JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Trust-aware block chain-based SDVN for Secure Vehicular Communication

[1]Pathak Pankaj, [2]Vattam Jayarajesh,

[1] ME-Research Scholar, [2]Assistant Professor

[1]Department of Electronics and Telecommunication Engineering, [2]Department of Electrical Engineering,

[12]ARMIET, Thane, India

Abstract: The vehicular ad hoc network (VANET) is one of the emerging techniques, which provides network services to the vehicles to enable effective communication between the vehicles. Software-defined networking (SDN) helps to improve the performance of the network and a new method called software defined vehicular network (SDVN) solved the security issues in the roads by tracking the vehicles of the attacker. There are still securities issues in the SDVN hence in this research VANET model for the intrusion detection will be employed. The neural networks are employed in the proposed VANET for performing complex calculations so as to find intrusions in the transportation system.

Index Terms **- SDN, Vehicular network, Trust management, Block-chain Technology**

I. INTRODUCTION

Vehicle ad-hoc networks (VANETs) is now emerging as a new trend in the urban environment, which aims to reduce the transportation issues, like car accidents, congestions in traffic and pollution [9-11] [6] . The VANET has three major divisions such as, vehicles, road side units (RSU) and the department of motor vehicles (DMV) [18] [8]. VANETs emerge as an effective connection in between the vehicles, which permits the drivers and the road operators to provide instructions regarding the real-time traffic data. VANET needs an efficient collaboration of traffic, which includes mostly two groups of communication, they are communication carried out between the vehicles (V2V) and the cooperation between the vehicles and infrastructures (V2I) [6]. VANET with the use of inter-vehicular communication is a pursuing technology for enhancing the safety and circulating the traffic details [1]. Even though, in V2I and V2V, vehicles transfer warning signals and instructions for managing the traffic to enhance the safety in roads and to enhance the driving experience in cities [12-14] [6]. due to the evolutions in the modern vehicles, which are now designed with advanced features not only require VANETs for enhancing the safety but also required to protect the numerous amounts of the data produced in the urban regions [6]. Enhancements in the Intelligent Transportation Networks (ITS), helps in reduction of accidents, fuel cost and the traffic congestions and so on are needed in urban areas for the mobility issues of vehicles [15,16] [8]. So, VANETs are widely used in ITS to ameliorate the efficiency in transport, safety driving in addition to road security [17] [8].

Though, the VANET is one of the effective methods for extending communication to vehicles, which still encounters various problems [19] [2]. With the arrival of SDVN, the vehicles have the ability to communicate with the controllers [20] [2] and are highly flexible, scalable, adaptive and programmable vehicular network surrounding [21][22] [2] in the SDVN [2]. SDVN is an emerging network architecture in order to aid the ITS that comprises many smart applications [23,24] [3], consisting notification of emergencies, predicting the violation of traffic rules, accessing speed limit, collecting tolls and avoiding collisions. But, the information requirements for the application of ITS is blooming and advancing the architecture of SDVN and are capable to address the rise of traffic information [24] [3].

In the SDVN, the main part is the control plane, which takes decisions regarding the routing and hence, the SDVN optimization control plane improves the capability of the whole system network [3]. Software Defined Network (SDN) in addition to the centralized features makes an advantageous medium for configuring the network, improving the performance and managing the resources in VANET. Hence, the combination of SDN to VANET known as software define vehicular network (SDVN) had acquired the attention from both the industries and the academics [25] [1]. Additionally, because of the restricted capability of computations of a single SDN, there are still issues in scalability for accessing numerous amounts of requests, in which it employs additional controllers for processing complex computations and remodeling the structure of the large network systems [2]. As there are little complexities present in the SDVN designing an efficient routing protocols is challenging in the research field.

In order to address the difficulties in various intrusion prediction systems a secure VANET communication network using the machine learning model is employed for examining the information, determining the type of threats and then differentiating the destructive nodes from the normal nodes. In the VANET, various architectures of IDS are modeled for the vehicles and are light weight for meeting the demands of the intelligent monitoring of distributed surroundings [6]. A new method for scheduling the link-level and to enhance the performance delivery of VANET and to reach the necessities of QoS regarding the delay in transmission, the link comprises of receiving node and sending node.

Every transmission is called as link that can transfer one or more packets of data [1] researches on IoV assists to encourage the evolutions of advanced transportation systems and accelerating additionally the process of urban regions and hence, the researches on urban regions using IoV is carried out. For edge computing, IoV, artificial intelligence and other technologies are linked to the vehicular driving of Joint Delay and Energy-Vehicle Computational task Offloading based advanced edge computing model [5] that provides an effective routing protocols for detecting the intrusion attacks.

II Objective:

This section explains the main objectives of this research which are enumerated as follows,

- To review and analyze the various existing intrusion detection techniques and to find out the challenges in the performing research.
- To develop and design an intrusion design framework on the basis of the machine learning method.
- To mathematically develop a training algorithm that trains the neural network classifier in order to generate an accurate output.

III Significance:

The significance of this research is the use of the machine learning model with the use of neural network for the effective prediction of intrusion in the road thereby predicting the malicious vehicles.

IV. Literature Review:

S.NO	AUTHOR	METHOD	ADVANTAGES	DISADVANTAGES
1.	Yong Zhang *et al.* [1]	a novel link-level scheduling strategy,	This method enhanced the performance of collision avoidance and decreased the miss my packet issue.	The high execution time is the main drawback.
2.	Na Lin *et al.* [2]	a novel cost-effective controller placement problem (CPP)	This method had higher packet delivery ratio	The high energy consumption is the main drawback
3.	Ilora Maity *etal.* [3]	mobility-aware scheme	This method accurately determines the location of the controller for processing the requests	The lack of storage facilities is the main issue in this method.
4.	Liang Zhao *et al.* [4]	online sequential learning-based adaptive routing scheme	This method efficiently gathers the real time traffic data and processed them accurately.	Latency is the main issue of this syetem.
5.	Zhihan Lv *et al.* [5]	Internet of Vehicles (IoV) model	This method efficiently enhanced the load sharing rate.	Real time cases were required to be evaluated.
6.	Hind Bangui *et al.* [6]	machine learning model	This method enhanced the detection accuracy.	This method had to be enhanced in terms of detection of intrusion
7.	L. Ellen	Pairing-Free Signatures	This method efficiently	Unauthorized vehicles were not

	Funderburg *et al.* [7]	With Insider-Attack Resistance	identified the intrusions without employing the tamper proof devices.	identified correctly.
8.	Nitha C. Velayudhan*et al.* [8]	deep learning-centered intrusion detections system (IDS)	This method enhanced the security level and performance accuracy.	The detection accuracy of threats was required to be enhanced in terms of real life situations.

The viability of SDVN has been considered in a few early studies. By utilising SDN, literature [3] demonstrated heterogeneous vehicular communication and established a foundation for heterogeneous vehicular communication. The author of [5] worked on lowering transmission delay costs during cellular network download on the control plane. The related works in sdvn up to this point have been outlined in [6], while it has also highlighted the essential requirements and challenges of SDVN.

The primary idea behind the physical resource allocation problem is to use virtualization technology to partition a physical network into several mutually isolated virtual networks that can share the same underlying physical resources [10], which is within the purview of control plane optimization. The virtualization problem can be solved by abstracting real resources into virtual nodes and links, i.e., creating virtual networks that can deliver various services while maximising resource consumption. The mapping algorithm is a np-hard problem due to the diversity of virtual networks. The authors in [11] employed path migration to map nodes and links individually, based on the idea of bandwidth integration and traffic engineering. The goal of the multi-commodity flow challenge is to reduce costs in multi-commodity flows.

Although various studies have been conducted on SDVN, none of them consider the possibility that a hostile vehicle could present false resource requirements in order to degrade network performance, and no literature has previously explored the relationship between trust management and SDVN. As a result, we combine the SDVN with trust management for the first time in this paper.

Vehicle network trust management can be classified as centralized, decentralized, or block chain-based decentralized trust management. Several literatures have investigated the architecture and operation method of centralized trust management systems. To acquire, calculate, and store the trust value of all cars in [7, 12], a fully trusted central server with powerful processing capacity is used. [13] presented a reputation-based notification strategy in which vehicles detect traffic-relevant events and broadcast them to their neighbours. All vehicles will report the credibility report about their neighbors to the central server after calculating the message credibility sent from neighbours. In light of the feedback reports, the central server will update vehicle reputation values. While all of the aforementioned techniques are designed to use a fully trusted central server that cannot be hacked, the single point of failure remains a fatal flaw in this architecture. Meanwhile, as the number of intelligent vehicles grows, the central server will not always be able to meet the stringent QoS requirements.

A data-centric trust management scheme was described in the decentralized trust management system [14], in which each receiver estimates each piece of received data and aggregates them to determine traffic events. This type of scheme was implemented on the vehicle side, but problems may emerge due to the vehicles' limited visibility. Each RSU was used for trust management in [9], and the RSU collected the vehicle ratings and utilized a special algorithm to generate each car's trust value. As a result of the insufficient and inconsistent storage information in RSUs, various RSUs may generate different trust values for the same vehicle.

Literature [15] used a joint proof-of-work (PoW) and proof-of-stake (PoS) consensus mechanism to obtain consensus across RSUs in trust management for automotive networks in block chain-based decentralized trust management systems. Although the approach is unique, it is impractical, as it wastes a significant amount of processing resources and decreases throughput. The user's privacy cannot be guaranteed because this approach is based on the public chain network. Unlike the previous systems, we construct a trust management scheme for SDVN and present a new consensus technique to reduce confirmation time in this study. RSU can give additional physical resources to cars with more credibility based on the trust value produced from the trust management system.

V. PROPOSED SYSTEM ARCHITECTURE

The prime intention of the research is to design and develop a secure SDVN with intrusion detection system, which will effectively identifies the malicious vehicles and block the fake message provided by the malicious vehicles to enhance the road safety. A block chain structure will be constructed with the road sensing unit, which collects the information of the vehicles passing in the road and deliver to a data storing unit. The trust value of every vehicle will be generated by the optimized neural network based on the based on the history rating stored in the block chain network. The road side unit (RSU) will collect the trust value from all the vehicles, which is generated by the neural network and terminates the fake message provided by the malicious vehicle. The neural network will be optimally tuned by the proposed Swarm attack optimization, which will be developed by integrating the swarming behavior of dragonfly [26] and bubble-net attacking behavior of whale optimization [27]. The real time data will be the input to the classifier and the intrusion will be predicted. The performance of the model will be evaluated using

the performance parameters like accuracy, precision, and F1-score. The experiment will be implemented in the PYTHON tool. Figure 1 shows the prediction model for intrusion detection in vehicles.

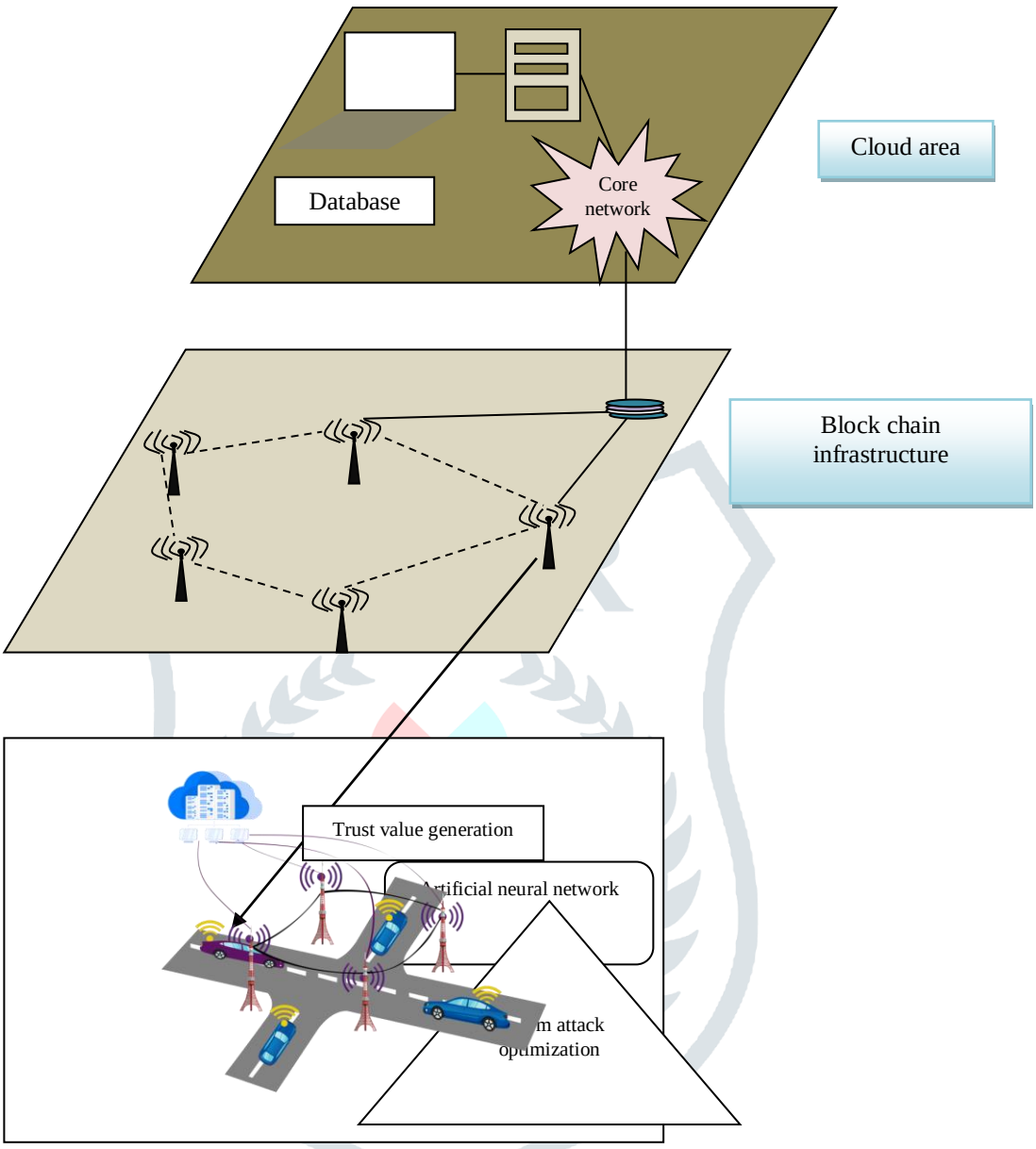

Fig: Proposed System Architecture

VI. CONCLUSION:

In this research the malicious attack will be effectively identified using the machine learning model. The optimization algorithm will be developed in this research based on the characteristics of whale and dragon fly to tune the machine learning classifier. Hence, it is expected that the proposed block chain method will attain best performance in terms of accuracy, precision and F1-score Real time data will be employed for evaluating the performance of the model.

.

ACKNOWLEDGMENT

We acknowledge the efforts by the experts who have contributed towards the development of project. We also acknowledge our guide's assistance and advice, as well as the journal's reviewers' support for adjustments and suggestions to improve the quality of the manuscript. We also appreciate the assistance and direction provided by our lecturers and guides, as well as the support provided by the journal's reviewers for adjustments and suggestions to improve the paper's quality.

REFERENCES

[01] Chen C, Wang Z, Guo B (2016) The road to the chinese smart city: progress, challenges, and future directions. IT PROF 18(1):14–17

[02] Nunes BA, Mendonca M, Nguyen X, Obraczka K, Turletti T (2014) A survey of software-defined networking: past, present, and future of programmable networks. IEEE Commun Surveys Tuts 16(3):1617–1634

[03] He Z, Cao J, Liu X (2016) SDVN: Enabling rapid network innovation for heterogeneous vehicular communication. IEEE Netw 30(4):10–15.

[04] Ozcevik ME, Canberk B, Duong TQ (2017) End to end delay modeling of heterogeneous traffic flows in software defined 5G networks. Ad Hoc Netw 60:26–39

[05] Li H, Dong M, Ota K (2016) Control plane optimization in software-defined vehicular ad hoc networks. IEEE Trans Veh Technol 65(10):7895–7904

[06] Yaqoon Y, Ahmad I, Ahmed E, Gani A, Imran M, Guizani N (2017) Overcoming the key challenges to establishing vehicular communication: is SDN the answer? IEEE Commun Mag 55(7):128–134.

[07 Mahmoud ME, Shen X (2011) An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks. IEEE Trans Veh Technol 60(8):3947– 3962.

[08] Li Z, Chi G, Tricia C (2014) On joint privacy and reputation assurance for vehicular ad hoc networks. IEEE Trans Mobile Comput 13(10):2334–2344.

[09] Huang X, Yu R, Kang J, Zhang Y (2017) Distributed reputation management for secure and efficient vehicular edge computing and networks. IEEE Access 5:25408–25420.

[10] Zheng Q, Zheng K, Zhang H, Leung VC (2016) Delay- optimal virtualized radio resource scheduling in software-defined vehicular networks via stochastic learning. IEEE Trans Veh Technol 65(10):7857–7867.

[11] Zhu Y, Ammmar M (2006) Algorithms for assigning substrate network resources to virtual network components. In: 25th IEEE international conference on computer communications (INFOCOM), pp 1–12.

[12] Lai C, Zhang K, Cheng N, Li H, Shen X (2017) SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs. IEEE Trans Intell Transport Syst 18(6):1559–1574.

[13] Li Q, Malip A, Martin KM, Ng S, Zhang J (2012) A reputation- based announcement scheme for VANETs. IEEE Trans Veh Technol 61(9):4095–4108.

[14] Raya M, Papadimitratos P, Gligor VD, Hubaux J (2008) On data- centric trust establishment in ephemeral ad hoc networks. In: IEEE 27th conference on computer communications (INFOCOM), pp 1238–1246.

[15] Yang Z, Yang K, Lei L, Zheng K, Leung VC (2018) Blockchain- based decentralized trust management in vehicular networks. IEEE Internet of Things Journal early access.

[16] Secinti G, Canberk B, Duong TQ, Shu L (2017) Software defined architecture for VANET: a testbed implementation with wireless access management. IEEE Commun Mag 55(7):135–141.

[17] Muzio JC, Rosenerg IC (1986) Introduction— multiple- valued logic. IEEE Trans Comput C-35(2):97–98 Nakamoto S (2008) https://bitcoin.org/bitcoin.pdf.

[18] Castro M, Liskov B (1999) Practical byzantine fault tolerance. In: Third symposium on operating systems design and implementa- tion (OSDI).

[19] Gonzlez A, Barra E, Beghelli A, Leiva A (2015) A sub-graph mapping-based algorithm for virtual network allocation over flexible grid networks. In: IEEE 17th International Conference on Transparent Optical Networks (ICTON), pp 1–4.

[20] Jiang M, Wang B, Wu M (2011) Research on network virtualization and virtual network mapping algorithm. Chin J Electron 39(6):1315–1320.

[21] Martin-Vega FJ, Aguayo-Torres MC, Gomez G, Entrambasaguas JT, Duong TQ (2018) Key technologies, modeling approaches, and challenges for millimeter-wave vehicular communications. IEEE Communication Magazine 56(10):28 C 35.

[22] Zhang, Yong, Mao Ye, and Lin Guan. "QoS-aware Link Scheduling Strategy for Data Transmission in SDVN," arXiv preprint arXiv:2102.00953, 2021.

[23] N. Lin, Q. Zhao, L. Zhao, A. Hawbani, L. Liu and G. Min, "A Novel Cost-Effective Controller Placement Scheme for Software-Defined Vehicular Networks," in IEEE Internet of Things Journal, vol. 8, no. 18, pp. 14080-14093, 2021.

[24] I. Maity, R. Dhiman and S. Misra, "MobiPlace: Mobility-Aware Controller Placement in Software-Defined Vehicular Networks," in IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 957-966, 2021.

[25] L. Zhao et al., "Novel Online Sequential Learning-Based Adaptive Routing for Edge Software-Defined Vehicular Networks," in IEEE Transactions on Wireless Communications, vol. 20, no. 5, pp. 2991-3004, 2021.

[26] Z. Lv, D. Chen and Q. Wang, "Diversified Technologies in Internet of Vehicles Under Intelligent Edge Computing," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2048-2059, 2021.

[27] Bangui, Hind, Mouzhi Ge, and Barbora Buhnova. "A hybrid machine learning model for intrusion detection in VANET." Computing pp.1-29, 2021.

[28] Funderburg, L. Ellen, Huimin Ren, and Im-Yeong Lee. "Pairing-Free Signatures With Insider-Attack Resistance for Vehicular Ad-Hoc Networks (VANETs)," IEEE Access, vol. 9 pp. 159587-159597, 2021.

[29]. Velayudhan, Nitha C., A. Anitha, and Mukesh Madanan. "Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC," Journal of Ambient Intelligence and Humanized Computing, pp.1-13, 2021.