ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(46), DOI: 10.17485/ijst/2016/v9i46/107112, December 2016*

Design of Misbehavior Detection Scheme by Combining Lane Change and Braking Alerts

Abdulhamid Aliyu Ardo[1,2]*, Anazida Zainal[1] and Fuad A. Ghaleb[1]

[1]Universiti Teknologi Malaysia. 81310, Johor Bahru, Malaysia;
abdulhamid.ardo@aun.edu.ng,
[2]Department of Computer Science, Federal University Dutse, Jigawa State, Nigeria

Abstract

Objective: To design and develop an enhanced Misbehaviour Detection Scheme (MDS) that addresses the problem of transmitting false information in Vehicular Ad hoc Network (VANET). **Methods/Analysis:** To achieve the purpose of this paper, data was collected through simulating a vehicle crash in different traffic scenarios. The data collected was then used to design a Misbehaviour Detection Scheme considering two inputs of Emergency Electronic Brake Light (EEBL) and Lane Change (LC). To confirm the veracity of transmitted Post-Crash Notification (PCN) alert, Bayes' rule was used to combine the two alert evidences. **Findings**: In each of the experiments conducted, the scenario belief values (probability of individual events) were calculated and Bayes' rule was used for combining the two evidences to obtain a better belief value. Simulation results show that increasing vehicle speed improves detection accuracy. Traffic scenarios having vehicles with low speed transmits fewer secondary alerts. Existing MDS uses single secondary alerts for verifying received PCN alerts. The proposed scheme combines evidences from more than one secondary alert to enhance the belief value of received PCN alert. **Applications/Improvements:** Combining multiple alert evidences shows that the proposed MDS makes significant enhancement to the existing scheme. Testing the proposed scheme with vehicles on high speeds shows 100% detection accuracy for transmitted PCN alerts.

Keywords: Braking Alerts, Lane Change, Misbehaviour Detection, Post-Crash Notification, VANET

1. Introduction

World report on road traffic injury prevention of 2014 identified road accidents and injuries as a major public health challenge that needs concerted efforts to be addressed. According to the World Health Organization (WHO) website, (WHO, 2014), an estimated 1.2 million people lost their lives and about 50 million are injured annually worldwide[1]. These figures are expected to increase by 65% in the next 20 years if nothing is done to prevent road accidents. Another report on Intelligent Transport Systems (ITS) showed that road congestion has caused the US an estimated $200 billion of fuel and 4.2 billion lost working hour's annually[2]. VANET can be defined as a class of Mobile Ad-hoc Network (MANET) which is used by vehicles in communicating with other vehicles or road infrastructure. The main goal of implementing a VANET is to ensure safety and comfort for road users. Thus, deployment of a Vehicle Ad hoc Network (VANET) has the ability of improving traffic efficiency and also preventing road accidents caused by vehicular congestions.

*Author for correspondence

Generally, Vehicle Ad-hoc networks (VANETs) are described as a wireless network having a group of vehicles communicating within a short range. The communication range is typically within 100 to 300 meters where vehicles exchange messages regarding their positions and also certain events[3]. There are many types of applications designed for VANET systems specifically to ensure safety and comfort of the users. Some of these applications include the Post-Crash Notification (PCN), Emergency Electronic Brake Light (EEBL), Road Hazard Condition Notification (RHCN), and Stopped/Slow Vehicle Advisor (SVA) among others. The PCN application is used in the case of the occurrence of an accident where vehicles send alert message to other vehicles notifying them of a crash that has already occurred. In the case of the EEBL, it is used to notify other vehicles of a sudden decelerating vehicle so as to prevent rear vehicles colliding. The RHCN informs other vehicles about the condition of the road while SVA conveys information about vehicles that are moving with very slow speed. Communication within the vehicular network is termed V2X communication i.e. meaning it can be between two vehicles (V2V) or between a vehicle and the road infrastructure (V2I). One special feature exhibited by VANETs is the high mobility of nodes which makes the communication range of the network to be short-lived since nodes enter and leave the network frequently. VANETs are concerned with real time communication, therefore handles life critical information. This brings a lot of challenges that hinder the creation of a communication channel that is safe as well as secured for the network users[3]. The vulnerable nature of VANET due to its peculiar features makes it an easy target since VANETs are susceptible to most type of passive and active attacks caused by malicious or malfunctioning vehicular nodes[4].

One major challenge identified in VANET is the security of transmitted information by communicating vehicular nodes[5]. It is important to detect misbehaving nodes in an effective manner because some vehicles may transmit false information which can lead drivers to take a false decision. Hence, it is necessary for vehicles to verify all messages received to confirm if corresponding events contained in an alert is true or false. VANETs refer to this verification process as Misbehavior Detection. False decision can also be caused by the selfish behaviour of drivers to free a lane just for its usage. Malfunctioning of road infrastructure such as the road side units is also another reason for false decisions. In VANET, the problem of inspecting transmitted information to detect false message is called data-centric misbehaviour. Data-centric misbehaviour considers the trustworthiness of transmitted information rather than considering the source of the information[6]. Node centric approach is also another technique used in detecting misbehaviour where misbehaving nodes are identified and sometimes penalized by a Certification Authority (CA). To identify malicious nodes, a system of distinguishing between the different communicating nodes is required. This is done through nodes authentication by a third party mostly a Public Key Infrastructure (PKI) that issues a private and public key to each node.

In order for information to be transmitted effectively, there is a need to secure transmitted information from attackers. Privacy and integrity of transmitted information are the basic security requirements of VANET. Others include authentication, confidentially and non-repudiation of the sender and receiver of information. Integrity means information can only be accessed or modified by those who are authorized such as authenticated vehicles, Road Side Units (RSU) and also the CA. Meanwhile authentication is when the receiver of a message checks how legitimate the message is and also verifies who the sender is. This is done to ensure that all transmitted messages are truly coming from legitimate sources. One common authentication problem is when attackers impersonate a vehicle such as an ambulance to surpass set speed limit without been detected and sanctioned. In[7] identified another serious problem of vehicular networks as the protection of drivers' sensitive information from malicious attackers called Privacy. A number of privacy problems are related to location-based services where for example, a node with malicious intent eavesdrops to gather information that will help it track other vehicles location. Finally, non-repudiation ensures the sender and receiver of a message can be tracked so that none of them will deny sending or receiving a particular message[7]. Non-repudiation seeks to identify both sender and receiver any given time.

In VANET, different types of attacks can be detected at the different layers of the network. For example, in the physical layer malicious attackers outside the network may launch a DoS attack to jam the network or deceive sensors to send false information. In the data link layer, vehicles can send bogus information by altering beaconing rate or launching channel capturing attack. At network level, a malicious node can spoof the identity of another node to receive specific information. Another serious threat is the presence of black hole attack in the network where an attacker claims to be in a better position to forward alert messages[8]. Also, at the application layer malicious vehicles may generate false messages such as when a vehicular node claims multiple identities which can be referred to as a Sybil attack. Thus, to have a secured network with good traffic safeties, VANETs require designing an effective and efficient Misbehaviour Detection Scheme (MDS) that will ensure proper protection against malicious nodes.

The rest of this paper is organized as follows. Section 2 provides a brief overview of related works. An overview of the proposed MDS and framework is presented in section 3. The simulation results in section 4 show the potential of the proposed MDS. Analysis and evaluation of the proposed MDS is discussed in section 5. Finally section 6 concludes the work with some future directions.

There has been a lot of research in the area of VANET privacy and security. The two broad categories of misbehavior detection schemes in the literature are: Node-centric misbehavior detection and data-centric misbehavior detection. In node-centric detection, communicating nodes needs to be distinguished through secure authentication so that only genuine authenticated nodes are allowed to participate in the network communication. To design a node-centric misbehavior scheme, some existing studies suggest the basing of trust with a third party mostly a PKI which issues credentials to communicating nodes[5,9]. In the data-centric scheme, the aim is to detect misbehavior in the messages transmitted by the nodes by comparing information received from other vehicles. This scheme is not very much concerned about the identities of the transmitting nodes but to link between the messages to reliably distinguish between them[10]. Thus, any vehicle sending false information such as a crash or false traffic congestion will be considered to be misbehaving.

In[11] did an investigation of Post-Crash Notification (PCN) scenarios which use the actual expected trajectories of a vehicle to decide if a vehicular node is transmitting a false alert or not. They used the node's possible behaviour as the expected trajectory of the vehicle. The model has a drawback of detecting misbehavior only after vehicles have reached the event location. This means a vehicle needs to be at the event location before detecting the misbehavior which is not sufficient for safety. Another model proposed by[12] created a reference model of vehicle's behavior and any alert message that does not conform to the model is termed misbehavior. It has a weakness of considering only primary information to verify received alert messages. Considering only primary information is not sufficient especially when a dense road scenario is used with different groups of vehicles to certainly verify received alerts. These two models discussed above have similar problem as vehicular nodes do not have a fixed behavior pattern. Drivers might act maliciously now and later send information that is correct and also useful to the network.

In the research work of[13] a MDS was designed by observing vehicle nodes behavior to detect nodes that drop received packets more than the set threshold value using an algorithm known as Detection of Malicious Vehicles (DMV). Nodes are classified into two lists; i.e. black and white lists in order to distinguish honest nodes from malicious vehicles. In[14] proposed an enhancement to the DMV algorithm in[13]. The enhanced MDS reduced the impact of black hole attack in VANET which makes the scheme more secured and also efficient. In[15] proposed a probabilistic misbehavior detection scheme which is based on secondary alerts. The secondary alerts are transmitted in response to PCN alert which is referred as the primary alerts in the model. The Secondary alerts were used to verify if received primary alerts are true or false. The highlighted drawback of this scheme is that it does not consider serious issues such as message loss and Sybil attack. Also, the alerts that other vehicles receive may not be the first of such since PCN alerts are periodic and therefore continue sending until the crash is cleared. The

more vehicular nodes transmit warning messages, the more the traffic congestion. Thus, this increases redundant rebroadcast of warning messages which leads to heavy and long-lasting traffic congestion and collision.

Another technique that uses the concept of Statistical models is proposed by[3] which improved Vulimiri's framework by reducing the approximation error of the MDS. The model defines a safe region known as the Fox Hole region whereby the safety value of a vehicle will be determined using its present location and also vehicles actual speed. The problem with this scheme is that it considers only static events like the happening of a crash on the road or some bad weather condition ahead. Another limitation is its collection of weightage data which takes too long. The delay experienced during weightage data collection might lead drivers to take false decision. This is because when the drivers act on a piece of information when the usefulness of that information has expired, there is a high probability that decisions taken will not be very effective. In the real world situation, waiting causes delay and if decisions are made immediately the chance is that some important messages to be used in voting might be lost[16]. Delay in VANET leads to various degrees of consequences ranging from false decision to traffic accidents and injury. In[17] proposed a model for adaptive decision making. The model uses the RSU for making quick and effective decision.

In[18] proposed a MDS which detects malicious nodes that transmits false information about vehicle speed and position. Vehicles receiving the alerts use information in the transmitted beacon message to determine if a node is honest or malicious. The scheme uses its current and previously received information for judging the nodes behavior. If the information does not match, then the suspicion index value is increased. When a vehicle suspicion index is greater than the set threshold value then the vehicle is considered as a malicious node. A highlighted advantage of the scheme is that it does not cause additional overhead to the communication channel. Another research work by[19] proposed a scheme that detects malicious vehicles that transmits false congestion information or non-exiting vehicular nodes. The scheme measures vehicle velocity and distance and uses radar to verify reported congestion events by vehicles.

2. Overview of the Research Framework

This research framework is divided into three sequential phases where each phase depends on the previous one. Phase-1 is focused on designing a crash scenario to collect data from the simulation of multiple vehicles behaviour during a crash. Phase-2 is aimed at developing Misbehaviour Detection Scheme (MDS) and phase-3 tests and validates the proposed MDS. These phases are depicted in the Figure 1.

2.1 The Proposed MDS Design

TThis section explains how the proposed MDS was designed. How the scheme works and also how it differs from other existing schemes. The major difference between the existing and the proposed schemes is the number of secondary alerts used for verifying transmitted PCN alerts. In the scheme[15] a vehicle receives PCN alerts and if the condition for transmitting SVA alert is satisfied based on vehicle speed, the SVA alerts are transmitted. Vehicle records the number of corresponding SVA alerts received after the receipt of a PCN alert earlier. The vehicle calculates the probability of SVA alerts given that a crash had already occurred. If the calculated belief value is less than the scenario threshold, then a false alert is detected else true alert is transmitted. For the proposed scheme, a vehicle first receives a PCN alert that a crashed had occurred. The numbers of corresponding EEBL and LC alerts were recorded for distances and time before, during and also after the crash. The probability for LC and EEBL events were calculated using the correlated behaviour of the two alerts. Probability for combining multiple evidence using Bayes' rule was used to calculate the degree of belief (β) for LC and EEBL given a crash has already occurred in both crash and no-crash scenarios. The belief value represents the detection accuracy for determining a true alert or misbehaviour. Equation (1) shows the prob-

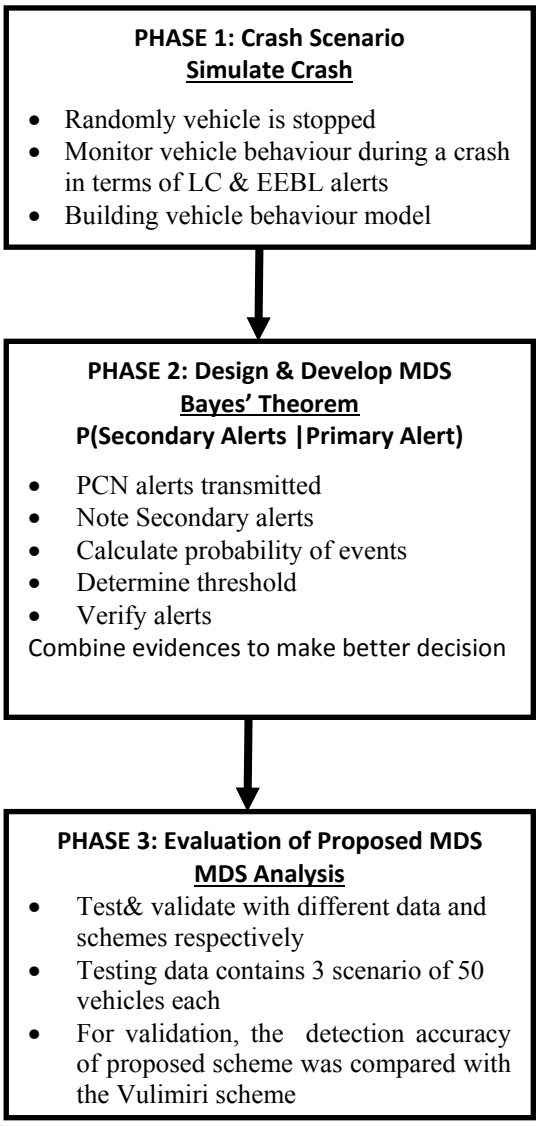

Figure 1. Research framework.

ability combining rule for correlating the two dependent events.

$$P(PCN \mid EEBL \cap LC) = (P(PCN) * P(EEBL \mid CRASH) * P(LC \mid CRASH)) / (P(PCN) * P(EEBL \mid CRASH) * P(LC \mid CRASH)) + P(NOCRASH) * P(EEBL \mid NOCRASH) * P(LC \mid NOCRASH) \quad (1)$$

The Bayes' rule combining evidence formula in Equation (1) calculates the probability of combining the individual probabilities of vehicles LC and EEBL. The numerator combines the evidence from the PCN alert (crash) with the braking and also the lane change. In the denominator, the already calculated probability in the numerator was added to the no crash probability of lane change and braking to obtain the total combined probability of the two events.

3. Simulation Results

This section shows the results of testing the proposed MDS using different sets of data as described in Table 1.

Table 1 shows different traffic scenarios simulated for testing the modelled scenarios. The first (3) scenarios had the same number of vehicles with progressively increasing speeds. The fourth scenario contained three groups of cars having different speeds and also politeness factor. The experiments conducted are as follows:

3.1 Experiment 1: Crash Scenario with 100 Vehicles (30-50km/hr)

This experiment shows how vehicles moving with low speed respond to PCN alerts. As observed, only few

Table 1. Scenario settings.

Scenarios Simulator settings	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Vehicles Count	100	100	100	150
Speed	30-50km/hr	40-60km/hr	60-100km/hr	30-50km/hr, 40-60km/hr, 60-100km/hr
Time slot value	10 sec	10 sec	10 sec	10 sec
Monitored distance	250 m	250 m	250 m	250 m
Politeness factor	1.0	0.7	0.3	1.0, 0.7 0.3
Road lane count	3 lane	3 lane	3 Lane	3 lane

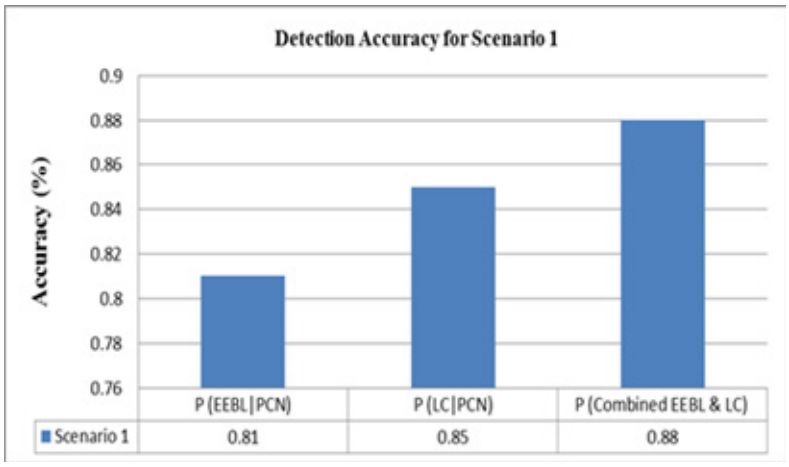

Figure 2. Scenario 1 detection accuracy.

EEBL alerts were transmitted from the simulated vehicle scenario. As compared with LC alerts, it was noticed to have a higher probability. In this experiment, the scenario belief values for each alert were calculated using Bayes' rule for determining the probability of individual events and combining the two evidences to obtain a better belief value. Figure 2 shows the detection analysis of EEBL and LC in scenario 1.

Figure 2, the alert with the lowest detection rate is the braking alert. This is expected as vehicles moving with slow speeds tend to transmit very few braking alerts. Considering the LC alerts gave a better detection rate for a crash as the detection rate was observed to have increased from 81% when considering braking to 85% when examining the LC behaviour of vehicles. Combining the two alerts gave a better detection accuracy rate of 88%. This clearly shows that combining multiple evidences improves the detection rate.

3.2 Experiment 2: Crash Scenario with 100 Vehicles (40-60km/hr)

The second experiment was modelled to show the behaviour of average speed moving vehicles in highway scenario. Figure 3 shows the response of 100 vehicular nodes to transmitted PCN alert. The Figure also shows that speed influences the behaviour of vehicles around the crash location. The increase in the belief values for all transmitted alerts was a direct response of increasing vehicles speed

3.2 Experiment 3: Crash Scenario with 100 Vehicles (60-100km/hr)

This experiment was conducted to show the behaviour of vehicles in high speed scenario. The detection accuracy of vehicles is further improved because vehicles moving

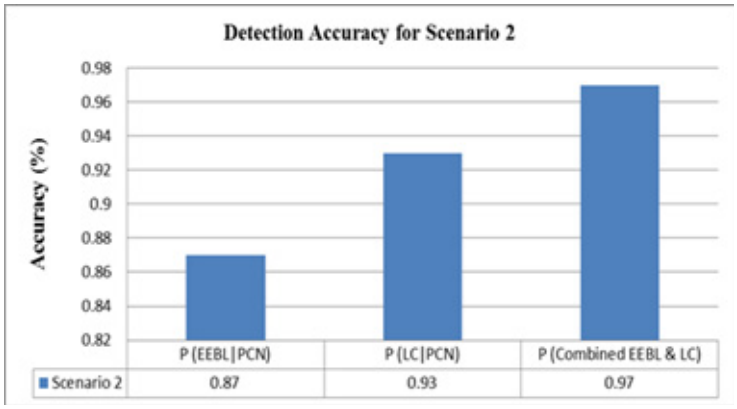

Figure 3. Scenario 2 detection accuracy.

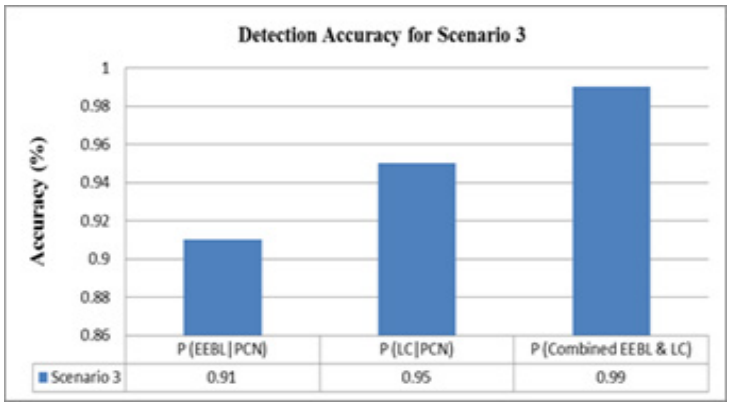

Figure 4. Scenario 3 detection accuracy.

with high speed transmit a large number of both LC and EEBL alerts around the crash location. On the contrary, vehicles having low speed tend to transmit lesser secondary alerts in response to received primary alert. The degree of belief (β) significantly increased in high speed scenarios. Figure 4 illustrates the behaviour of high speed vehicles during a crash event.

Figure 4 shows a huge increase in the belief values between the two alerts and the combined evidences of the two. It clearly illustrates that increasing vehicle speed increases the detection accuracy rate.

4. Analysis and Evaluation of Proposed MDS

This section shows how the number of false and true alarms was counted in order to determine the detection accuracy of the proposed MDS. Each of the three scenarios was simulated ten (10) times and the number of true and false PCN detected was recorded. Calculated combined probabilities of each of the (3) three scenarios simulated in experiments 1 to 3 was taken as the threshold for detecting false alarm. Any simulation run

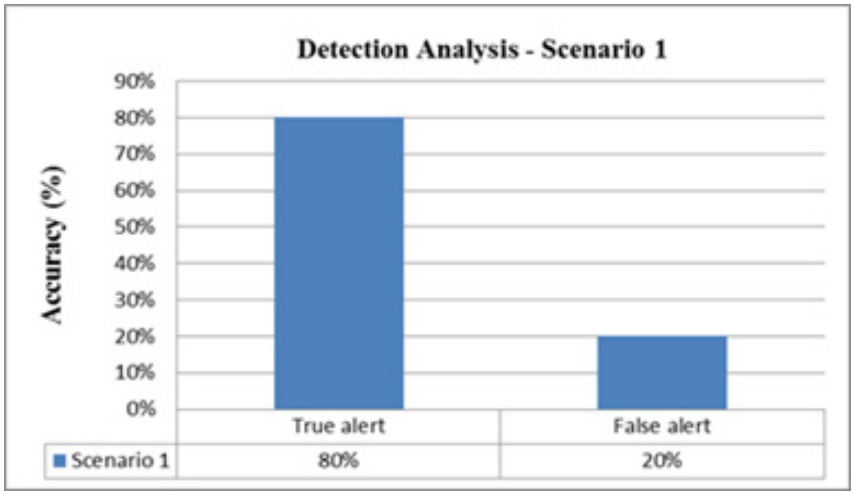

Figure 5. Detection analysis – scenario 1

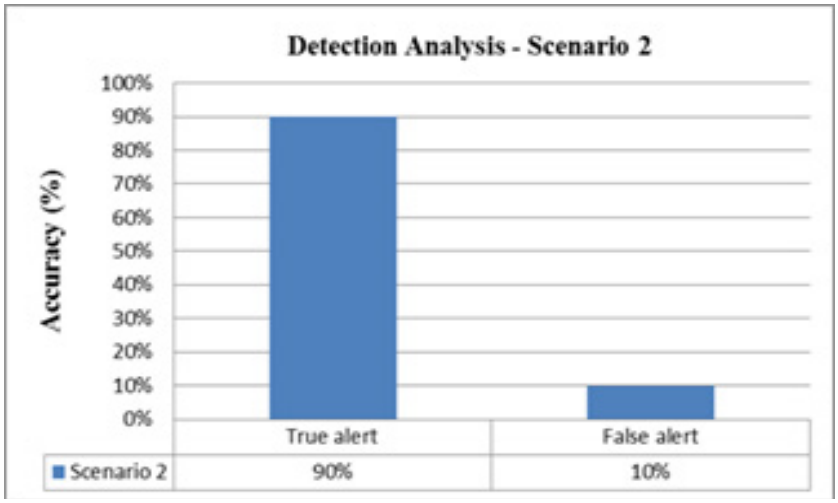

Figure 6. Detection analysis – scenario 2.

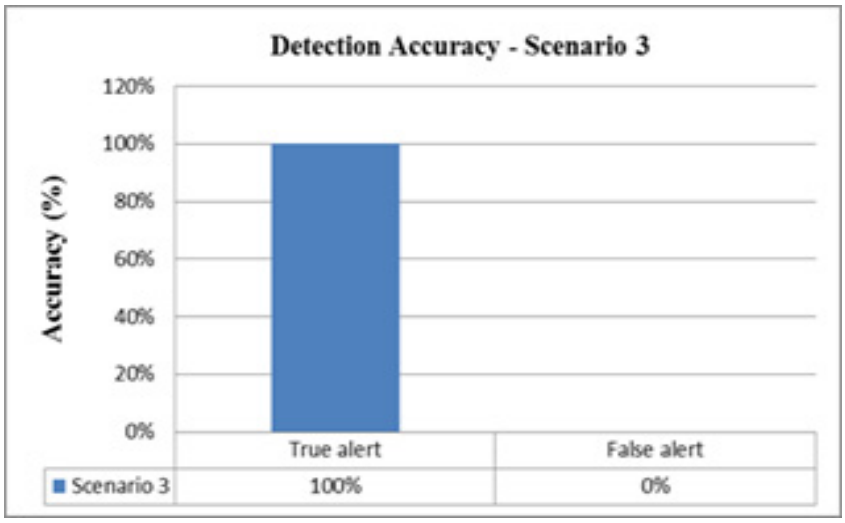

Figure 7. Detection analysis – scenario 3.

having a combined probability of alert events less than the scenario threshold is classified as a false alarm while a calculated combined probability greater or equal to scenario threshold was taken to be a true alarm. Figure 5 shows the probability of simulating ten (10) experimental

Figure 5 shows the result of simulating scenario 1 ten times. It can be seen that the proposed MDS was able to detect 8 runs correctly by having a calculated combined probability equal to experiment 1 threshold value of 88% for 6 runs and above the threshold in 2 simulation runs. The proposed MDS failed to detect PCN correctly in two simulation runs thereby having a calculated probability less than the scenario threshold. For validating the proposed MDS using scenario 2 calculated probabilities, Figure 6 shows the results of simulating the scenario ten times as done for scenario 1.

In Figure 6, the proposed MDS was able to detect all false PCN except one in the 5th simulation run. These results explain the relationship of detection rate with vehicle speed. It was observed that increasing the vehicle speed provided a better accuracy for verifying received PCN alerts. In all the simulated runs, calculated probability confirms the presence of a crash event.

Next, this paper estimated the probability of secondary alerts in detecting the accuracy of alerts in scenario 3. Figure 7 shows that all transmitted PCN alerts were correctly verified with 100% accuracy. None of the ten simulated scenarios had a belief value less than the scenario threshold. Therefore, it can be concluded that progressive behaviour of vehicles to increase speed on highway scenario gives a good result for verifying PCN alerts for detecting misbehaviour. Thus, it is important to estimate probability of events from traffic models having high vehicles speed.

As stated earlier, scenario 3 detects all transmitted PCN alerts correctly. Therefore, it represents the best scenario among the simulated traffic models with 100% detection accuracy.

4.1 Proposed MDS Feature Analysis

The most important requirement considered in the proposed MDS is the safety of the scheme. The scheme has the ability to monitor the lane change and braking behaviour of slow and also fast moving vehicles on a highway scenario. The numbers of secondary alert messages trans-

mitted were used to verify the truth or falsity of received PCN alerts.

4.2 Detection Accuracy

The number of lane change and braking alerts provides useful information for verifying the correctness of received PCN alerts. Detection is accurate as long as the numbers of transmitted secondary alerts are large enough to convince a driver that the reported event has actually occurred.

The proposed enhanced MDS work by continuously recording the number of LC and EEBL transmitted by vehicles at the crash region. The number of transmitted LC and EEBL of vehicles around the crash location was much higher than that of vehicles in other road segments. Vehicles with very high speed around the crash region transmits large secondary alerts which gives a better belief value, while vehicles on low or average speed needs to transmits more alerts to convince road users about the correctness of PCN alert.

4.3 Comparison of Proposed MDS with Existing Scheme

The proposed MDS was compared with the Vulimiri scheme based on the calculated belief values. Vehicles need to be properly informed about the road condition ahead so as to make quick decision. In doing so, vehi-

Table 2. Belief values.

Scenarios	Vulimiri Scheme	Proposed Scheme
Scenario 1	0.81	0.88
Scenario 2	0.87	0.97
Scenario 3	0.91	0.99

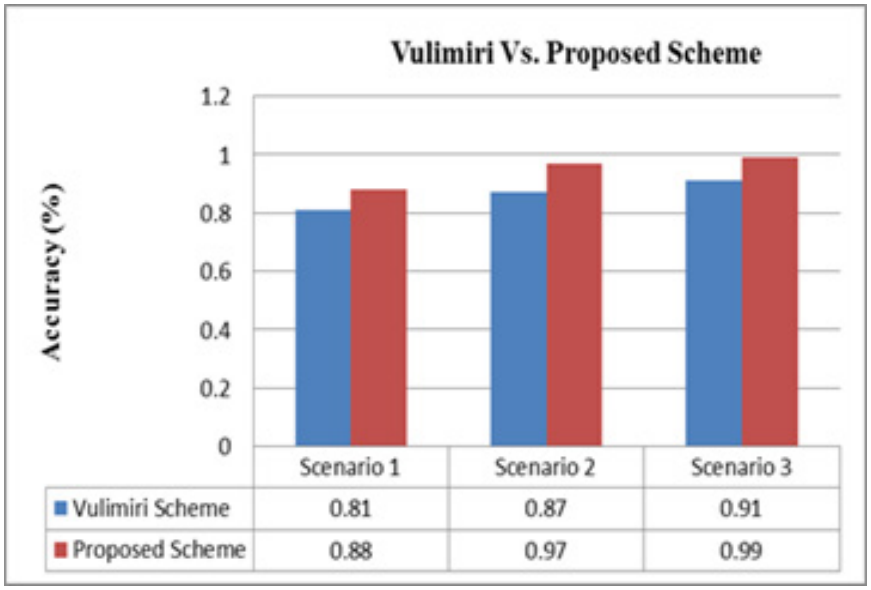

Figure 8. Vulimiri vs. proposed scheme.

cles continuously verify received PCN alerts by using the number of secondary alerts transmitted around the assumed crash location. Unfortunately, a number of the existing schemes work by building vehicles reputation models which have low detection accuracy. Some other schemes[3,11,18] use predictive mechanisms of verifying primary alerts which is also not accurate. Since VANETs handle life critical information, any small error might cause an unfavourable event. Avoiding accidents so as to enhance driving performance is an important factor considered in vehicle safety applications. The receipt of a substantial number of secondary alerts makes drivers to be properly informed about the road condition thereby enhancing driving performance which leads to increase safety. Table 2 compares the belief values of the Vulimiri scheme with the proposed scheme.

In each scenario, the proposed scheme gives a better belief value for verifying a received PCN alert. For both scheme, vehicles moving with high speed on the highway detects misbehaviour more accurately. Scenario 3 having the highest speed of the 3 scenarios verifies all PCN alerts with 100% accuracy as shown in the experiment 3 of section IV. Figure 8 shows the comparison between Vulimiri scheme and the proposed MDS.

5. Conclusion

This paper discussed how a Misbehavior Detection Scheme was developed using the crash scenario dataset was designed. The developed MDS had (5) components. These components include receiving PCN, recording secondary alerts, estimating scenario probability, calculating scenario threshold and finally transmitting true alert or reporting misbehavior. The Bayesian approach was used to calculate the probability of secondary events given that a primary event has already occurred. Results from ten (10) simulation runs of crash were used to calculate the degree of occurrence of events.

Using the proposed MDS to verify PCN alert shows that scenario 3 provided the best results with 100% detections accuracy. This means all received alerts were correctly verified by the scheme. The scheme also shows that vehicles in high speed scenarios verify alerts more correctly than scenario with low moving vehicles. This paper compared the proposed scheme with the existing Vulimiri scheme. Results from simulation shows that the number of secondary alerts transmitted in the proposed scheme can be correlated to detect the correctness of a received PCN alert. Information from the behavior of vehicles in terms of lane change and braking alerts transmitted provided a useful source of information in identifying the correctness of PCN alerts. A high number of LC and EEBL transmitted around crash location assure the correctness of detection accuracy. The paper presented different scenarios for different cases of PCN alerts. In each case, the proposed scheme shows that an event was detected with a higher accuracy rate.

6. References

1. WHO. 10 Facts on Global Road Safety, 2014. Date Accessed: 24/3/2016. Available at: www. Goggle.com.
2. Stephen E. Explaining International IT Application Leadership: Intelligent Transportation Systems. The Information Technology and Innovation Foundation, Jan 2010.
3. Harit SK, Singh G, Tyagi N. Fox-Hole Model for Data-Centric Misbehavior Detection in VANETs. Paper Presented at the Computer and Communication Technology (ICCCT), Nov 2012, p. 271-7.
4. Maria EM, Arun KP. Threat Analysis and Defence Mechanisms in VANET, International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Jan; 3(1):47-53.
5. Ruj S, Cavenaghi MA, Zhen Huang, Nayak A, Stojmenovic I. On Data-Centric Misbehavior Detection in VANETs. Paper Presented at the Vehicular Technology Conference (VTC Fall), IEEE, 2011 Sep, p.1-5.
6. Raya M, Papadimitratos P, Aad I, Jungels D, Hubaux JP. Eviction of Misbehaving and Faulty Nodes in Vehicular Networks, IEEE Journal on Selected Areas in Communications. 2007; 25(8):1557-68.
7. Hoa LAV, Cavalli A. Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey, International Journal on Ad Hoc Networking Systems (IJANS). 2014; 4(2).
8. Fuad AG, Anazida Z, Murad A Rassam. Data Verification and Misbehaviour Detection in Vehicular Ad-hoc Networks, Journal Technology Sciences and Engineering. 2015; 73(2):37–44.

9. Georgios K, Onur A, Eylem E, Geert H, Boangoat J, Kenneth L, Timothy Weil. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions, IEEE Communications Surveys and Tutorials, Fourth Quarter. 2011; 13(4):584–616.
10. Uzma K, Shikha A, Sanjay S. A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks. Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing, 2015, p. 339.
11. Mainak G, Anitha V, Arobinda G, Arzad AK, Skanda NM. Detecting Misbehaviors in VANET with Integrated Root-Cause Analysis, Ad Hoc Networks. 2010; 8(7):778-90.
12. Philippe G, Dan G, Jessica S. Detecting and Correcting Malicious Data in VANETs. Paper presented at the Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, Philadelphia, PA, USA. 2004, p. 29-37.
13. Daeinabi A, Rahbar AG. Detection of Malicious Vehicles (DMV) through Monitoring in Vehicular Ad-Hoc Networks, Multimedia Tools Appl. 2013; 66(2):325–38.
14. Kadam, M, Limkar S. New Approach for Detection and Prevention of Misbehave/Malicious Vehicles from VANET. In: Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA). AISC, 2013, 247, p. 287–95.
15. Vulimiri A, Gupta A, Roy P, Muthaiah SN, Kherani AA. Application of Secondary Information for Misbehavior Detection in VANETs, 9th International IFIP-TC6 Networking Conference, Networking Chennai. 2010; 6091:385-96.
16. Zhen H, Sushmita R, Marcos C, Amiya N. Limitations of Trust Management Schemes in VANET and Countermeasures. IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, 2011, p.1228-32.
17. Wei YC, Chen YM. Adaptive Decision Making for Improving Trust Establishment in VANET. 16th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2014, p.1-4.
18. Barnwal RP, Ghosh SK. Heartbeat Message Based Misbehavior Detection Scheme for Vehicular Ad-Hoc Networks. In: 2012 International Conference on Connected Vehicles and Expo (ICCVE), 2012, p. 29–34.
19. Huang D, Williams SA, Shere S. Cheater Detection in Vehicular Networks. In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, p. 193–200.