A Deep Learning Based Driver Classification and Trust Computation in VANETs

Shrikant Tangade
Electronics and Communication Engg.
REVA Institute of Technology and Management
Bengaluru, India
Email: shrikantstangade@reva.edu.in

Sunilkumar S. Manvi
School of Computing&IT
REVA University
Bengaluru, India
Email: ssmanvi@reva.edu.in

Stive Hassan
Electronics and Communication Engg.
REVA University
Bengaluru, India
Email: stive.lf@gmail.com

***Abstract*—Vehicular ad hoc networks (VANETs) are most promising technology for smart transportation systems to provide road safety. However, VANETs are more vulnerable to malicious nodes and susceptible to a number of security attacks. In order to provide security against these attacks, most of the researchers have presented cryptography based schemes. These schemes ensure legitimate sender but cannot prevent broadcasting bogus message from legitimate sender. Hence, many researchers have proposed trust management based schemes to address internal attacks. However, these schemes encounter with complex iterations and computation overhead. To address these issues, in this paper, a deep learning based driver classification and trust computation (DL-DCTC) scheme is proposed. The sequential Deep Neural Network models are presented to calculate reward-points based on driver behaviour and classify fraudulent and non-fraudulent message / driver. The trust of a vehicle is computed using its reward-points earned during Vehicle to Vehicle (V2V) communications. Extensive simulation results are presented to validate effectiveness of proposed DL-DCTC scheme. The performance analysis showed that proposed scheme's performance is comparatively improved by reduction in computation overhead.**

***Keywords*–VANET, Security, Deep Learning, V2I, V2V.**

I. Introduction

The vehicular ad hoc networks (VANETs) are highly dynamic network of vehicles, which uses Dedicated Short Range Communication (DSRC) technology for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. Each vehicle is embedded with On-Board Unit (OBU) and roads are fixed with static Road Side Units (RSUs), these enable V2V and V2I communications [1]. The VANET emerges as a most popular technology in both academia and industry in the domain of intelligent transportation systems (ITSs), since, it significantly improves road safety and traffic congession. The safety and traffic servies include intersection collision avoidance, vehicle post crash warning, lane changing assistance, traffic and road condition warnings [2]. VANET is thus visualized to be one of the most important ITS applications.

In VANETs, each vehicle broadcasts life critical safety messages for every 300 milliseconds inorder to provide safety to vehicle passengers [3]. These broadcast safety messages may be vulnerable to security attacks and also may arise one more security issue, the notion of trust among different peers. Therefore our foremost objective is to overcome these security and trust issues before we deploy VANET applications in practice. The unique characteristics of VANETs such as high mobility, dynamic topology, and distributed operation made security in VANET a challenging task [4].

In order to provide security in VANETs, many researchers proposed various security schemes and most of these schemes are based on cryptography authentication. Literature shows a limitation of message authentication schemes can only ensure that messages are sent from legitimate senders, but cannot prevent a legitimate sender from broadcasting bogus or altering the message. To address this kind of internal attacks, researchers have proposed trust management based security schemes [5]. The main objective of employing trust in VANETs is to detect dishonest peers as well as malicious data sent by these dishonest peers, and to give incentives for these peers to behave honestly and discourage self-interested behavior. As per literature survey, the trust management schemes that have been proposed are classified into three categories, they are: (i). entity oriented, (ii) data oriented, and (iii). hybrid [6]. Trust evaluation is based on various factors, such as, reward points, history of past interactions, recommendations from neighboring nodes, etc.

Trust management between neighboring vehicles is also challenging due to random distribution and high mobility of vehicles. However, most of the existing trust based security schemes are featured with complex iterations. These can lower the VANET performance and increase in network latency. Thus, Deep Learning algorithms are suitable to increase reliability, lower latency, and detect security issues in VANETs. In this paper, we propose a Deep Learning based scheme for secure communications in VANETs.

A. Problem Statement

The primary goal of this paper is to propose a deep learning based driver classification and trust computation (DL-DCTC) scheme for secure communications in VANETs. The sequential Deep Neural Network models are proposed to calculate reward-points and trust-value of vehicle is computed using reward-points earned during V2V communications. The proposed Deep Neural Network model is suitable approach for detecting and analyzing security issues in VANETs.

978-1-7281-1220-6/19/$31.00 ©2019 IEEE

B. Our Contribution

A Deep Learning algorithms are suitable to increase reliability, lower latency, and detect security issues in VANETs. In summary, this papers major contributions are as follows.

- Firstly, we provide first sequential Deep Neural Network model-1 of four hidden layers to calculate reward-points based on driver behaviour.
- Secondly, we provide second sequential Deep Neural Network model-2 to verify whether driver is fraudulent or non-fraudulent through reveived message.
- Thirdly,we formulate trust-value computaion by providing reward-points calculated using Deep Learning approach.
- Finally, we demonstrate performance analysis of DL-DCTC scheme.

C. Organization of the paper

The remainder of this paper is organized as follows. Section II provides survey of related work. Section III presents DL-DCTC scheme in detail with the sequential Deep Neural Network models and trust computation. Section IV presents performance analysis and simulation results of DL-DCTC. Finally, Section V summarizes concluding remarks and future work.

II. Related Work

Already many researchers have presented some excellent trust-based security schemes in VANETs. These schemes are still hard to ensure secure communications because most existing security schemes are featured with complex iterations and lower network performance. In this section, we briefly review existing trust-based schemes in VANETs.

Bimeyer *et al.* [7], Li *et al.* [8], and Li *et al.* [9] have been presented third trust party (TTP) based trust management schemes. These TTP based schemes require centralized reputation server or center to establish and maintain a global reputation system. In such scenario, there is more chance to attack this centralized system by attackers, which leads to single point of system failure and its high cost to maintain such TTP. Haas *et al.* [10], Raya *et al.* [11] have proposed trust management scheme, which relies on infrastructure and makes use of certificates.

Minhas *et al.* [12] and Mrmol *et al.* [13] have proposed entity-centric trust models. The [12] develop a multifaceted trust modeling approach to find out the entities that are broadcasting bogus data. The [13] proposed a trust and reputation infrastructure-based (TRIP) trust scheme relying on RSUs to detect selfish or malicious vehicles. Gurung *et al.* [14], Rawat *et al.* [15], and Hussain *et al.* [16] proposed data-centric trust models. In [14], presented trust model to evaluate the trustworthiness of a broadcasted message directly based on content conflict and similarity. The [15] proposed trust scheme based on a received signal strength (RSS) of the received message to measure the trust level of the message. The [16] proposed data-centric trust scheme, where email-based and networks-based social trusts are adopted. The major drawbacks of data-centric trust models are latency and data sparsity. Some researchers have presented Hybrid trust models, where, trustworthiness of both vehicles and data are evaluated. Li *et al.* [17] and Abdelaziz *et al.* [18] have proposed Hybrid trust schemes. In [17], attack-resistant trust management scheme (ART) cope with malicious attacks by evaluating trustworthiness of both vehicles and messages. In [18], a hybrid trust model is proposed to strengthen the message relay and detect DoS attacks.

Recently many researchers are working on Machine Learning and Deep Learning based trust management schemes to reduce the complex iterations of existng trust based security schemes. Raya *et al.* [19] proposed a scheme, where, Bayesian and Dempster Shafer Theory (DST) techniques are used for trust computation. Grover *et al.* [20] and [21] proposed a Machine Learning framework for misbehavior classification and detection. Lpez *et al.* [22] presented trust management scheme, where, sigmoid function was employed for computing the result of non-linear function by considering the input vectors.

III. The Proposed DL-DCTC Scheme

The proposed scheme has two phases, they are, Phase-I: initialization and off-line registration and Phase-II: trust computation based on driver behaviour. First we present a VANET architecture model used in the proposed work and then we discuss the detailed Phase-I and Phase-II steps of DL-DCTC scheme.

A. Network Architecture

The VANET architecture model presented in this paper is shown in Fig. 1. This model consists of four primary components, they are: (i). OBU, (ii). RSU, (iii). Agent of Trusted Authority (ATA), and (iv). Regional Transport Office (RTO). The detailed description of these components are explained as follow.

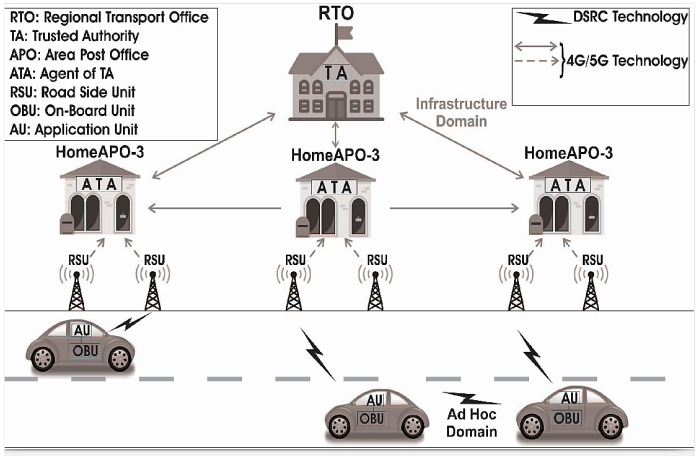

Fig. 1. VANET architecture

- OBUs: It is embedded in each vehicle which enables V2V and V2I communications.

- RSUs: These are stationary units deployed on road side for V2I communications.
- ATA: The Area Post Offices (APOs) are embedded with ATA. It computes new trust-value of vehicles with the help of RSUs.
- RTO: It is the supreme trusted entity in VANET called as trusted authority (TA). It manages the off- line registration of ATAs, RSUs, and vehicles by pair of private and public keys.

The list of notations used in this paper are listed in Table I.

TABLE I
NOTATIONS USED AND THEIR DESCRIPTION

Notation	Description
TA	Trusted Authority
RTO	Regional Transport Office
ATA	Agent of TA
APO	Area Post Office
RSU	Road Side Unit
OBU	On-Board Unit
V	a vehicle in the netwpork
Vi	Sendind vehicle in the netwpork
RID_{ATA}	Real-ID of ATA
RID_{RSU}	Real-ID of RSU
RID_{V}	Real-ID of 'V'
PrK_{ATA}	Private Key of ATA
PuK_{ATA}	Public Key of ATA
PrK_{RSU}	Private Key of RSU
PuK_{RSU}	Public Key of RSU
PrK_{V}	Private Key of 'V'
PuK_{V}	Public Key of 'V'
PuK_{RTO}	Public Key of RTO
SrK_{RTO}	Secrete key of RTO
SrK_{ATA}	Secrete key of ATA
SM_{Vi}	Safety-Message of vehicle Vi
$Frwd_{SM}$	Forwarded SM_{Vi}
AltMsg	Alert-Message
TV_{Code}	Code of trust-value
$PsID_{V}$	Unique temporary Pseudo-ID of 'V'
TmSt	Time Stamp
SIG_{PrK_V}	Signature of 'V' using its PrK_V
HC'	Hash Code calculates by RSU'
CTL_i	Current trust-level
RPs	Reward Points
$ReqRP_{Vi}$	Required RP of Vi
TL	Trust-Level
CLT	Current Top Level
BTRP	Total Reward Points required to reach from Base-level to Top-level
$BTRP_C$	BTRP of Current Level Range
$BTRP_N$	BTRP of Next Level Range

B. Phase-I: Initialization and Off-line Registration

Before ATAs, RSUs, and vehicles take part in VANET, they must register with trusted authority *RTO*. In this Phase-I, each *ATAs, RSUs* and vehicles register off-line with *RTO* as follow.

- The *ATA* registers with *RTO* with its real identity RID_{ATA}. The *RTO* then computes and uploads four keys along with its RID_{ATA} as shown in Eq. (1).

$$ATA = (RID_{\text{ATA}}, PrK_{\text{ATA}}, PuK_{\text{ATA}}, PuK_{\text{RTO}}, \&SrK_{\text{RTO}}) \quad (1)$$

- Each *RSU* also registers with the nearest *ATA* with its real identity RID_{RSU}. After off-line registration, the *ATA* uploads system credentials to the *RSU* as shown in Eq. (2).

$$RSU = (RID_{\text{RSU}}, PrK_{\text{RSU}}, PuK_{\text{RSU}}, PuK_{\text{ATA}}, \&SrK_{\text{ATA}}) \quad (2)$$

- Similarly, each vehicle *'V'* also registers with the *RTO* by its real identity RID_V. After off-line registration, the *RTO* uploads system credentials to vehicle with an initial trust-value (*TV*) as zero as shown in Eq. (3).

$$V = (RID_{\text{V}}, mPsID_{\text{V}}, PrK_{\text{V}}, PuK_{\text{V}}, TV_{\text{V}} = 0, HMAC_{\text{SrK}_{\text{RTO}}}(TV_{\text{V}}), SrK_{\text{ATA}}, \&PuK_{\text{RTO}}) \quad (3)$$

Once the registration is complete, *RTO* distributes vehicle's *'V'* credentials to all the *ATAs* within its coverage area.

C. Phase-II: Trust Computation Based on Driver Behaviour

In proposed scheme, the trust-value TV_V of a vehicle is compuatated using its reward-points based on driver behaviour of a broadcasting vehicle V_i. The Deep Neural Network is proposed to calculate reward-points and verify broadcasted safety-message is fraudulent or non-fraudulent. We considered trust-value (TV_V) is normalized value i.e. it ranges from 0 to 1.

In this proposed work, the format of the safety-message SM_{Vi}, which broadcast during V2V communications is considered as shown in Eq. (4).

$$SM_{\text{Vi}} = (AltMsg||Behaviour_{\text{Vi}}||TV_{\text{Curr}}||TV_{\text{Code}}|| HMAC_{\text{SrK}}(AltMsg||TV_{\text{Curr}})||PsID_{\text{V}}|| SIG_{\text{PrKv}}(AltMsg||TV_{\text{Curr}})||TmSt) \quad (4)$$

where '*Behaviour*' represents driver behaviour parameters of vehicle V_i as shown in Eq. (5).

$$Behaviour_{\text{Vi}} = (VS||DS||RPM||RSC||TC) \quad (5)$$

where, VS = Vehicle Speed, DS = Driving Style, RPM = Revolutions Per Minute, RSC = Road Surface Condition, TC = Traffic Condition.

Once the nearby *RSU* receives the broadcasted safety-message SM_{Vi} from vehicle V_i, it first authenticates the V_i and then calculates reward-points using Deep Neural Network-1 based on V_i's driver behavioural parameters. Next, the *RSU* verifies whether the received SM_{Vi} is fraudulent or non-fraudulent using Deep Neural Network-2. Finally, *ATU* computes new trust-value New_TV_{Vi} of V_i. The detailed steps of calculating reward-points and computing New_TV_{Vi} based on driver behaviour is discussed in the Algorithms-1, 2 and 3.

IV. RESULTS AND DISCUSSION

This section presents, the performance evaluation of proposed DL-DCTC scheme. The performance evaluation depicts efficiency of the scheme.

A. Simulation Environment

The proposed scheme is simulated in the computer system with Intel Core i3-3770, 3.4 GHz, and 4 GB RAM. We used the TensorFlow 1.6.0 open source software library with python 3.6 and network simulator ns-3 on Linux 64-bit operating system. The other network parameters which are considered for simulating proposed scheme is listed in Table III.

Algorithm 1 Trust Computation of a Vehicle

Input: $SafMsg_{Vi}$
Output: $NewTV_{Vi}$

1: **BEGIN**
2: First, the *RSU* authenticates the sending vehicle V_i then calculates reward-points and verifies received SM_{Vi} using Algorithm-2.
3: Next, *ATU* computes New_TV_{Vi} using reward-points calcuated based on driver behavioural parameters. The detailed steps of New_TV_{Vi} computation is presented in Algorithm-3.
4: **END**

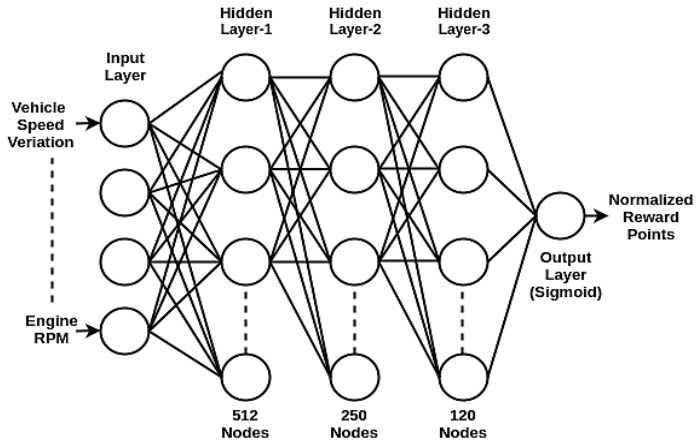

Fig. 2. Sequential Deep Neural Network Model-1

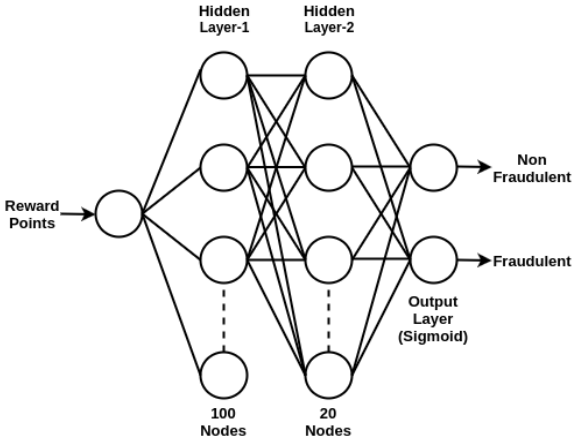

Fig. 3. Sequential Deep Neural Network Model-2

B. Performance Evaluation

The proposed DL-DCTC scheme performance is first analyzed by testing and training the proposed two Deep Neural Network models. Later, the proposed scheme is compared with existing schemes [23] and [24] which are denoted in graphs as ID-MAP (Identity-Based Message Authentication using Proxy vehicles) and Xiaoyan's, respectively.

Algorithm 2 Authentication and Verification by *RSU*

Input: SM_{Vi}
Output: RP_{Vi} and Fraudulent or Non_Fraudulent

1: **BEGIN**
2: Once the nearby *RSU* receives safety-message SM_{Vi} from the sending vehicle V_i, first it authenticates the sending vehicle V_i by calculating hash code *HC'* as shown in Eq. (6) and verifies calculated *HC'* with recived HMAC as given in next step.

$$HC' = HMAC(SrK_{\text{ATA}}, Behaviour_{\text{Vi}} || TV_{\text{Curr}}) \quad (6)$$

3: **if** *(HC' == HMAC (SrK, AltMsg ll* TV_{Curr}*))* **then**
4: Both vehicle and message are authenticated successfully. Next, the *RSU* calculates RP_{Vi} based on Vi's behaviours $Behaviour_{Vi}$ using Deep Neural Network Model-1 as shown in Fig. 2.
5: Next, the *RSU* verifies whether the sender or received SM_{Vi} is Fraudulent or Non_Fraudulent using Deep Neural Network Model-2 as shown in Fig. 3.
6: **if** *(*SM_{Vi} *== Non_Fraudulent)* **then**
7: The *RSU* forwards SM_{Vi} and sends calculated reward-points RP_{Vi} to *ATA* as shwon in Eq. (7) through secured channel for computing New_TV_{Vi}.

$$Frwd_{\text{SM}} = SM_{\text{Vi}} || RP_{\text{Vi}} || SIG_{\text{PrK}_{\text{RSU}}}(RP_{\text{Vi}} || TV_{\text{Curr}}) || TS_{\text{Frwd}} \quad (7)$$

8: **else**
9: The SM_{Vi} is Fraudulent hence *RSU* drops it.
10: **end if**
11: **else**
12: Either sending vehicle V_i or message SM_{Vi} is unauthenticated, hence, drops the received SM_{Vi}
13: **end if**
14: **END**

1) Deep Neural Network models accuracy: The proposed Deep Neural Network Model-1 as shown in Fig. 2 generates a validation accuracy of 82.17% and a testing accuracy of 79.55%, with a training, testing and validation split of 60%, 20% and 20%. The Fig. 4 shows a scatter plot of the model based prediction to the actual calculated reward-points. The second Deep Neural Network Model-2 as shown in Fig. 3 generates training and testing accuracies of 80% and 76% respectively. The Fig. 5 shows non-fraudulent test, where, the number '0' at Y-axis depicts a fraudulent and number '1' depicts a non-fraudulent.

2) Compuatation overhead: In the proposed DL-DCTC scheme, the safety-message SM_{Vi} is appended with driver behavioural parameters $Behaviour_{Vi}$, the *HMAC*, current trust-value TV_{Curr}, and digital signature of sending vehicle as shown in Eq. (4). The receiving *RSU* verifies *HMAC* to ensure

Algorithm 3 Computation of New Trust-Value

Input: $Frwd_{SM}$, TV_{Curr}, *CLT, and* $BTRP_C$
Output: New_TV_{Vi}

1: **BEGIN**
2: The *ATA* starts computing new trust-value TV_{New} of sending vehicle V_i as soon as it receives $Frwd_{SM}$ by *RSU* through secured channel.
3: The *ATA* calculates the required reward-points $ReqRP_{Vi}$ of V_i to reach current level top *CLT* (for e.g.:- if TV_{Curr} is 0.24, *CLT* is 0.3, and $BTRP_C$ is 150) by refering Table II as shown in Eq. (8).

$$ReqRP_{\mathrm{Vi}} = \{(CLT - TV_{\mathrm{Curr}}) \times 10\} \times BTRP_{\mathrm{C}} \quad (8)$$

4: The *ATA* calculates acquired reward-points $AcqRP_{Vi}$ using $ReqRP_{Vi}$ and $BTRP_C$ *as shown in Eq. (9).*

$$AcqRP_{\mathrm{Vi}} = (BTRP_{\mathrm{C}} - ReqRP_{\mathrm{Vi}}) \quad (9)$$

5: The *ATA* calculates the new trust-value New_TV_{Vi} of V_i by making use of $ReqRP_{Vi}$, $AcqRP_{Vi}$, and $BTRP_C$ as shown in Eqs. (10) and (11).
6: **if** ($ReqRP_{Vi} > AcqRP_{Vi}$) **then**
7:

$$New\_TV_{\mathrm{Vi}} = TV_{\mathrm{Curr}} + \frac{AcqRP_{\mathrm{Vi}}}{(BTRP_{\mathrm{C}} \times 10)} \quad (10)$$

8: **else**
9:

$$New\_TV_{\mathrm{Vi}} = CLT + \frac{(AcqRP_{\mathrm{Vi}} - ReqRP_{\mathrm{Vi}})}{(BTRP_{\mathrm{N}} \times 10)} \quad (11)$$

10: **end if**
11: The *ATA* stores new trust-value New_TV_{Vi} of V_i in its database and also updates with *RTO*. And whenver it receives a request $REQ_{TV_{Upid}}$ for trust-value updation from V_i, it updates with New_TV_{Vi}.
12: **END**

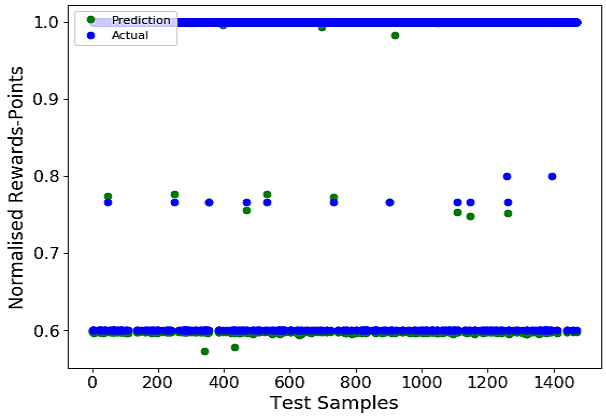

Fig. 4. Prediction Vs. Actual Value of Reward Points

TABLE II
TRUST TABLE TO BE REFERRED TO CALCULATE AND VERIFY THE TRUST LEVEL (TL) OF A NODE

Trust Level (TL)	Required Reward Points (BTRP)
0 - 0.1	50
0.1 - 0.2	100
0.2 - 0.3	150
0.3 - 0.4	200
0.4 - 0.5	250
0.5 - 0.6	300
0.6 - 0.7	350
0.7 - 0.8	400
0.8 - 0.9	450
0.9 - 1.0	500

TABLE III
NS-3 SIMULATION PARAMETERS

Parameters	**Value**
Area	1000 m x 1000 m
Number of Vehicles	100
Speed of Vehicles	80 km/hr to 100 km/hr
Communication Range of Vehicles	100 m To 500 m
Number of RSUs	3
Channel Bandwidth	6 Mb/s
Total Safety-Message (Packet) Length	165 B
Simulation Time	200 s

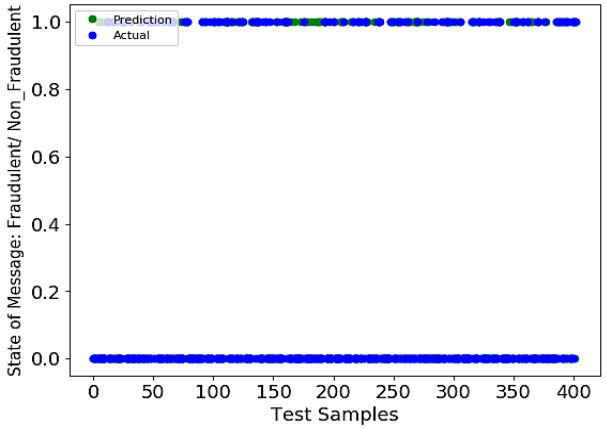

Fig. 5. Prediction Vs. Actual Value of Non-Fraudulent Test

message integrity and authentication of the sending vehicle. The *RSU* then make use of $Behaviour_{Vi}$ to calculate reward-points *RPs*. The computation of New_TV_{Vi} is carried out by *ATA*. Whereas, digital signature is verified by *ATA* for further revocation of unauthorized vehicles. The Fig. 6 depicts that the computation overhead of proposed DL-DCTC scheme is very less as compared to other schemes. The safety-message used in Xiaoyan's and ID-MAP schemes take 16 ms and 18.75 ms for verification of signatures, respectively. Whereas, in proposed DL-DCTC scheme, HMAC takes only 4 ms and 3 ms for authentication and trust computation respectively. Hence, total computation overhead of DL-DCTC scheme is 7 ms.

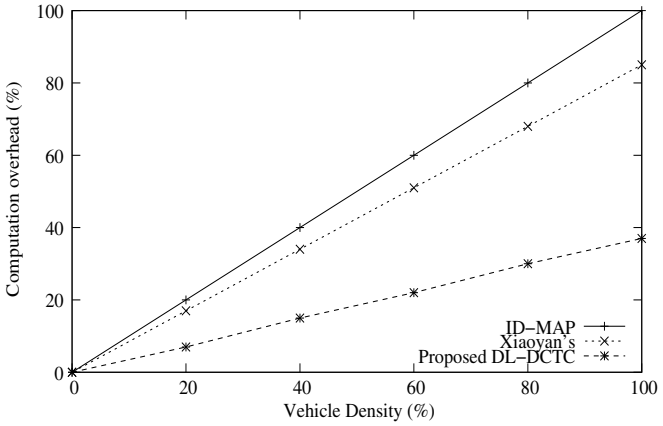

Fig. 6. Computation overhead

V. Conclusion

In this paper, a DL-DCTC scheme is proposed to classify driver by his/her behaviour and then compute vehicle trust using its reward-points. The proposed scheme has two phases. In phase-I, all network entities register off-line with *RTO* and initializes with system parameters. The phase-II is trust computation based on driver behaviour. In phase-II, we presented two Deep Neural Network Models. The *RSU* calculates reward-points based on driver behaviour and verifies whether driver is fraudulent or non-fraudulent using model-1 and model-2 respectively. The *ATA* then computes new trust-value of a vehicle based on its reward-points. The simulation results show the effectiveness of proposed scheme. The proposed scheme's performance can be further improved by employing deep reinforcement machine learning techniquie.

References

[1] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions", Vehicular Communications, vol. 9, pp. 268-280, 2017.

[2] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy", IEEE Trans. Intell. Transp. Syst., DOI. 10.1109/TITS.2018.2818888, pp. 1-17, Mar. 2018.

[3] Dedicated Short Range Commun. (DSRC). [Online]. Available:http://standards.ieee.org/develop/wg/1609 WG.html, 2015.

[4] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in VANETs", IEEE Trans. Veh. Technol., vol. 67, no. 9, pp. 8647-8655, Sep. 2018.

[5] C. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and Pietro, "Trust management for vehicular networks: An adversary-oriented overview", IEEE Access, vol. 4, pp. 9293-9307, Dec. 2016.

[6] J. Zhang, "A survey on trust management for VANETs", in Proc. IEEE International Conference on Advanced Information Networking and Applications, Biopolis, Singapore, pp. 105-112, Mar. 2011. for securing vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst., vol. 17, no. 4, pp. 960969, Apr. 2016.

[7] N. Bimeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility", in Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl. ACM, pp. 73-82, 2012.

[8] Q. Li, A. Malip, K. M. Martin, S. L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs", IEEE Trans. Veh. Technol., vol. 61, no. 9, pp. 4095-4108, Nov. 2012.

[9] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs", in Proc. 5th Int. Conf. IEEE Intell. Netw. Collaborative Syst. (INCoS), pp. 210-214, Sep. 2013.

[10] J. J. Haas, Y.C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET", in Proceedings of VANET, pp. 89-98, 2009.

[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks", IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[12] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks", IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 41, no. 3, pp. 407-420, May 2011.

[13] F. G. Mrmol and G. M. Prez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks", J. Netw. Comput. Appl., vol. 35, no. 3, pp. 934-941, 2012.

[14] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks", in Proc. Int. Conf. Netw. Syst. Secur., pp. 94-108, 2013.

[15] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking", Ad Hoc Sensor Wireless Netw., vol. 24, nos. 3-4, pp. 283-305, 2015.

[16] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. T. Seo, "A hybrid trust management framework for vehicular social networks", in Proc. Int. Conf. Comput. Social Netw., pp. 214-225, 2016.

[17] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks", IEEE Trans. Intell. Transp. Syst., vol. 17, no. 4, pp. 960-969, Apr. 2016.

[18] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust model with delayed verification for message relay in VANETs", in Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), pp. 700-705, Aug. 2014.

[19] M. Raya, P. Papadimitratos, V. D. Gligor, and J.P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks", in INFOCOM 2008. The 27th IEEE Conference on Computer Communications. pp. 1238-1246, 2008.

[20] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in vanet", in International Conference on Advances in Computing and Communications. Springer, pp. 644-653, 2011.

[21] J. Grover, V. Laxmi, and M. S. Gaur, "Misbehavior detection based on ensemble learning in vanet", in International Conference on Advanced Computing, Networking and Security. Springer, pp. 602-611, 2011.

[22] J. Lpez and S. Maag, "Towards a generic trust management framework using a machine-learning-based trust model", in Trustcom/BigDataSE/ISPA, 2015 IEEE, vol. 1., pp. 1343-1348, 2015.

[23] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733-1743, 2015.

[24] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Tran. Veh. Technol.*, vol. 63, no. 2, pp. 907-919, Feb. 2014.