's the status of RSU, is it broadcasting the same alert?
Does ConVai exchange satisfy the alert threshold?
Yes
Do other vehicles and RSU put the same alert
Enhanced vehicle trustiness
Yes
Output of roadside sensors has the same alert
No
Yes
Endorse vehicle V3 trustiness
Status of the receive alert is it true
Yes
No
Degrade vehicle V3 trustiness
Enlist RSU/vehicle V3 authorized for Comm.
Enlist RSU/vehicle V3 as malicious
Broadcast FSAMs
End

Figure 3: Flow chart of VANSEC security model.

```
Input: V1, V2, V3, RSUs.
Output: Only authorized node (vehicle/RSU) Broadcast information.
Nodes participating in communication session are {V1, V2, V3, and RSU}
V3 ← broadcasts an alert ← {V1 not in range while V2 and RSU receive the broadcast}
    V1 in range of V2 ← Receives broadcast from V2
    V1 ← receives an alert from RSU and Local sensors
        V1 compares ← Alert {V2, RSU and Sensors}
        V1← Verifies authenticity {V2, V3 and RSU}
    If vehicle/RSU not registered
    then
    Mismatch
Notify ← ConVai exchanged and verification Server {Discard the alert message}
Also Notify ← V3 Trustiness degraded {V3 are black listed}
   else
   Match ← Registered and Authentic {V3, V2, RSU}
Update ← ConVai exchange {Satisfied basic security goals}
Enlist ← Endorse V3/RSU trustiness
Allow ← V3 V2 and RSU
Broadcast ← Alert if any
   end if
```

Algorithm 1

scale. As we want to assign weights in affirming reports and contradicting reports, hence we have utilized this parameter. These weights are used to make a decision on relaying the messages if the equation is true. MMP is used in the decision-making process to allow the sender for communication or stop it. In (1), M_v is the valid mass metric whereas $M\neg_v$ represents contradiction.

$$\frac{M_v}{M_v + (M\neg_v)} < 1 - \xi. \tag{1}$$

The system took the source and event reporter's own confidence in the report received and then followed the received report for further action. Further, neighbor validity is also updated after looking over the results of the taken decision. If (1) becomes true, then the node is allowed for communication. However, this approach is unsafe in live safety applications, where dissemination of invalid activity may be disastrous. So, it is important to understand the nature of the reporter node well before making any decision. In trust-based approaches, the node-computed trust is a function of their own observations and opinion of neighbor nodes.

Our scheme VANSec is more immune and resistive against different kinds of attacks and thwarts malicious node penetration attempts to the entire network. It is basically based on trust management approach. The aim of the scheme is to identify malicious data and false nodes. In the designed scheme, at the beginning the node has information about the network behavior and nature. It investigates event accuracy from information received or from its own analysis. In the VANSec model, when a node undergoes unusual changes, it forwards these changes to surrounding nodes through a broadcast message and alerts nodes to switch into a safe mode. It is also possible that malicious nodes misguide other nodes through falsified FSAMs and drive the network for its benefits.

In the VANSec model, any node that receives FSAMs goes into a verification phase to understand the nature of information received before taking any decision. Therefore, a process is required to judge the correctness of received information, while the destination node holds a series of consequences achieved from received information and sender to verify the message's validity. Before any judgment about the accuracy of received information from the sender, a trust/confidence value for that sender's authenticity is established. The confidence value for the Sth sender at time interval n can be written as $C_S\ (n)$ where, for the message correctness about a consequence verification, the mass metric is used shown in (1), where $C_S\ (n)$ comes true if it follows (2).

$$0 \le Cs(n) \le 1. \tag{2}$$

The node has two containers: information containing a consequence is marked as P-container and is also represented by a binary digit 1, and a bin with no consequence is marked with NP-container in which also a binary digit 0 is lap to the NP-container. Average confidence values are computed from these containers utilizing sender confidence. Suppose P-container has S sender and NP-container has Q sender, the average confidence of each container at time interval n is given as

$$\begin{gathered} C_1(n) = \sum_{i=1}^{S} \frac{C_i}{S}, \\ C_o(n) = \sum_{J=1}^{Q} \frac{C_j}{Q}, \end{gathered} \tag{3}$$

where $C_1\ (n)$ is the average confidence of an event and $C_0\ (n)$ is the average confidence of no consequence. The normalized confidence of the node from each pot is called the mass metric of the given container which is shown in (4), where $m_i\ (n)$ is the mass metric of the ith node for bin 1 and $m_j\ (n)$ for the jth node for pot 0.

$$m_i(n) = \frac{c_i(n)}{C_1(n)},$$
$$m_j(n) = \frac{c_j(n)}{C_o(n)}. \tag{4}$$

When a node confirms a consequence in its previous report and later it cannot deny from its previously submitted report; similarly if the node denies a consequence, then one cannot confirm the same event; hence, masquerading is not allowed then. The mass metric confidence for each pot is computed to judge whether the consequence is true based on information received. The average mass metric confidence for these pots is given below:

$$C^1{}_{\text{avg}}(n) = \sum \frac{m_i(n) * c_i(n)}{S},$$
$$C^0{}_{\text{avg}}(n) = \sum \frac{m_j(n) * c_j(n)}{Q}. \tag{5}$$

In the decision-making process in VANSEC, the node utilizes the average mass metric confidence value to determine whether the consequence occurred or not. Hence, authentic source notifies an accurate consequence which does not threaten the decision. From (5), it is clear that $C^1{}_{\text{avg}}(n) - C^0{}_{\text{avg}}(n) > 0$ $Q > 0$, while $C^1{}_{\text{avg}}(n) > (n) >$ min ac cepted M_t when $Q = 0$ where $0 < C_{\text{avg}}(.) < 1$ and $0 <$ min ac cepted $M_t < 1$ which are the decision-making rules.

Any observation violating from the true consequence is considered malicious or eccentric; otherwise, it will be a genuine analysis. Our VANSEC model collects evaluator/judge and neighbor responses and also enlists misbehavior activity for a long time.

5.1. Evaluator/Judge Response. Evaluator/judge response is the response of a specific evaluator with a given sending source. Evaluator response is expressed in terms of eccentric ratio (ER), which evaluates whether the sender is malicious or honest. ER is defined as follows and is represented by Ω_n (s) where s is the sender/generator of packets in time interval n. $f_n\ (s)$ is the incorrect packet and $w_n\ (s)$ is the total number of packets generated by the source.

$$\text{ER} = \frac{\text{Modified or incorrect packets}}{\text{Total packets generated by source}} \Rightarrow \Omega_n(s) = \frac{f_n(s)}{W_n(s)}. \tag{6}$$

If the ER is analyzed and it crosses a particular threshold, say "Ψ," then a flag raises up indicating the source as a malicious entity and activity related to that node which is marked as untrue or false. If the ER value remains below the threshold "Ψ," then it fails in detection of malicious nodes. ER is also a decision-making ratio. To identify the node's true nature, an average ER is used.

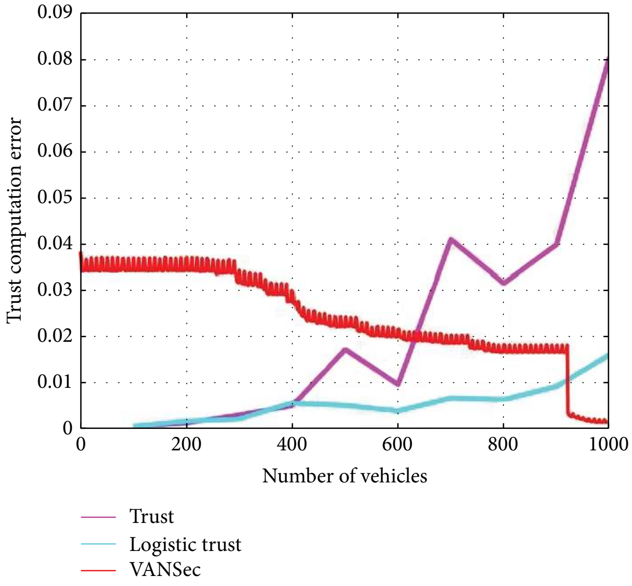


Figure 4: Trust computation error versus number of vehicles.

$$\overline{\Omega n(s)} = \frac{1}{n}\sum_{i=1}^{n}\frac{f_i(s)}{W_i(s)}. \tag{7}$$

Any node willing to establish a communication session with the source computes the ER first, so in the future the node easily broadcasts a list of trusted honest nodes and malicious nodes to its neighbor nodes. On reception of the list, the destination node updates its list of honest and malicious entries. Let us suppose that x is the node recognition entity, then λ_x is the number of malicious values received about x where H_x is the honest count. The receiving node establishes two parameters τ_x and π_x expressed with a relation given in (8). To estimate value for node x, these parameters are used.

$$\tau_x = H_x + 1, \pi_x = \lambda_x + 1. \tag{8}$$

The reputation tally for node x is

$$\text{Best tally}_X = \frac{\tau_x}{\tau_{x+\pi_x}}, \tag{9a}$$

$$\text{Worst tally}_X = \frac{\pi_x}{\tau_{x+\pi_x}}. \tag{9b}$$

From (9a) and (9b) Best Tally for x can be computed as

$$\text{Best tally}_X = 1 - \text{worst tally}_X. \tag{10}$$

5.2. Neighbor Response. Neighbor response is a response faced by neighbor nodes of a particular sender. It is an expectation obtained from neighbor nodes of a given sender in terms of binary values (0, 1). When the response of the neighbor node is binary digit 0, it means that the specific sender is malicious, while if it is one, then it points an honest node, where $Z_n(s)$ is the total number of received zeros and $O_n(s)$

Table 3: Trust computation error per 200 vehicles.

Protocol	200	400	600	800	1000	Average	% improvement
VANSec	0.03453	0.0280	0.0210	0.0166	0.00194	0.02041	4.463
Trust	0.001757	0.00719	0.0270	0.0718	0.0894	0.03942	7.30
L. trust	0.001757	0.00445	0.00546	0.00890	0.0119	0.0054	1.00

is the total number of received ones. Then, the neighbor response $N_n(s)$ is calculated as

$$N_n(s) = \frac{Z_n(s) + 1}{Z_n(s) + O_n(s) + 2}. \quad (11)$$

If there is no advice received about the sender and neighbor nodes, then the neighbor response $N_n(s)$ will assume a value of 0.5. Our proposed VANSec model uses characteristic confidence (CC) to filter out incorrect advices. CC uses the idea of resemblance and coherency or uniformity of advices for specific neighbors, where resemblance $R_n(L)$ is calculated between evaluator (J) and sender (L) of the data. Resemblance is calculated using the Jaccard similarity (JS) tally or score [26].

$$R_n(L) = \frac{1}{s}\sum_{g=1}^{s} \frac{A_L \cap A_{yg}}{A_L \cup A_{yg}} \quad (12)$$

Let A_L be the L sender's advice where evaluator J has its own analysis. Other advices from geographically closed nodes $y_1 \dots y_d$ are $\mathrm{A}_{y1} \dots \mathrm{A}_{yd}$ used to compare and calculate JS tally. In order to analyze the behavior of L, a time average of resemblance tally (score) is computed which is

$$\mathrm{Res}(n)[J, L] = \epsilon \ast R_n(L) + (1 - \epsilon) \ast R_{n-1}(L). \quad (13)$$

The CC in the VANSEC model also takes uniformity of advices for the current source. Suppose $I_n(L)$ is the advice value for sender L at time slot n, then $I_{n-1}(L)$ will be adviced at time $n-1$ for that sender. So the total value of advice or recommendation from L at time n will be $\|\mathrm{AL}\|$.

Hence, uniformity will be expressed through (14):

$$\beta_n(L) = \sum_{i}^{A_L} \frac{I_n(L) \oplus I_{n-1}(L)^{\circ}}{\|A_L\|}. \quad (14)$$

To establish characteristic confidence for the VANSEC model, the time average of uniformity/coherency is used which is calculated below:

$$\overline{\beta}_n(J, L) = \varphi \ast \beta_n(L) + (1 - \varphi)\beta_{n-1}(L). \quad (15)$$

Equation (15) shows average uniformity calculated among the evaluator (J) and source. Now combining both resemblance and uniformity to establish a CC for the VANSec model,

$$CC_n(J, L) = \theta_1 \ast R_{\mathrm{es}(n)}[J, L] - \theta_2 \ast \overline{\beta}_n(J, L) +_3 \ast R_{\mathrm{es}(n-1)}[J, L]. \quad (16)$$

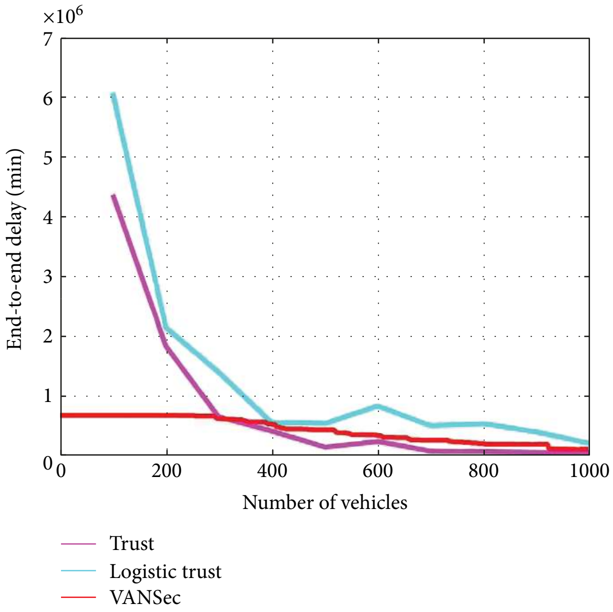


Figure 5: End-to-end delay (minutes) versus number of vehicles.

So from (16), we can easily calculate CC for a specific node and judge the nature of advice or recommendation reliability. In the VANSec model, if the value of CC falls below a particular threshold, say Υ, then the advice value for that specific node is filtered to be utilized in complete confidence trust estimation. After filtering out false untrue advices, the neighbor L and evaluator J responses along with the fanion (flag) $P_n(s)$ are collected in the VANSec model

$$t_n(J, L) = \frac{1}{1 + e^{L.\vec{C}.C_o}}, \quad (17)$$

where $L = [\Omega_n(s), C_S(n), P_n(s), t_{n-1}(J, S)]$, $\vec{c}$ is the mass metric associated with each of the abovementioned parameters, and C_o is the bias and is chosen on the basis of initial confidence trust of the nodes. If initial trust assigned to a node is 0.3, then C_o will be approximately −0.85. Once the value of $\vec{c}$ is found, then a new confidence value should be computed and updated using (17). If the new calculated confidence trust value falls below threshold Δ, then the node is considered malicious, and fanion $P_n(s)$ is raised; similarly, if the confidence/trust is above threshold Δ_L, then the node is marked as a true one and $P_n(s)$ goes down.

Table 4: End-to-end delay (minutes) per 200 vehicles.

Protocol	200 v	400 v	600 v	800 v	1000 v	Average	% improvement
VANSEC	0.67	0.55	0.39	0.29	0.17	0.414	1.00
Trust	2.8	0.31	0.09	0.031	0.031	0.6524	1.576
L. trust	2.34	0.75	0.52	0.473	0.274	0.8714	2.104

The performance rate will be identified in terms of valid optimistic rate (VOR), invalid optimistic rate (IOR), and consequence detection probability (CDP). VOR is the probability of identifying an invalid/false node as invalid or untrue, while IOR is the probability of pointing an honest node as a malicious node. CDP is the probability of identifying the true result.

VOR is mathematically shown in the following equation:

$$\mathrm{VOR} = \frac{P(\mathrm{I/I})}{P(\mathrm{I/I}) + P(\mathrm{H/I})}. \tag{18}$$

where $P(I/I)$ is the probability of identifying a node as an intruder such that the given node is also intruding or malicious, while $P(H/I)$ identifies an intruder or false malicious node as a true or valid node. Similarly, IOR can be calculated via using the following relation.

$$\mathrm{IOR} = \frac{P(I/H)}{P(\mathrm{H/H}) + P(\mathrm{I/H})}. \tag{19}$$

6. Simulation, Results, and Discussion

We compared our scheme to the present and tested schemes in terms of different performance metrics like TCE, EED, ALD, and NRO. To verify our VANSEC scheme to be efficient than the existing techniques, a comparison is done using simulation.

6.1. Trust Computation Error. Trust computation error (TCE) is the mean square error between the predicted/calculated and known/observed or actual trust value assessment of the vehicles. TCE can also be found through tracking the root mean square (RMS) of the calculated trust computed for all nodes. Figure 4 shows the execution of VANSec technique which is most favorable and has optimal performance than the trust scheme with logistic trust (LT). Keeping in view Table 3, VANSEC has consistency among the values of TCE with an increase of 200 vehicles in each step, while in case of trust and logistic trust techniques there is no such consistency among the values of TCE with 200 vehicles per step increase recorded.

Moreover, the TCE contributes to an interpretation that trust estimation in VANSec is more active, precise, and authentic, while in case of trust and logistic trust techniques, TCE values are not so active to properly handle altered data by misbehavior node data size, which may be a possibly malicious vehicle forwarding fake information to the destination vehicle. From Table 3, our proposed methodology of VANSec shows that our scheme is 11.6% and 7.3% more efficient in terms of TCE than the LT and trust schemes are, respectively, while the trust scheme is 4.3% more efficient in terms of TCE than LT. The enhancement in the performance of VANSec is due to the fact that our model calculates trust for all nodes randomly and identifies malicious node from their negative feedback. VANSec performed well in the presence of a huge number of false or malicious node concentrations. The reason for the good performance in a malicious environment is the feature of feedback metric credibility in the VANSec algorithm.

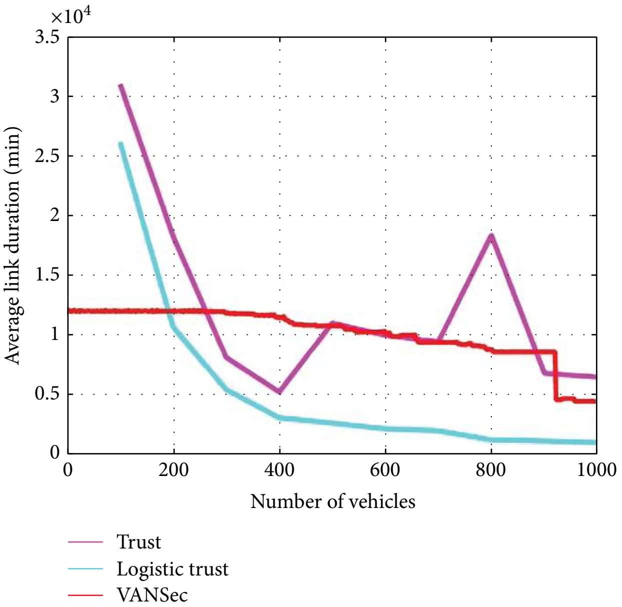


Figure 6: Average link duration (minutes) versus number of vehicles.

6.2. End-to-End Delay. The time taken by FSAMs to travel in a VANETs/VANSec model from the source vehicle to the destination vehicle is called end-to-end delay. Due to high mobility scenarios in VANSec, on-time delivery of FSAMs may be delayed. To prevent latency in packet delivery, delay-tolerant networks (DTNs) are favored to be used, in order to minimize end-to-end delay in VANETs. Figure 5 depicts that the performance of the VANSec algorithm is better than trust and logistic trust techniques. Figure 5 and Table 4 show close consistency along with an increase of 200 vehicles in each step. The table values for VANSec with the increase in number of vehicles also depict a consistent reduction in packet end-to-end latency.

Such coherent gradual reduction in end-to-end delay declares VANSec more logical than trust and logistic trust approaches. It is clearly depicted from the table that there is

Table 5: Average link duration (minutes) per 200 vehicles.

Protocol	200 v	400 v	600 v	800 v	1000 v	Average	% improvement
VANSEC	1.20	1.139	1.008	0.8775	0.4438	0.9337	2.594
Trust	1.06	0.3062	0.2139	0.1217	0.0978	0.3599	1.00
L. trust	1.824	0.5221	0.9957	1.833	0.6466	1.1642	3.234

no such consistency in the values of EED which are recorded with the increase in number of vehicles. From Table 4, it is concluded that average EED delay in the case of VANSec technique is approximately 0%. The trust and LT schemes face 57.6% and 5.2% longer delay, respectively, than the VANSec algorithm does, whereas the trust scheme has 52.4% more EED than the LT scheme does.

So, from these simulation results, the VANSec algorithm has enormous performance rather than trust and LT techniques. VANSec's outperformance than the rest of the two algorithms is due to the fact that our scheme considerably needed less information about the network behavior and route discovery process, which remarkably reduced the network overhead and suggested best for dynamic and ascendable networks.

6.3. Average Link Duration. Average link duration is the communication link lifespan estimation established among source and destination vehicles to exchange FSAMs. In VANETs, a path choice is an important parameter for good performance and better data rate. But in VANETs, link duration depends on various parameters like transmission range of the vehicle, intervehicle distance, vehicle density, and vehicle velocity which made link duration stability a challenging job. We used average link duration because link duration depends on the verity of parameters.

Figure 6 depicts our scheme VANSec to be more stable and reliable. Also, Table 5 reveals that our proposed scheme has stable link duration. For each step, there is a uniform increase in number of vehicles of 200 vehicles per step. From Table 5, we concluded that our designed VANSec technique provides 29.7% and 7.8% more reliable and stable ALD than trust and LT techniques, respectively. However, LT ALD is 21.9% more than the trust algorithm. So, an increase in the number of vehicle VANSec preserves link stability and very little gradual change noticed in the average link values. It means that ALD in the VANSec scheme is more reliable and stable.

However, the remaining schemes trust and LT undergo sudden change in ALD with increase in vehicle density and small consistency which are observed in ALD values. So comparison results show that our proposed VANSec scheme has better efficiency in terms of average like duration, and very little packets are lost. Such ambiguity in our VANSec protocol's better efficiency is that our algorithm chooses and prefers more stable and reliable routes/links among nodes for data transmission which has high link stability timing interval.

6.4. Normalizing Routing Overhead. Normalized routing overhead is a ratio of transmitted routing packets divided by the number of data packets delivered at the destination node. Figure 7 depicts an overhead returned by VANSec, trust, and logistic trust. Effects of overhead of these schemes are shown with the increase in vehicle density, respectively, depicted in Figure 7 and Table 6.

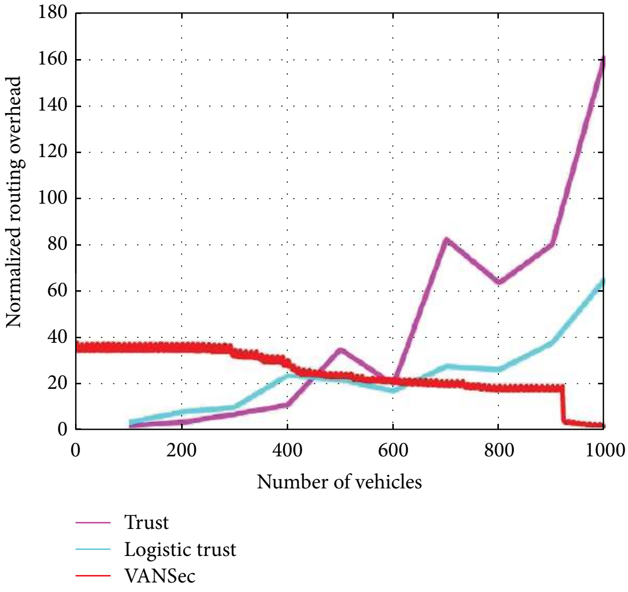


Figure 7: Normalized routing overhead versus vehicle density.

In Figure 7, the vehicle's density is adjusted at 1000 vehicles. We notice that our algorithm VANSEC has significant reduction in load with an increase in number of vehicles. In the VANSec scheme, overhead/load gradually reduces with the increase in vehicle density, while in other two algorithms, overhead enormously increases with increase in number of vehicles.

From Figure 7 and Table 6, it is concluded that overhead recorded in VANSec is nearly 0%, while trust and LT schemes in comparison with VANSec face 27.5% and 14% more NRO overhead, respectively; also, trust has 13.5% more load or NRO than LT does. So, in conclusion, VANSec is 27.5% and 14% more efficient than trust and LT protocols, respectively.

The particular improvement in our scheme is due to the fact that our designed scheme considerably reduces route request (RReq) query to conceive routes and choose the most stable and reliable route for transmission of data packets. This results in minimal route failure and considerably small number of control messages; that is, overhead is required to detect a route for information exchange. Table 6 shows a gradual reduction in NRO values with 200 increase in vehicle

Table 6: Normalized routing overhead per 200 vehicles.

Protocol	200 v	400 v	600 v	800 v	1000 v	Average	% improvement
VANSec	34.53	28.01	21.07	16.63	1.94	20.5	1.00
Trust	1.781	14.39	54.07	143.6	178.8	78.53	3.83
L. trust	7.028	17.8	21.85	35.61	47.7	26.1	1.28

density per step, while trust and LT procedures favor sudden change in NRO with 200 increase in vehicle density per step. From this analysis, our scheme outperforms the rest of the two schemes.

7. Conclusion

VANET is a subclass and an application of MANETs. Early VANET networks were a car-to-car (C2C) communication network basically designed for data exchange among vehicles. Later on, the feature of vehicles to roadside infrastructure were also added to the VANET network to make the system more efficient for data exchange to ensure safety of vehicles and humans and avoid unpleasant situations. VANET is a building key block of the ITS framework also known as intelligent transportation networks (ITNs). VANET is basically a design for the disseminations of cooperative awareness messages (CAMs) in the network for long distances among the vehicles and RSUs in range. For V2V communication, the IEEE 1609 WAVE protocol stack was designed on IEEE 802.11p WLAN standard utilizing a frequency band of 5.9 GHz for DSRC. Researchers proposed the verity of routing schemes aiming at enhancing the performance of vehicle information interchange among source and destination vehicles in the VANET system by taking into account various performance parameters. From comparison of different routing algorithms, we demonstrated that if a scheme is better in one response, it faces certain challenges in another response.

To avoid hazardous circumstances, FSAMs or any other emergency messages required priority based on time dissemination among vehicular nodes and roadside infrastructure and assurance of its flawless delivery at a receiving node is a most critical task. In case of such critical situation link failure occurs, the packets of FSAMs may face delay and once can face the worst tragic situation in sense of loss of precious lives and property.

In our research work, we have studied a variety of routing techniques including but one an analysis of designed technique VANSec, with already existing techniques trust and logistic trust in terms of different performance metrics like TCE, ALD, EED, and NRO with respect to an increase in vehicle density. VANSec is compared with trust and LT schemes because the modelling done in our scheme and the parameters considered closely match with the environment catered in those schemes along with the same parameters taken. In terms of performance metric TCE, VANSec is 11.6% and 7.3% efficient than LT and Trust are, respectively, while the trust scheme is 4.3% efficient than LT. From the EED comparison, we found VANSec to be 57.6% more efficient than trust and 5.2% than LT; also, trust schemes faced 52.4% more delay than LT did. Similarly, in terms of ALD, VANSec provides 29.7% and 7.8% more stable link duration than trust and LT did; however, LT is 21.9% more efficient ALD than trust. In terms of NRO, our proposed VANSec protocol has 27.5% and 14% lesser load than trust and LT, while trust has approximately 13% more NRO than LT. From these observations, we concluded that performance of our designed scheme in terms of these parameters is more valuable and authentic than the trust and LT algorithms. Our research shows that the VANSec scheme has better stability period, less latency, and improved data rate over trust and LT schemes.

Data Availability

No such data exists for our research; results are simulation based.

Disclosure

This work is an extension of our already published paper in conference "ARV2V: Attack Resistant Vehicle to Vehicle Algorithm for Trust Computation Error in VANETs."

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] D. Puccinelli and M. Haenggi, "Wireless sensor networks: applications and challenges of ubiquitous sensing," *IEEE Circuits and Systems Magazine*, vol. 5, no. 3, pp. 19–31, 2005.

[2] M. A. Matin and M. M. Islam, "Overview of wireless sensor network," in *Wireless Sensor Networks - Technology and Protocols*, IntechOpen, 2012.

[3] O. Altintas, F. Dressler, F. Hagenauer, M. Matsumoto, M. Sepulcre, and C. Sommery, "Making cars a main ICT resource in smart cities," in *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 582–587, Hong Kong, 2015, IEEE.

[4] D. Patel, M. Faisal, P. Batavia, S. Makhija, and M. Mani, "Overview of routing protocols in VANET," *International Journal of Computer Applications*, vol. 136, no. 9, pp. 4–7, 2016.

[5] V. Duduku, V. Ali Chekima, F. Wong, and J. A. Dargham, "A survey on routing protocols in vehicular ad hoc networks," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 12, 2015.

[6] M. J. Piran, G. Rama Murthy, G. Praveen Babu, and E. Ahvar, "Total GPS-free localization protocol for vehicular ad hoc and sensor networks (VASNET)," in *2011 Third International*

Conference on Computational Intelligence, Modelling & Simulation, pp. 388–393, Langkawi, Malaysia, 2011, IEEE.

[7] M. N. Rajkumar, M. Nithya, and P. HemaLatha, "Overview of VANETs with its features and security attacks," *International Research Journal of Engineering and Technology*, vol. 3, no. 1, 2016.

[8] A. Luckshetty, S. Dontal, S. Tangade, and S. S. Manvi, "A survey: comparative study of applications, attacks, security and privacy in VANETs," in *2016 International Conference on Communication and Signal Processing (ICCSP)*, pp. 1594–1598, Melmaruvathur, India, 2016, IEEE.

[9] R. Barskar and M. Chawla, "Vehicular ad hoc networks and its applications in diversified fields," *International Journal of Computer Applications*, vol. 123, no. 10, pp. 7–11, 2015.

[10] A. Jain and D. Sharma, "Approaches to reduce the impact of DOS and DDOS attacks in VANET," *International Journal of Computer Science*, vol. 4, no. 4, 2016.

[11] A. Suman and C. Kumar, "A behavioral study of Sybil attack on vehicular network," in *2016 3rd International Conference on Recent Advances in Information Technology (RAIT)*, pp. 56–60, Dhanbad, India, 2016, IEEE.

[12] R. Boon, *Post-Accident Analysis of Digital Sources for Traffic Accidents*, University of Twente, Enschede, Netherlands, 2014.

[13] S. Gupte and M. Younis, "Vehicular networking for intelligent and autonomous traffic management," in *2012 IEEE International Conference on Communications (ICC)*, pp. 5306–5310, Ottawa, ON, Canada, 2012, IEEE.

[14] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[15] H. Liu, Y. Chen, H. Tian, T. Wang, and Y. Cai, "A novel secure message delivery and authentication method for vehicular ad hoc networks," in *2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, pp. 135–139, Wuhan, China, 2016, IEEE.

[16] P. Wararkar and S. S. Dorle, "Transportation security through inter vehicular ad-hoc networks (VANETs) handovers using RF trans receiver," in *2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pp. 1–6, Bhopal, India, 2016, IEEE.

[17] M. N. Mejri and J. Ben-Othman, "GDVAN: a new greedy behavior attack detection algorithm for VANETs," *IEEE Transactions on Mobile Computing*, vol. 16, no. 3, pp. 759–771, 2017.

[18] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[19] Y. Agarwal, K. Jain, and O. Karabasoglu, "Turning conventional vehicles in secured areas into connected vehicles for safety applications," in *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, pp. 538–542, Chongqing, China, 2016, IEEE.

[20] Mujeeb Ur Rehman, Sheeraz Ahmed, Sarmad Ullah Khan, Shabana Begum, and Atif Ishtiaq, "ARV2V: Attack resistant vehicle to vehicle algorithm, performance in term of end-to-end delay and trust computation error in VANETs," in *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–6, Sukkur, Pakistan, 2018, IEEE.

[21] A. S. Al Hasan, M. Shohrab Hossain, and M. Atiquzzaman, "Security threats in vehicular ad hoc networks," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 404–411, Jaipur, India, 2016, IEEE.

[22] M. N. Mejri, N. Achir, and M. Hamdi, "A new security games based reaction algorithm against DOS attacks in VANETs," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 837–840, Las Vegas, NV, USA, 2016, IEEE.

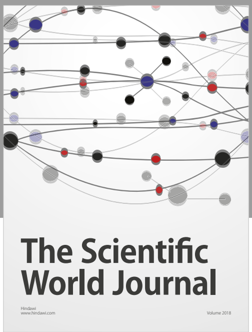
[23] C. A. Kerrache, A. Lakas, and N. Lagraa, "Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control," in *2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, pp. 1–4, Ras Al Khaimah, UAE, 2016, IEEE.

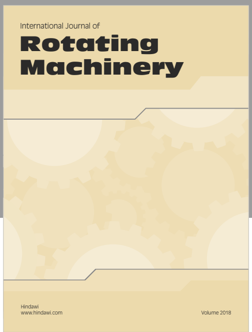
[24] K. Rostamzadeh, H. Nicanfar, S. Gopalakrishnan, and V. C. M. Leung, "A context-aware trust-based communication framework for VNets," in *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 3296–3301, Istanbul, Turkey, 2014.

[25] S. Ahmed and K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in *2016 IEEE Wireless Communications and Networking Conference*, pp. 1–6, Doha, Qatar, 2016, IEEE.

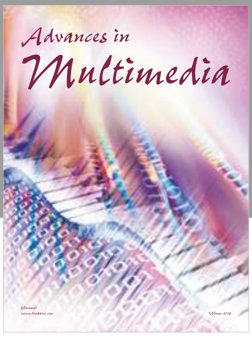
[26] S. Ahmed and K. Tepe, "Evaluating trust models for improved event learning in VANETs," in *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–4, Windsor, ON, Canada, 2017, IEEE.

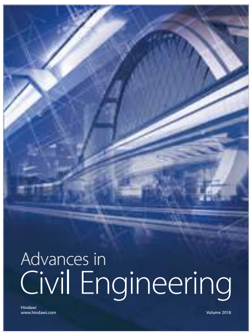
Journal of
Engineering

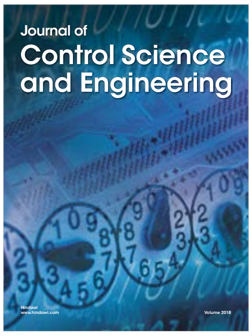

The Scientific
World Journal


International Journal of
Rotating
Machinery

Journal of
Sensors

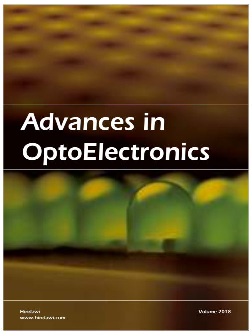

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

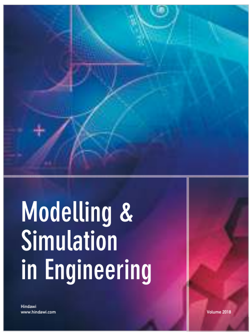
Journal of
Robotics

Journal of
Electrical and Computer
Engineering


Advances in
OptoElectronics

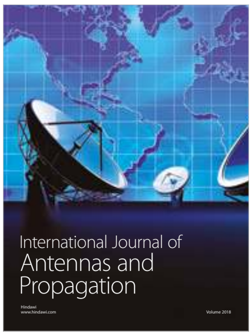
VLSI Design

International Journal of
Navigation and
Observation

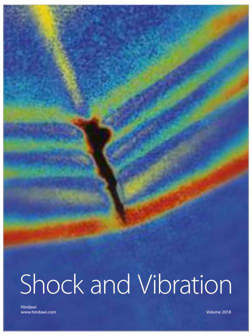

Modelling &
Simulation
in Engineering

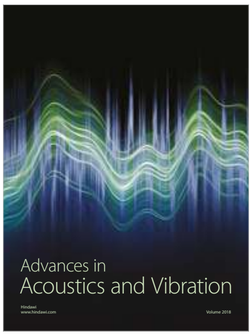
International Journal of
Aerospace
Engineering

International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration