Noname manuscript No.
(will be inserted by the editor)

Machine Learning-driven Optimization for Intrusion Detection in Smart Vehicular Networks

Ayoub Alsarhan* · Abdel-Rahman Al-Ghuwairi · Islam T. Almalkawi · Mohammad Alauthman · Ahmed Al-Dubai

Received: date / Accepted: date

Abstract An essential element in the smart city vision is providing safe and secure journeys via intelligent vehicles and smart roads. Vehicular ad hoc networks (VANETs) have played a significant role in enhancing road safety where vehicles can share road information conditions. However, VANETs share the same security concerns of legacy ad hoc networks. Unlike exiting works, we consider, in this paper, detection a common attack where nodes modify safety message or drop them. Unfortunately, detecting such a type of intrusion is a challenging problem since some packets may be lost or dropped in normal VANET due to congestion without malicious action. To mitigate these concerns, this paper presents a novel scheme for minimizing the invalidity ratio of VANET packets transmissions. In order to detect unusual traffic, the proposed scheme combines evidences from current as well as past behaviour to evaluate the trustworthiness of both data and nodes. A new intrusion detection scheme is accomplished through a four phases, namely, rule-based security filter, Dempster–Shafer adder, node's history database, and Bayesian learner. The suspicion level of each incoming data is determined based on the extent of

Ayoub Alsarhan (Corresponding Author)
Department of Computer Information System, Hashemite University, Jordan. E-mail: ayoubm@hu.edu.jo.

Abdel-Rahman Al-Ghuwairi
Department of Software Engineering, Hashemite University, Jordan. E-mail: ghuwairi@hu.edu.jo.

Islam T. Almalkawi
Department of Computer Engineering, Hashemite University, Jordan. E-mail: eslam.malkawi@hu.edu.jo.

Mohammad Alauthman
Department of Computer Science, Faculty of information technology, Zarqa University, Zarqa, Jordan. E-mail: malauthman@zu.edu.jo.

Ahmed Al-Dubai
School of Computing; Edinburgh Napier University, Edinburgh, UK. E-mail: A.Al-Dubai@napier.ac.uk.

its deviation from data reported from trustworthy nodes. Dempster–Shafer's theory is used to combine multiple evidences and Bayesian learner is adopted to classify each event in VANET into well-behaved or misbehaving event. The proposed solution is validated through extensive simulations. The results confirm that the fusion of different evidences has a significant positive impact on the performance of the security scheme compared to other counterparts.

Keyword: intrusion detection; smart city; malicious nodes; security; misbehavior detection.

1 Introduction

Recently, VANETs are adopted to significantly reduce traffic accidents, enhance road safety and traffic congestion, and to improve the driving experience. In order to increase drivers' awareness, smart vehicles cooperate to relay safety messages and road condition to other vehicles and roadside units (RSU) [23, 20, 5, 6, 12, 2]. However, VANETs have security concerns since information is transmitted via open space environment without any central support. In this environment, malicious node can join a network at any time and inject false messages wirelessly[12]. Unsecured nodes can expect to maliciously manipulating the stream of packets. For enhancing safety, malicious nodes should be prevented from changing safety messages. In VANET, source and destination nodes which are not in the same range relay on intermediate nodes for forwarding messages to the final destination. It would be an excellent opportunity to interpose on the traffic stream and manipulate it maliciously if a malicious node has been selected as a relay node. Therefore, the reliability of the VANET depends upon the intermediate nodes.

For safety application in VANET, timely and accurate information represents the backbone of information security. The accuracy factor represents the ability of VANET to deliver the state of road and traffic correctly and timely. Failure of safety message delivery could impose a human life threat. However, VANETs are prone to the risk of numerous security threats and attacks that make VANETs unable to deliver the services to users. These services include: providing access to spectrum for communication, providing access to VANETs's resources such as database, or reporting data to RSU. Hence, these attacks have several impacts on the performance and security of VANETs. For instance, the following are attacks that VANET may face [12]:

- Broadcast Tampering where attackers may send false safety messages. Injecting false safety message in VANET may cause an accident by following fake safety messages.
- Dropping some packets.
- Consuming VANET resources by sending a high volume of messages.
- The eavesdropper vehicle may modify, or reroute some packets.

Motivated by these observations, this paper proposes a new Intrusion Detection System (IDS) using Dempster–Shafer theory and Bayesian classifier

to prevent possible future security attacks in VANET. IDS is a cyber-security system used to detect malicious node and attacks in any network. For each event in VANET, our intrusion detection scheme collects evidences from multiple sources and fuse them to calculate the suspicion level of an event. Firstly, Dempster–Shafer theory is used to fuse uncertain information from multiple sources (i.e. evidences) to make an inference about the event. Dempster–Shafer theory is a mathematical theory proposed by Shafer in [22] to combine the evidences from multiple sources of information for reaching the final decision. The purpose of an aggregator operator is blending multiple sources of evidences meaningfully for summarizing and simplifying bulk data to detect intrusion. The final decision in Dempster–Shafer theory is hypothesis selected from a given set of hypothesis. In our work, the hypothesis set contains the class for a new event. Malicious activity is a subset of hypothesis set. Dempster-Shafer's framework assigns the belief for each hypothesis assigned based on the basic probability for each evidence.

In addition to Dempster-Shafer's framework, our security scheme uses intelligent learning system to incorporate prior knowledge and observed data on anomalous activity to classify each event into normal, or abnormal. Bayesian classifier possess several properties that enable it to detect intrusion accurately. The classifier assumes the probability of one evidence does not affect the probability of other. In presence of uncertainty of information, Bayesian classifier provides a formal and rational way of reasoning. Furthermore, optimal decisions can be extracted according to the quantities of interest. The classifier simulates human thinking and behavior because of its ability to reason and learn. Because of mathematical foundation of the classifier, it has been adopted in many areas of science and engineering including intrusion detection problem [8, 22, 4]. The classifier requires only one scan of training data to compute the required probabilities and it omits the tuple if it contains missing data. To the best of our knowledge, this is the first intrusion system that integrate information fusion and Bayesian learning. The main contributions of this work can be summarized as follows:

- Clustering mechanism is adapted where a cluster head (RSU) assures that communication is only achieved between trustworthy nodes.
- A four-phase intrusion detection scheme is proposed and evaluated. We consider incorporating rule-based filtering system, event-specific trust, and prior knowledge. A multi- source of evidence cyber-security system has two distinct advantages over other security schemes especially when used with a proper fusion algorithm:
  - A single source of information may provide faulty, erroneous results, and there is no way for accurate intrusion detection results. A multi-source of evidence system provides results with diverse accuracy. Faulty information can be easily detected with the help of a proper fusion algorithm and using multiple sources of evidence.

  - Multiple sources of evidence system receive information with wide variety and characteristics. Thus, it enables creating a more robust security system with less interference.
- The intrusion detection scheme is a hybrid-based monitoring solution that uses Dempster-Shafer's framework for combining the evidences from multiple sources of information and Bayesian classifier for events classification.Yet, researchers neglected exploring sufficiently well how to combine this information into one comprehensive security system for modeling intrusion detection in the domain of VANETs. The main concern of IDS is handling the imprecise, fuzzy, ambiguous, inconsistent, and even incomplete information about nodes. Dempster-Shafer's framework is adopted to manage uncertainty in VANET.

The rest of this article is organized as follows. First, related work and our contributions to the paper are introduced in Section 2. Next, VANET is presented in Section 3. We describe the proposed security scheme in Section 4. Then, we present some of the performed tests and show the performance of the VANET under different conditions with our scheme in Section 5. Finally, the article is concluded in Section 6.

2 BACKGROUND

Nowadays, there is a widespread of VANETs applications over the world. Enhancing road safety is one of the most important applications of VANETs. In a vehicular environment, the communication-based automotive applications span both the vehicular to vehicular communication (V2V) and vehicular to infrastructure (V2I) communication modes as illustrated in Fig.1 RSU transmits safety messages about road and traffic conditions to drivers. However, these messages are propagated in open space environments that make security issues is the biggest challenging concern. Furthermore, IDS are unable to detect newly attacks because of the tremendous growth in information over VANET. Our proposed IDS is a hybrid-based monitoring solution that uses Dempster-Shafer's framework for combining the evidences from multiple sources of information and Bayesian classifier to incorporate prior knowledge to detect intrusion.

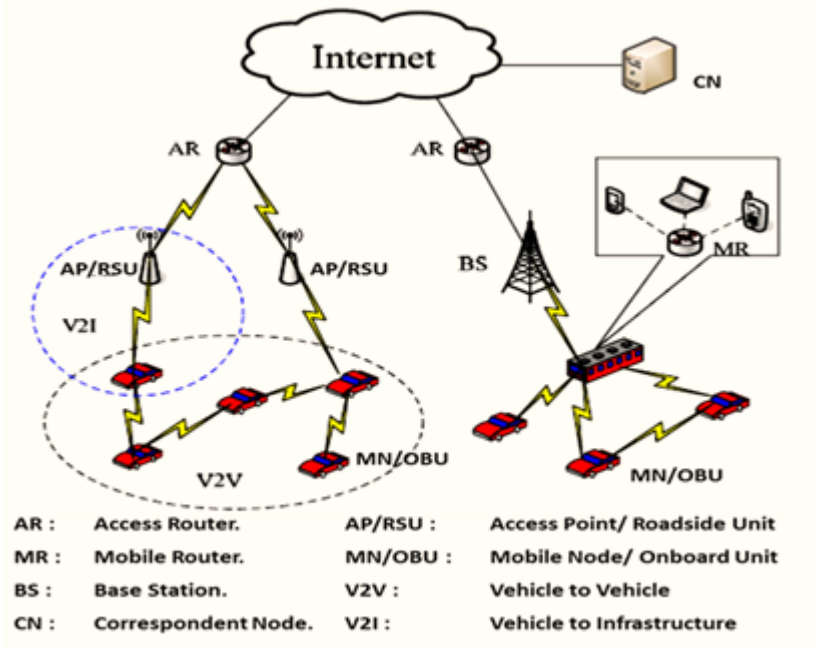

Fig. 1: Architecture of VANET

2.1 Background on DEMPSTER-SHAFER THEORY for Intrusion Detection

RSU in our scheme combines evidences from multiple sources to estimate the likelihood of an intrusion for each event in VANET. The Dempster-Shafer theory is well suited for this problem since it computes suspecting level by fusing conflicting multiple pieces of evidence. In this section we review the Dempster-Shafer theory in the context of intrusion detection. An efficient algorithm was presented in [34] to carry out belief calculation for a given hypothesis. In [18], new IDS proposed where certain node executes Dempster-Shafer for fusing multiple pieces of evidence. This node collects the information provided by the nodes in the network and makes the final decision for each event. In [14], authors proposed new scheme for securing safety messages in VANET. The main concern of the proposed scheme is maintaining the service between nodes by preventing DoS attacks in VANET. The scheme uses Kohonen's self-organizing map (SOM) [24] classifier for detecting misbehavior node. It analyzes the behavior of each vehicle. A feature map is generated by SOM to arrange similar classes. Dempster-Shafer theory was used to find attacker. Trace file was used as input for the classifier. Multimodal biometrics are integrated with IDS in [7] to overcome the shortcomings of unimodal biometric systems. Multimodal biometrics are widely used [15] for authentication where IDSs are modeled as sensors reporting the security state of the system. In

order to increase the accuracy of IDS, more than one device are selected to gather data. The collected date are fused using Dempster-Shafer theory. Security posture is used to decide whether or not authentication is required for each user. Furthermore, biosensors are selected using security posture. In [30], new trust model was proposed for securing communication in VANET. In order to verify road information, the model consider data trust instead of entity trust. It adopts Dempster-Shafer theory for increasing robustness and credibility of the model. Authors proposed new mechanism for detecting selfish and collusive behaviors in VANET. The mechanism uses Dempster-Shafer evidence to distinguish selfish nodes.

2.2 Machine learning based IDS for Network Intrusion Detection

Machine learning based IDS is proposed to handle various newly arising attacks. It has been used to extract new patterns of attacks from large databases. In [3], the authors proposed new IDS that adopted the Bayesian classifier to detect new intrusion. KDD dataset was used to compute the parameters for the classifier. The classifier was tested using a large subset of KDD dataset. The results stressed the ability of the classifier to detect new intrusions with a high accuracy rate. In [32], support vector machine (SVM) was used to detect false message attacks and message suppression messages. The proposed scheme consists of the data trust model and vehicle trust model. The data trust model adopts SVM to classify new messages based on its content and vehicle attributes. DST was used in the vehicle trust model to aggregate multiple trust assessment reports about the vehicle for extracting the final trust level for the node. The results showed that the accuracy of the proposed model is higher than the neural network model.

A Tow-layer filter was proposed in [33] to detect spurious messages. The coarse filter performs rapid filtration while fine filtration gives more accurate results. Each message pass through these filters for detecting a spurious message. Several sources of information were used to classify messages. These sources include: timelines of information, node reputation, and event location. In order to secure communication in VANET, a fuzzy trust model based on experience and plausibility was proposed in [26]. In the proposed model, a series of security checks are executed for intrusion detection. For each event, the location is checked by fog nodes. The results showed that the fuzzy model overcomes the uncertainty and imprecision of data. In order to detect false messages, a new framework was proposed in [19] to model the trustworthiness of nodes. The proposed model incorporates rules, experience, priority, and majority-based trust. The new algorithm was proposed to combine these sources of information. A new scheme for maintaining security and privacy was introduced in [27]. Besides securing data, the proposed scheme aggregates the collected data from vehicles and excludes the data of malicious node by obtaining a list of trustworthy nodes from trust authority. The efficiency of the proposed scheme was demonstrated by simulation.

A new attack on the VANET application was presented in [16]. The attacker broadcasts the scene aligned traffic safety message which may cause care accident, or traffic jams. The authors analyzed the reasons why traditional schemes fail to handle this attack. They proposed a new scheme to resolve this security threat. The new framework for verifying the truth or falsity of the safety message in VANET was proposed in [28]. In the proposed framework, the messages generated in response to another alert (primary alert) are used to compute the degree of belief for the primary alert. The authors proposed a Historical Feedback based Misbehavior Detection Algorithm (HFMDA) for detecting the misbehavior nodes in VANET [13]. In this algorithm, a vehicle sends an alert message to the RSU which checks the database to verify the truth or falsity of the message based on the past history of the node. Two parameters are stored in the history database: event notifications, and true event notification. One limitation of security schemes is that they are susceptible to tactical attacks such as self-promoting attacks and bad-mouthing attacks. In addition to tactical attacks, these schemes may violate location privacy since each vehicle is assumed to have a unique ID. To handle these drawbacks, the authors integrated trust management with the pseudonym technique in [29]. The reputation model was used to provide feedback on reputation. For false alarm detection, information entropy and the majority rule were applied to the reputation accumulation algorithm.

Recently, researchers began adopting deep learning methods for IDS. Deep learning has several architectures such as neural network models which include: Deep Belief Networks (DBN), convolutional neural networks, and recurrent neural networks [17]. In order to achieve highly accurate results in IDS, these architectures have been applied to IDS. In [17], Restricted Boltzmann Machine (RBM) and a deep belief network were used for IDS. In [1], the authors adopted a deep neural network (DNN) in the proposed scheme to detect new intrusion. Probability-based feature vectors are used to compute the required parameters for the model. Novel deep learning technique has been used in [11] for intrusion detection. The proposed classifier adopted non symmetric deep autoencoder for unsupervised feature learning. New IDS was proposed in [25] for securing communication in VANET against several attacks such as the denial of service, integrity target, and false alert generation. The detection scheme relies on a set of rules for classifying the behavior of a vehicle.Furthermore, the authors proposed a new protocol for computing the trust level for each vehicle. Statistical techniques were used to detect false messages in [31]. The proposed IDS takes into account key aspects. These aspects include: transmission intervals, and vehicle density. Besides using clustering for IDS, trusted third parties were adopted to enhance security. Several of IDS have adopted the opinions of other nodes to achieve high detection accuracy. The main challenge is integrating these opinions. The majority voting mechanism was adopted in [21]. Weighted voting was used in [10]. The weight of each vote is assigned based on the node's attributes such as location proximity, and reputation.

It is worth indicating that some of the presented methods neglected the evaluation of the trustworthiness of nodes' data for IDS, while few have been assessing the trustworthiness of nodes by analyzing the history of the nodes. It is well known that every node has a certain traffic pattern behavior, which establishes an activity profile for it (i.e. packet drop rate, and modification rate). None of the existing IDSs try to capture these behavioral patterns as rules and check for any violation in subsequent data transmissions. Fortunately, these rules are usually static in nature. However, they become useless for IDS when the node adopts new patterns of behavior that are not yet known to the IDS. Hence, to achieve the highest detection accuracy, IDS should learn the behavior of malicious nodes dynamically. IDS that fails to learn new patterns of malicious behavior becomes outdated and it generates a large number of false alarm. The malicious node can also attempt new types of attacks that should still get detected by IDS. Therefore, there is a need for developing IDSs which can integrate multiple evidences including patterns of genuine nodes as well as that of malicious nodes. In this article, to the best of our knowledge, a hybrid IDS for VANET that combines both machine learning and Dempster-Shafer theory is proposed.

More importantly, some of presented schemes consider the evaluation of the trustworthiness of the data shared among these nodes in VANET. In contrast, the proposed IDS detects malicious nodes based on reported data. RSU evicts these nodes form VANET after detecting them. Thus, multiple attacks can be avoided by focusing on nodes' data and node's behavior. In order to improve the accuracy of IDS, the suspicion level for each node is calculated considering the behavior of node. Moreover, the proposed IDS makes a decision more scientifically, dynamically, and adaptively where suspicion level for each node is calculated and changed with the number of communication transactions.

3 Network Overview

Each road is divided into segments (clusters). Each segment is managed by RSU. Each smart vehicle is equipped with a single IEEE 802.11b based transceiver. The spectrum is partitioned into non-overlapping channels (16 channels for each RSU with 5 MHZ spacing with transmission and power mask restrictions similar to the ISM band). In order to collect road status information (RSI), nodes in VANET (i.e., vehicles and RSUs) are equipped with different environmental sensors, processing, and wireless communication devices. Vehicles monitor road status information (i.e. the nearby vehicles) and report it to RSU. RSU processes data and then disseminates final road status to other vehicles and RSUs. Safety applications require timely and accurate RSI. j^{th} node is served by i^{th} RSU if:

$$S_{j,i} \geq H \tag{1}$$

where $S_{j,i}$ is the signal power received at i^{th} RSU from j^{th} node, and H is the threshold for signal power. Signal power is computed as follows:

$$S_{j,i} = S_0(\frac{d}{d_0})^{-n} \tag{2}$$

where d_0 is the close-in reference distance, n is the path loss exponent, and S_0 is the signal power at a distance d_0.

Algorithm 1: Road Information Management

Input:
N : total number of nodes in VANET.
Send_node_attrib(): method to send node's attributes.
Send_MaliciousNode_List(): method to send malicious nodes list for trustworthy nodes.
$\tilde{L}$:Link status vector.
Collect_road_data(): method for gathering link data.
SendData(): method to exchange link data.
Merge_Data(): method to merge results from vehicles.
Output:
F_S: Final link status.
N_c: set of trustworthy nodes.
N_m: set of malicious nodes.

```
for j=1,..,N do
    Read_node_attrib(j)
    if (IDS(j)! = malicious_node()) then
        N_c = N_c ∪ j
    end
    else
        N_m = N_m ∪ j
    end
end
Send_MaliciousNode_List()
for j=1,..,N_c do
    L̇= Gather_road_ data()
    SendData( L̇)
end
F_S = Merge_Data()
Send_final(F_S)
```

Let $N = \{n_1, n_2, ..., n_c\}$ be the set of nodes on which the trustworthiness of the nodes' data is performed. Let $P = \{P(n_1), P(n_(2)), \ldots, P(n_c)\}$ is the set of profiles for nodes, where $P(n_i)$ corresponds to the profile of i^{th} node. The profile of a node is a set of attributes containing information like node ID, event time and location, and time since the last event. Let $T^j_{k,\varphi}$ is the suspicion level for j^{th} event of node k, and φ is the time gap from the previous event. In VANET, RSU runs the proposed security scheme to detect malicious nodes. RSU excludes malicious nodes from the network by informing trustworthy nodes to discard any message from malicious nodes. We apply Algorithm 1 for road information management. For the clear exposition, the primary notations used throughout the problem description are summarized in Table 1.

Table 1: List of Relevant Notations

Notations	Description
K	number of segments for a road
$S_{j,i}$	the signal power received at i^{th} RSU from j^{th} node
H	threshold for signal power
S_0	signal power at distance[d]_0
d_0	close-in reference distance
n	Path loss exponent
P	set of profiles for nodes
$P(n_i)$	profile of i^{th} node
$T^j_{k,\varphi}$	suspicion level for j^{th} of node k, and φ is the time gap from the previous event
P_i	packets' modification rate
M_i	number of modified packets at i^{th} node
T_i	number of packets sent by i^{th} node
D_i	Packet drop rate
R_i	number of dropped packets at i^{th} node
C	set of clusters in VANET
A_t	set of attributes for each node
O_i	degree of outlierness for i^{th} node
ϵ	radius for the neighborhood of i^{th} node
MinPts	minimum number of points required in the e-neighborhood
$G_\epsilon(i)$	neighborhood of i^{th} node
$sim(i,j)$	similarity between i^{th} node and j^{th} node
Ω	set of mutually exclusive and exhaustive possibilities
$m_i(h_i)$	basic probability for hypotheses i
E_i	event i
B_j	occurrence of a transmission for j^{th} node
$P(E_i \mid h_2)$	probability of occurrence of event E_i given that it is generated by trustworthy node
W	number of well-behaved events
U	total number of tuples in the database
λ_W	arrival rate for well-behaved events
λ_m	arrival rate for misbehaving events
μ_W	mean parameter for well-behaved events
σ_W	standard deviation for well-behaved events
μ_M	mean parameter for misbehaving events
σ_W	standard deviation for misbehaving events
TP	misbehaving events that were correctly classified
FP	Well-behaved events classified as intrusion
TN	well behaved events that were classified correctly
FN	misbehaving events that were incorrectly classified as well behaved.
FP%	percentage of false alarms
FN %	ratio of well-behaved cases which is incorrectly classified as misbehaving
A	percentage of correct predictions of intrusions compared to all predictions Accuracy

4 Hybrid IDS for city-based smart highways

The proposed security system consists of generic as well as node-specific rules which detect incorrect information and identify data validity. The system measures the extent to which the node's behavior deviates from the normal profile of the node. Each node in VANET maintains knowledge of normal nodes' behavior in the network. This normal behavior can have rules like an average

data rate. The scheme assigns the initial suspicion level for each event. The initial suspicion levels are aggregated to obtain an overall suspicion level by applying Dempster–Shafer theory. Bayesian learning is used to strengthen or weaken the suspicion level based on the similarity of an event with bogus or genuine event history. Four different components are used in the proposed security scheme. These components include: security-risk filter, Dempster–Shafer adder, event history database, and Bayesian learner.

4.1 Security-risk filter (SRF)

Each event in VANET is analyzed using node-specific rules to measure the trustworthiness of the vehicle node. SFR is used to determine whether the observed event of node deviates from the normal profile. Several rules can be used in this layer of the security system. We briefly discuss two of the rules in this section.

4.1.1 Stranger nodes

Each node in VANET should register itself with RSU. The most basic check performed by RSU is checking whether the node is registered or not. The node is stranger if it is not registered with any RSU in VANET and it has never sent/received messages from any RSU. This check does not help us in identifying malicious nodes with complete certainty since a stranger node could show a good behavior. The suspicion level for a stranger node should be very high.

4.1.2 Outlier detection

Outlier is defined as rare event (i.e. dropping high percentage of packets) in VANET with extremely small probability of occurrence that could result in extreme measurements. For example, each node in VANET usually sends and receives similar number of packets. Since a malicious node is likely to deviate from the node's profile, its behavior can be detected as exceptions to the neighbors. In VANET, all events are stored in RSU's event list. The event list displays a list of events with a name, description, place, and start/end time. In order to specify the malicious node, RSU observes the modification and packet drop rate for each node. For i^{th} node, packets' modification rate P_i is computed as follows:

$$P_i = \frac{M_i}{T_i} \tag{3}$$

where M_i is the number of modified packets by i^{th} node, and T_i is the number of packets sent by i^{th} node. Packet drop rate D_i is computed as follows:

$$D_i = \frac{R_i}{T_i} \tag{4}$$

where R_i is the number of dropped packets at i^{th} node. RSU observes and records the abnormal nodes in its cluster. Furthermore, it keeps track of the total amount of incoming and outgoing packets for each node. Nodes are divided into clusters. Let $C = \{C_1, C_2, ..., C_c\}$ is the set of clusters in VANET and $A_t = \{a_1, a_2, \ldots, a_m\}$ is the set of attributes for each node that used to generate clusters.

For i^{th} node in VANET, the possible attributes are total amount of incoming and outgoing packets, modification packet drop rate, and packet drop rate. A behavior of i^{th} node is detected as an outlier if it does not belong to any cluster set. Such an observation gives evidence that the i^{th} node could be a malicious node.

In our work, DBSCAN (density-based spatial clustering of applications with noise) algorithm is used to filter out outliers and clustering. DBSCAN clusters together nodes that are similar to each other according to the same attributes (i.e. modification and packet drop rate). The behavior of a node is detected as an outlier if it lies alone in a low-density cluster. We measure the extent of deviation of node behavior by its degree of outlierness. The degree of outlierness for i^{th} node is computed as follows [22]:

$$o_i = \begin{cases} 1 - \frac{\epsilon}{A_i}, if\ |G_\epsilon(i))| < MinPts \\ 0, \qquad\quad otherwise \end{cases} \tag{5}$$

where ϵ is the radius for the neighborhood of i^{th} node, MinPts is the minimum number of points required in the e-neighborhood, and G_ϵ(i) is the neighborhood of i^{th} node which can be defined as follows [22]:

$$G_\epsilon(i) = \{j | sim(i,j) \leq \epsilon\} \tag{6}$$

where $sim(i,j)$ is the similarity between i^{th} node and j^{th} node. Similarity is computed as follows [22]:

$$sim(i,j) = \frac{M_{i,j}}{T_i} \tag{7}$$

where $M_{i,j}$ is the number of matched packets. DBSCAN algorithm requires that each object in a cluster C_i should have at least a minmum number of neighbors (MinPts). Hence, the density of each cluster should exceed some threshold. In our work, the values of the parameters MinPts and ϵ are determined using the heuristic that proposed in[21]. While large values of ϵ lead to less number of clusters, lower values generate more number of clusters. Also, the value of MinPts determines the number of clusters; higher values of MinPts lead to less number of clusters. If the value is set too high, some outlying nodes may not be identified. Furthermore, no cluster will be formed since the MinPts condition is not met for higher values. However, a lot of clusters will be created if both parameters are set too small. Each object in the system is treated as a separate cluster if the value of MinPts is set to 1. Furthermore, outlier behavior is identified as a separate cluster. Different attributes can be used for creating clusters. Usually, security scheme is subject to a large number

of events in VANET for authorization. However, most of these events being genuine in terms of security. Security filter is essential for separating out most of the easily recognizable genuine behaviors from the rest.

4.2 Evidences fusing using Dempster–Shafer adder (DSA)

For each activity of node, DSA computes an overall belief value by fusing all sources of evidence. For each node, the evidence is associated with multiple events for misbehavior detection scheme. In our work, DSA is used to combine evidence in security system. Dempster–Shafer theory (DST) is a general framework based on statistical interference for plausible reasoning. DST is a mathematical theory of evidence-based on belief functions and reasoning. It assumes a finite non-empty set Ω which is called the frame of discernment (FoD). FoD can be defined as follows:

$$\Omega = \{H_1, H_2, H_3, .., H_n\} \tag{8}$$

FoD Ω is a set of mutually exclusive and exhaustive possibilities when satisfying :

$$H_i \cap H_j = \phi, \forall i, j \in \{1, ..., n\} \tag{9}$$

For the misbehaving nodes detection problem, FoD Ω consists of three possible values for any suspected event which is given as:

$$\Omega = \{misbehaving, Well - behaved, suspicious(unknown)\} \tag{10}$$

For every behavior of i^{th} node in VANET, the rules contribute their independent evidence about the behavior of the node. DST fuses all evidence together using a numerical procedure. It computes an overall belief for the node's behavior. For any suspected event, the set Ω consists of two possible values, namely, misbehaving and well-behaved. Thus, the power set has three possible elements: hypothesis h_1= {misbehaving} implying that the node is misbehaving one, hypothesis h_2 ={well-behaved} implying that the node is trustworthy, and the universe hypothesis U implying that the event is suspicious. The evidence provided by n evidential sources are represented as basic probability assignments $m_1, m_2, \ldots, m_n$ over a common universe U which combined by means of DST to joint basic probability assignment denoted by $m_1(x) \oplus m_2(y) \oplus ... \oplus m_n(z)$. In our work, n basic probabilities $m_1(x), m_2(y), \ldots, m_n(z)$ are combined as follows:

$$m(h_1) = m_1(x) \oplus m_2(y) \oplus .... \oplus m_n(z) = \frac{\sum_{x \bigcap y \bigcap ... \bigcap z = h_1} m_1(x) * m_2(y) * .... * m_n(z)}{1 - \sum_{x \bigcap y \bigcap ... \bigcap z = \phi} m_1(x) * m_2(y) * .... * m_n(z)} \tag{11}$$

We assume that if the node is stranger then there is a high probability that it is an untrustworthy node and low probability that it is trustworthy. We consider the following basic probability assignments:

$$\begin{aligned} (h_1) &= \alpha \\ m_1(h_2) &= \beta \\ m_1(U) &= \gamma \end{aligned} \tag{12}$$

Clearly, if $m_1(h_1)$ is set too high, the likelihood that behavior of the node is classified as misbehaving will go up. However, high values of α may raise the number of false alarms significantly. Similarly, if β is set high, the number of suspicious events goes up, which increases the number of misses (misbehaving). For each detected event as an intrusion (i.e. outlier), the basic probability is assigned as follows:

$$\begin{aligned} m_2(h_1) &= 1 - \frac{\epsilon}{A_i} \\ m_2(h_2) &= 1 - (1 - \frac{\epsilon}{A_i}) \\ m_2(U) &= 0 \end{aligned} \tag{13}$$

For the intrusion hypothesis (i.e. h_1), the combination of the two evidences (i.e stranger, and outlier rules) can be expressed as follows:

$$P(h_1) = m_1(h_1) \oplus m_2(h_1) \tag{14}$$

Similarly, the genuine hypothesis for the new event can be expressed as follows:

$$P(h_2) = m_1(h_2) \oplus m_2(h_2) \tag{15}$$

All events in the system are registered in the repository component. History records of both well-behaved and misbehaving events are used to extract the profile for each node in VANET. This database is used to extract characteristics of the two classes. Each event is represented by a set of attributes containing information like vehicle ID, the total amount of incoming and outgoing packets, packet drop rate, ID's of the message, delay time of the message, speed, and location of sender and receiver. While observing the current behavior of a node (i.e. the number of dropped and modified packets), we also accumulate and analyze past behavior in terms of packet drop and modification rate for a node. The transmission data for a node in the database is required for detecting outliers. The expected behavior of the node is to breach any of the security principles. This can be achieved by modifying packets or drop some of them. However, to avoid detection, malicious nodes may drop or modify a large number of packets at longer time gaps or a small number of packets at shorter time gaps. Attackers may also carry out the attack at

longer time gaps. This would be difficult for a security scheme to detect the attack if the behavior of the attacker resembles the genuine node's profile in VANET.

To study the frequency of transmission of i^{th} node, we consider the time gap between successive transmission. The transmission gap is divided into n mutually exclusive and exhaustive events – $E_1, E_2, \ldots, E_n$.The occurrence of i^{th} event depends on the time since the last transmission. Let $T(E_i)$ represent the total amount of time that has elapsed since the occurrence of E_{i-1}.The occurrence of the event E_i can be represented as follows:

$$E_i = True \left\{ \exists (B_i \Lambda (T_{i-1} < T_{i-1} + T(E_i) \leq T_i) \right\} \tag{16}$$

where B_j is the occurrence of transmission of j^{th} node within $T_{i-1} + T(E_i)$ since the last transmission at T_{i-1}. The tuples in the history database are divided into two classes: misbehaving, and well-behaved class. The class of each event is defined as follows:

$$L(E_i) = \begin{Bmatrix} well-behaved, D_i < \rho, \, R_i < \omega \\ misbehaving, D_i \geq \rho, \quad R_i \geq \omega \end{Bmatrix} \tag{17}$$

Let $P(E_i \mid h_2)$ is the probability of occurrence of an event E_i given that a trustworthy node generates it. This probability is computed as follows:

$$P(E_i \mid h_2) = \frac{W}{V} \tag{18}$$

where W is the number of well-behaved events in the database and U is the total number of tuples in the database. The probability of occurrence of an event E_i given that the malicious node generates the event is computed as follows:

$$P(E_i \mid h_1) = \frac{M}{V} \tag{19}$$

where M is the number of misbehaving events in the database. Using Eqs. (18) and (19), the probability of occurrence of the event E_i is computed as follows:

$$P(E_i) = P(E_i \mid h_1)P(h_1) + P(E_i \mid h_2)P(h_2) \tag{20}$$

The initial belief m(h_1) of Eq. (11) is updated by using Bayes rule after adding new events to the history database.

4.3 Bayesian learner-based Intruder's Classification

Bayesian learning (BL) is a statistical tool that is used to update the probability for believe by using new evidences and information. Hence, the believe is updated whenever new information becomes available. In our work, belief revision using BL is expressed as follows:

$$P(h_1 \mid E_i) = \frac{P(E_i \mid h_1)P(h_1)}{P(E_i)} \tag{21}$$

By substituting Eq. (20) in Eq. (21) we get:

$$P(h_1 \mid E_i) = \frac{P(E_i \mid h_1)P(h_1))}{P(E_i \mid h_1)P(h_1) + P(E_i \mid h_2)P(h_2)} \tag{22}$$

BL updates the suspicion level (S_i) of the i^{th} node for each activity in the light of the new evidence E_i. S_i is the probability that the current behavior is misbehaving and the node is the untrustworthy. BL is used to find the most probable hypothesis for the event using the history database. This probability is known as a posteriori hypothesis $P_{max}(h_1)$ which can be computed as follows:

$$P_{max}(h_1) = \max_{h_1 \in \Omega} P(h_1 \mid E_i) \tag{23}$$

The posterior probability for each hypothesis in Ω is calculated using Bayesian rule and the hypothesis with the highest posterior probability is accepted. The malicious node detection problem has the following two hypotheses: $h_1 = misbehaving$, and $h_2 = well - behaved$. By substituting Eqs. (11), (18) and (19) in Eq. (21), the posterior probability for a hypothesis h_1 is computed as follows:

$$P(E_i \mid h_1) = \frac{P(E_i \mid h_1)P(h_1)}{P(E_i \mid h_1)P(h_1) + P(E_i \mid h_2)P(h_2)} \tag{24}$$

The posterior probability for hypothesis h_2 is computed as follows:

$$P(E_i \mid h_2) = \frac{P(E_i \mid h_2)P(h_2)}{P(E_i \mid h_2)P(h_2) + P(E_i \mid h_1)P(h_1)} \tag{25}$$

Future actions are decided by a security scheme based on the accepted hypothesis.

4.4 Securing VANETs Using Proposed IDS

The proposed scheme is presented in algorithm ??1. Firstly, it reads the event parameters such as event time, node ID, and number of packets as well as the design parameters such as ϵ, H, and MinPts. SRF handles each new event. The basic probability values from SRF are combined using DST to get the initial belief for each hypothesis. The event is considered to be an intrusion if $P(h_1) > P(h_2)$. The event is considered as genuine and is accepted if $P(h_1) < P(h_2)$. However, if $P(h_1) = P(h_2)$ the event is accepted and the node is treated as suspicious. If the node is stranger, then it inserted into the suspect node list.

The security scheme waits for the next event generated by each suspected node. SFR checks all the packets sent by the suspected node. It assigns initial

Algorithm 2: Intrusion Detection System

Input: MinPts, φ, N
Assign_probability- Strange-rule($m_1(h_1), m_1(h_2), m_1(U)$)
Assign_probability- Outlier-rule($m_2(h_1), m_2(h_2), m_2(U)$)
Compute $(P(h_1), P(h_2))$
if *(* $P(h_1) < P(h_2)$ **then**
  Accept(event)
end
else if *(* $P(h_1) > P(h_2)$*)* **then**
  Reject(event)
  if *(Not-Check_node_in_Black_List(Node_ID))* **then**
    Add_Suspect_table(Node_ID)
    Read_parmeters_Next_Event(E_i)
    $P(E_i \mid h_2) = \frac{W}{V}$
    $P(E_i \mid h_1) = \frac{M}{U}$
    $P(E_i \mid h_1) = \frac{(P(E_i|h_1)P(h_1))}{(P(E_i|h_1)P(h_1)+P(E_i|h_2)P(h_2))}$
    $P(E_i \mid h_2) = \frac{(P(E_i|h_2)P(h_2))}{(P(E_i|h_2)P(h_2)+P(E_i|h_1)P(h_1))}$
    if $(P(E_i \mid h_1) < P(E_i \mid h_2))$ **then**
      Accept(E_i)
      Delete_Node_Suspect_table(Node_ID)
    end
    else if $(P(E_i \mid h_1) > P(E_i \mid h_2))$ **then**
      Reject(E_i)
      Add_node_in_Black_List(Node_ID)
      Inform_nodes_Black_List()
    end
    else
      Wait_Event(Node_ID)
      Go to 12
    end
  end
end

belief to the event. If the event is found to be suspicious, it is inserted in the suspect table. Each event in VANET is time stamped. For i^{th} suspected node, SRF determines the event that has occurred outside E_i's set. Next, it computes$P(E_i \mid h_1)$, and $P(E_i \mid h_2)$ from the database. Then, the posterior beliefs $P(h_1 \mid E_i)$, $P(h_2 \mid E_i)$, $P_{max}(h_1)$, and $P_{max}(h_1)$ are computed.

$P(h_1 \mid E_i)$, and $P(h_2 \mid E_i)$ are the updated beliefs about the last event of the suspected node based on the evidence from the database. The value of $P(h_1)$ is taken as suspicion level in the first round. When the next event occurs, the new suspicious and posterior beliefs are computed based on parameters of the event. If $P(h_1 \mid E_i) \leq P(h_2 \mid E_i)$ then the SFR applies the DSA to combine evidences (i.e. $P(h_1)$, and $P(h_1 \mid E_i)$) for getting the final suspicion level.The current round $P(h_1)$ value is stored at the end of each round unless $P(h_1 \mid E_i) < P(h_2 \mid E_i)$. We apply Algorithm 2 for intrusion detection.

Whenever an event is classified as an intrusion, the corresponding node and the associated messages are discarded from VANET. RSU informs other nodes in VANET to discard all packets originated from these nodes.

5 Simulation and results

In this section, simulations are conducted to demonstrate the effectiveness and usefulness of the proposed security scheme by testing it with large scale data, where Table 2 lists the used simulation parameters. Due to the unavailability of real-life benchmark data set that contained the required features for testing (i.e. packet drop rate, and packets' modification rate), we developed a simulator to generate synthetic events that represent the behavior of trustworthy node as well as that of the malicious node.

The simulator was designed to handle various real-life scenarios that would be normally experienced in VANET. Firstly, any actual events database in VANET contains events of misbehavior nodes interspersed with genuine events. Secondly, genuine events are mostly similar to a set of nodes. Thirdly, the genuine events and events of malicious nodes are independent and they have separate arrival rates. These practical situations are modeled using a Markov Modulated Poisson Process (MMPP) and two Gaussian distribution functions. All events in VANET follow the Poisson arrival rate. The system has two states: a well-behaved state and a misbehaving state. Assume λ_W is the arrival rate for well-behaved events and λ_m is the arrival rate for the misbehaving state. Gaussian distribution is used to generate a number of dropped packets and modified packets for trustworthy nodes. By varying the values of mean (μ_W) parameter and the values of standard deviation (σ_W) different nodes' behaviors can be generated. For malicious nodes, Gaussian distribution is used to generate different behavior by changing the mean parameter (μ_M) and the standard deviation (σ_W) during the generation of misbehaving events.

Standard metrics are used to analyze the performance of the proposed security scheme under different system conditions. These metrics include:

- True positives (TP) are the misbehaving events that were correctly classified [9].
- False positives (FP) are the well-behaved events classified intrusion [9] (also called false alarms).
- True Negatives (TN) are the well-behaved events that were classified correctly [9].
- False Negatives (FN) are the misbehaving events that were incorrectly classified as well-behaved [9].

We examine the performance under different parameter settings.

5.1 Impact of threats on the performance of IDS

For comparison, we choose the IDS (BPNN) proposed in [33]. Since this system focuses on detecting spurious messages, it is the one closest to the proposed approach among all the methods presented in Section 2. Furthermore, we also study the improvement achieved by using Bayesian learning with Dempster's rule of combination.

Table 2: Simulation Parameters

Parameter	Value	
Number of nodes	200	
Number of channels per RSU	40	
Number of messages per node	Random	
Type of interface per node	802.11 b	
MAC layer	IEEE 802.11 b	
Transmission power	0.1 watt	
Packet size	512	
Max Vehicle Speed	80 km/h	
Number of malicious nodes	10,20,30,40, 50	
Simulation Device	Intel i5 Core	2.50GHz
	Process cores	2 x 2.50GHz
	RAM	6 GB
	OS	Windows 7 64 bit

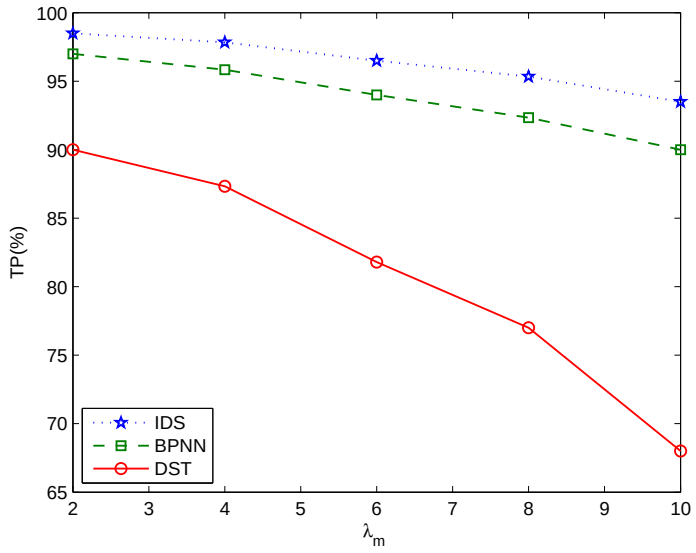

Fig. 2: True positive mean under different values of malicious node's arrival rates

In Fig. 2, we show the variation of mean TP under various values of arrival rates for malicious nodes (i.e., the number of abnormal events tuples in the database). IDS is the proposed approach in this work and DST denotes the use of DST only for intrusion detection. It is apparent from Fig. 2 that use of Bayesian learning improves the performance of our IDS by about 15–25% points in TP. IDS achieves the highest detection rate because it considers the node's behavior and trustworthiness of nodes' data.

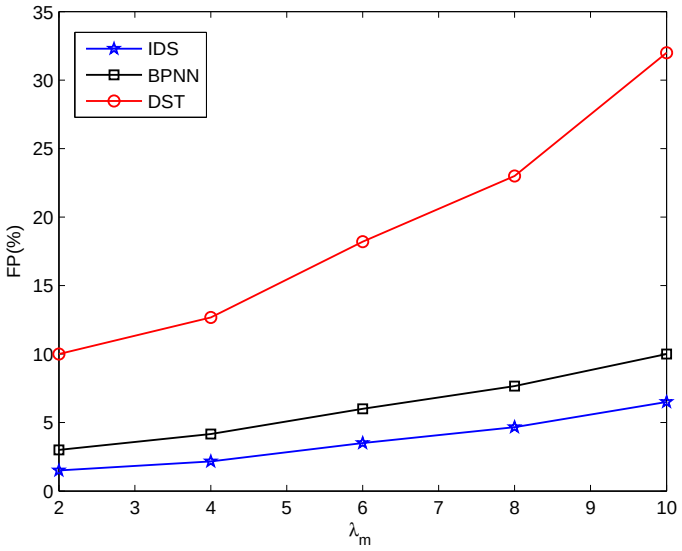

Fig. 3: False positive rate under different values of malicious node's arrival rates

FP% metric is used to measure the performance of IDS in terms of failure in detecting normal behaviors, in other words, the percentage of false alarm. FP% is computed as follows [9]:

$$FP\% = \frac{FP}{FP + FN + TP + TN} \tag{26}$$

IDS on the other hand, has lower FP than only DST based approach as shown in Figure 3. Use of BL, however, brings down the FP to values close to 2.5% since it uses more evidences, especially the trustworthiness of nodes' data. False Negative rate (FN) metric measures the ability of IDS to handle a genuine malicious node. It can be defined as the ratio of well-behaved cases such as a malicious node, which is incorrectly classified as misbehaving. FN% is computed as follows [9]:

$$FN\% = \frac{FN}{FP + FN + TP + TN} \tag{27}$$

Figure 4 presents a comparison of the IDS' FN against DST and BPNN. It is seen from Fig. 4 that the use of IDS brings down the FN to values close to 1%.

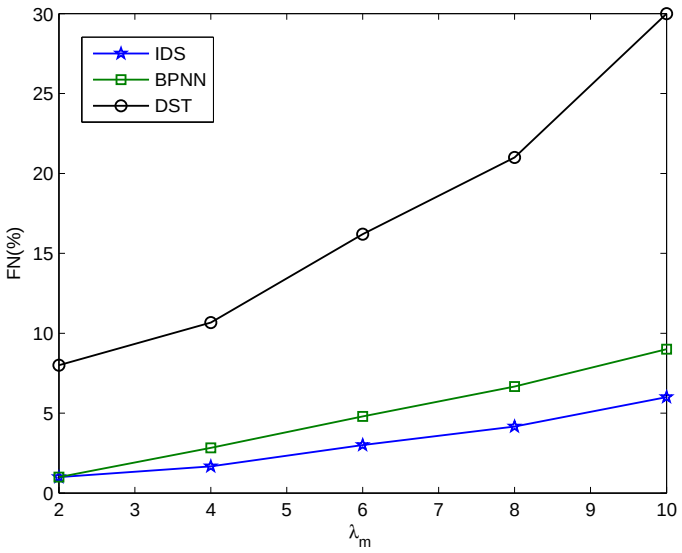

Fig. 4: False negative rate under different values of malicious node's arrival rates

Accuracy rate A refers to the percentage of correct predictions of intrusions compared to all predictions. The accuracy rate is computed as follows [9]:

$$A = \frac{TP + TN}{FP + FN + TP + TN} \tag{28}$$

Accuracy rate is the most important factor for evaluating the performance of IDS. We have compared the achieved rate of our IDS with other schemes in Figure 5. The proposed IDS accuracy rate outperforms the other models since it incorporates Dempster–Shafer theory and Bayesian learning within the same model, which is not the case in other models.

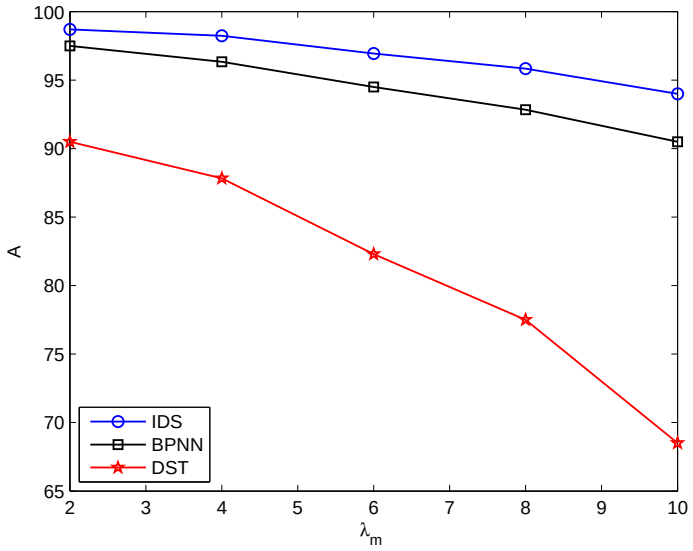

Fig. 5: Accuracy rate under different values of malicious node's arrival rates

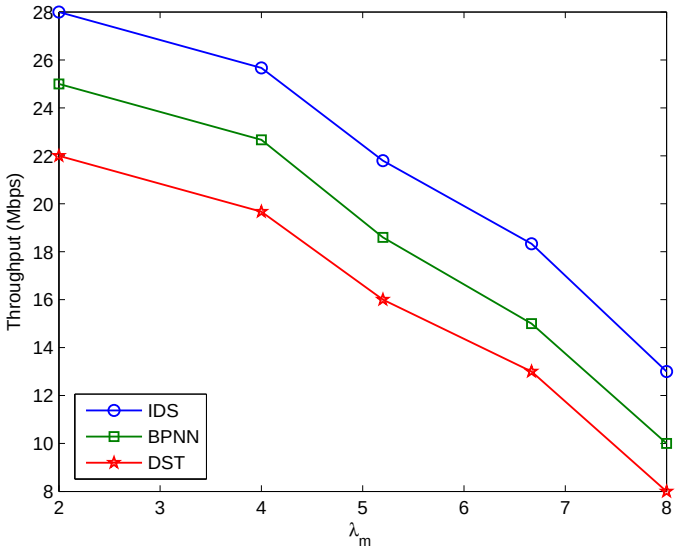

Fig. 6: Throughput under different values of malicious node's arrival rates

5.2 Impact of threats on VANET performance

To study the effect of threat on the performance of VANET, we measure throughput under various values of node's arrival rates. It is apparent from Figure 6 that the throughput shifts into the higher level when the number of malicious nodes decreases to the lowest possible number. The achieved IDS throughput outperforms the other models since it incorporates more evidence for intrusion detection. In our scheme, RSU excludes malicious nodes for the network. Malicious nodes may drop a large number of packets and keep sending false reports to other nodes. Hence, the number of dropped packets increases significantly, which lowers throughput. The packet drop ratio is plotted under various values of arrival rates of malicious nodes as shown in Figure 7. It can be observed that the drop ratio increases as the number of malicious nodes is increased. Our scheme excludes malicious nodes in VANET. Thus, the drop ratio is decreased when an attack is detected and attackers are prevented from forwarding packets.

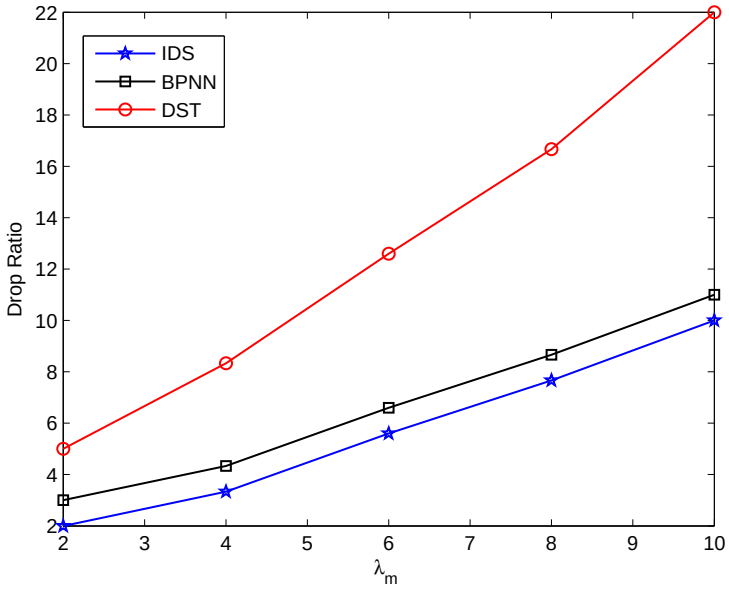

Fig. 7: Drop ratio under different values of malicious nodes arrival rates

6 Conclusion and future work

Although most of the cyber-security systems show good results in detecting attacks, they are struggling to avoid the modification of safety messages by malicious nodes in VANET. This assumes significance especially in the domain of attacks detection in VANET where a cyber-security system needs to

minimize the ratio of modified packets but, at the same time, does not wish the nodes to feel too much restricted in communication. We have proposed a novel intelligent security scheme based on the integration of three approaches, namely: rule-based-filtering system, event-specific trust, and prior knowledge. The main concern of the proposed hybrid IDS is preventing cyber-security attacks in VANET. A Dempster-Shafer theory is used to calculate the risk of attacks by combining multiple pieces of evidence, while BL is used to update the risk level of attacks using the history of database and attacks classification model. Comparative studies show the effectiveness of the proposed IDS through a set of experiments. While combining rules using Dempster–Shafer theory achieves high accuracy, BL shifts the accuracy to a higher level. Based on the simulation results, we conclude that the appropriate approach for addressing detecting intrusions in VANET where the patterns of behavior are complex is achieved by the fusion of multiple evidences and learning in IDS. In the near future, we plan to extend the proposed model to utilize big data collected from real systems. Furthermore, we wish to incorporate the Deep-learning algorithm within IDS for detecting new attacks. The proposed IDS can be further improved by combining more conflicting evidences.We wish to assess the performance of our security scheme on real time system using cyber threat questionnaire where we can analyze areas of potential or actual vulnerabilities. Furthermore, we plan to conduct interview to determine how the system performs.

References

1. Alrawashdeh, K., Purdy, C.: Toward an online anomaly intrusion detection system based on deep learning. In: 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 195–200. IEEE (2016)
2. Alsarhan, A., Al-Dubai, A.Y., Min, G., Zomaya, A.Y., Bsoul, M.: A new spectrum management scheme for road safety in smart cities. IEEE Transactions on Intelligent Transportation Systems **19**(11), 3496–3506 (2018)
3. Altwaijry, H.: Bayesian based intrusion detection system. In: IAENG Transactions on Engineering Technologies, pp. 29–44. Springer (2013)
4. Bahrololum, M., Salahi, E., Khaleghi, M.: Anomaly intrusion detection design using hybrid of unsupervised and supervised neural network. International Journal of Computer Networks & Communications (IJCNC) **1**(2), 26–33 (2009)
5. Bhoi, S.K., Khilar, P.M.: Vehicular communication: a survey. IET networks **3**(3), 204–217 (2013)
6. Bitam, S., Mellouk, A., Zeadally, S.: Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks. IEEE Wireless Communications **22**(1), 96–102 (2015)
7. Bu, S., Yu, F.R., Liu, X.P., Mason, P., Tang, H.: Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. IEEE transactions on vehicular technology **60**(3), 1025–1036 (2010)
8. Farid, D.M., Rahman, M.Z.: Attribute weighting with adaptive nbtree for reducing false positives in intrusion detection. arXiv preprint arXiv:1005.0919 (2010)
9. Han, J., Kamber, M., Pei, J.: Data mining concepts and techniques third edition. Morgan Kaufmann (2011)
10. Huang, Z., Ruj, S., Cavenaghi, M.A., Stojmenovic, M., Nayak, A.: A social network approach to trust management in vanets. Peer-to-Peer Networking and Applications **7**(3), 229–242 (2014)

11. Kang, M.J., Kang, J.W.: Intrusion detection system using deep neural network for in-vehicle network security. PloS one **11**(6) (2016)
12. Katar, C.: Combining multiple techniques for intrusion detection. Int J Comput Sci Network Security **6**(2B), 208–218 (2006)
13. Kumar, A., Singh, J.R., Singh, D., Dewang, R.K.: A historical feedback based misbehavior detection (hfmd) algorithm in vanet. In: 2016 2nd International Conference on Computational Intelligence and Networks (CINE), pp. 15–22. IEEE (2016)
14. Kushwah, N., Sonker, A.: Malicious node detection on vehicular ad-hoc network using dempster shafer theory for denial of services attack. In: 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), pp. 432–436. IEEE (2016)
15. Liu, J., Yu, F.R., Lung, C.H., Tang, H.: Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. IEEE transactions on wireless communications **8**(2), 806–815 (2009)
16. Lo, N.W., Tsai, H.C.: Illusion attack on vanet applications-a message plausibility problem. In: 2007 IEEE Globecom Workshops, pp. 1–8. IEEE (2007)
17. Ludwig, S.A.: Intrusion detection of multiple attack classes using a deep neural net ensemble. In: 2017 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1–7. IEEE (2017)
18. MacDermott, Á., Shi, Q., Kifayat, K.: Distributed attack prevention using dempster-shafer theory of evidence. In: International Conference on Intelligent Computing, pp. 203–212. Springer (2017)
19. Minhas, U.F., Zhang, J., Tran, T., Cohen, R.: A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) **41**(3), 407–420 (2010)
20. Narla, S.R.: The evolution of connected vehicle technology: From smart drivers to smart cars to self-driving cars. Ite Journal **83**(7), 22–26 (2013)
21. Sedjelmaci, H., Senouci, S.M., Abu-Rgheff, M.A.: An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet of things journal **1**(6), 570–577 (2014)
22. Shafer, G.: A mathematical theory of evidence, vol. 42. Princeton university press (1976)
23. Sharma, S., Kaul, A.: A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud. Vehicular Communications **12**, 138–164 (2018)
24. Shinji, M., Tsutomu, M.: Improvement of som visual stability by adjusting feature maps and sorting of leaning data. In: The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems, pp. 488–493. IEEE (2012)
25. Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q.: A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence **2**(1), 41–50 (2018)
26. Soleymani, S.A., Abdullah, A.H., Zareei, M., Anisi, M.H., Vargas-Rosales, C., Khan, M.K., Goudarzi, S.: A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. IEEE Access **5**, 15619–15629 (2017)
27. Sun, G., Sun, S., Sun, J., Yu, H., Du, X., Guizani, M.: Security and privacy preservation in fog-based crowd sensing on the internet of vehicles. Journal of Network and Computer Applications **134**, 89–99 (2019)
28. Vulimiri, A., Gupta, A., Roy, P., Muthaiah, S.N., Kherani, A.A.: Application of secondary information for misbehavior detection in vanets. In: International Conference on Research in Networking, pp. 385–396. Springer (2010)
29. Wang, J., Zhang, Y., Wang, Y., Gu, X.: Rprep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled vanets. International Journal of Distributed Sensor Networks **12**(3), 6138251 (2016)
30. Wu, Y., Meng, F., Wang, G., Yi, P.: A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks. In: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), pp. 1–7. IEEE (2015)

31. Zaidi, K., Milojevic, M.B., Rakocevic, V., Nallanathan, A., Rajarajan, M.: Host-based intrusion detection for vanets: a statistical approach to rogue node detection. IEEE transactions on vehicular technology **65**(8), 6703–6714 (2015)
32. Zhang, C., Chen, K., Zeng, X., Xue, X.: Misbehavior detection based on support vector machine and dempster-shafer theory of evidence in vanets. IEEE Access **6**, 59860–59870 (2018)
33. Zhang, J., Huang, L., Xu, H., Xiao, M., Guo, W.: An incremental bp neural network based spurious message filter for vanet. In: 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 360–367. IEEE (2012)
34. Zomlot, L., Sundaramurthy, S.C., Luo, K., Ou, X., Rajagopalan, S.R.: Prioritizing intrusion analysis using dempster-shafer theory. In: Proceedings of the 4th ACM workshop on Security and artificial intelligence, pp. 59–70 (2011)