IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, May 2022

An Enhanced K Nearest Neighbor Classifier for Malicious Node Detection in VANET

Abhilash Sonker and R. K. Gupta
Department of Computer Science and Engineering and Information Technology
Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh, India

Abstract: *Recently, wireless communication technologies have become a vital part of our lives. The advancements made in communication technology, VANET systems is been introduced. With the increase of vehicles, different sorts of traffic are created in realistic environment. In some cases, the traffic is created by anomalies. Henceforth, the security of VANET communication becomes an important entity. In this paper, we proposed an enhanced k-Nearest Neighbor classifier that detected the malicious node in VANET. Generally, the classifier suffers from high computational cost in distance estimation during malicious node detection. The efficiency of the proposed classifier is experimented and implemented by validating the throughput and packet delivery rate. Compared to the existing classifier, the proposed classifier achieves 20-25% improvement. By doing so, the communication overhead and delay metrics have been achieved and also helps to minimize the computational storage costs.*

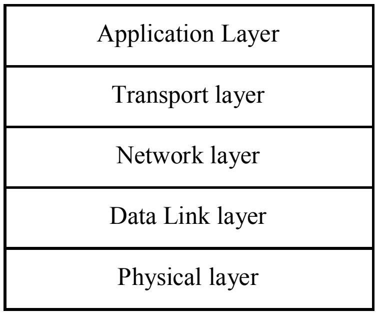
Keywords: Communication System, VANET, Detection efficiency, Security, Malicious nodes and k- Nearest neighbor classifier.

I. Introduction

The advancement made in vehicular technologies has demanded transport efficiency and road safety which turns out to be a significant area of research due to sophisticated vehicular and road infrastructure. As we know, an Adhoc network is a self-organized network i.e randomly distributed nodes, independent architecture, and so on. Vehicular Ad Hoc Networks (VANET) is the variant of Mobile Adhoc Networks (MANET) [1, 2, 3]. VANET performs similar to MANETs, where some nodes are attached to the road vehicles by following mobility constraints. Alignment with road networks has led to a high degree of determinism and predictability of vehicular traffic which requests the routing protocols for enhancing performance. Generally, IEEE 802.11p protocols standards are followed in VANET areas like predictions of accidents, efficient resource utilization and coordinating with other domains.

1.1 Architecture of VANET Communication:

IEEE 802.11p standard [4] is followed by most of the VANET communication system, the fig.1 presents the communication architecture of the VANETs. It comprises five layers, namely, application layer, transport layer, network layer, Data link layer, and physical layer.



Application Layer

Transport layer

Network layer

Data Link layer

Physical layer

Figure 1: VANETs Communication- Architecture [6]

The above layers have their own characteristics, in short, the physical layer is the foremost layer that takes raw data as input. The Data Link layer contributes to converting data into several packets. Routing protocols are defined in the network layer and communication between network entities given in the transport layer. The services of the above layers are integrated and coordinated with real-time applications. Here, the Network layer and transport layer are the core layers of VANET systems [5,6]. The routing layer (or) network layer is responsible for defining rules for packet transmission systems. Different types of routing protocols are suggested by the researchers. The main focus of the routing layer is to allow for scalability and integrity of the shared data in road networks. Once the routing protocols are efficiently designed, the communication protocols determine the success rate of the VANET systems.

1.2 Types of VANET Communication

The communication in VANETs are explained as follows:

1. Vehicle to any entities communication (V2A): The deployed vehicular nodes communicate with Road Side Units (RSU) [7] with the assistance of any centralized control, which is capable of monitoring and managing the local and global data of traffic and road constraints. It is restricted to communicate directly with similar vehicular nodes, to prevent real-time issues like congestion, and overheads.
2. Vehicle to Vehicle communication (V2V): With the help of broadcasting protocols like unicast and multicast, the vehicles can directly communicate with other vehicles.
3. Hybrid communication [8]: It combines the features of V2A and V2V communication models by extending the services of Road Side Unit (RSU) and On-Board Unit (OBU).

1.3 Motivation of the Study

Recently, hybrid communication is mostly studied by several researchers. The Internet has become an essential factor in VANET communication for navigation and maintenance of the vehicular nodes. Access Points (AP) [9] help for coordinating with network entities, to achieve scalable and secure communication paths. It is well-known that short communication paths are widely adopted which throws real-time issues like collision, improper communicator operations, anomalies invasion, and disconnected infrastructures. This becomes non-viable for real-time applications. Attack detection is one of the recent domain areas in VANET communication systems. Due to the failures of Access Points, the invasion of attackers is highly encountered in large-scale networks. This motivates us to delve into the study of developing a novel hybrid network for detecting the malicious nodes and assuring basic security primitives among the deployed vehicular nodes. Detection of misbehaving nodes in VANETs environment is a challenging task due to its dynamic topologies formation. In the VANET scenario, trust and reputation mechanisms were suggested for detecting the self-promoting attacks and bad-mouthing attacks. A node is declared as an ‘attacker’ by a consecutive trust report analysis, continuous vehicle updates and the revoked vehicles. Some malicious nodes generate false identities and expose them as normal vehicles. It convinces the other nodes by sending false information. This transmission damages communication networks. Henceforth, revocation schemes like voting are suggested to detect the Sybil attacks. Likewise, the distance between nodes is estimated for detecting false location information. The location of misbehaving nodes cannot be extracted. When the node moves on the flyover with loops, the actual distance of the nodes differs from the calculated Euclidean distance of the nodes. A group of nodes moves together in a group, then the misbehaviour nodes can’t be predicted. Henceforth, prior algorithms are not applicable to detect malicious behaviour in VANETs.

1.4 Organization of the Study

The rest of the section is arranged as follows:

- Section II presents reviews of existing techniques by stating their merits and demerits. It helps to find the research challenges prevailing in this environment.
- Section III presents the research methodology that gives a clear idea about the practical solutions to the above-stated research challenges.
- Section IV presents the experimental analysis that discusses the programming languages, simulation parameters, and network assumptions used for proving the efficiency of the proposed communication model.
- Section V presents the conclusion of the proposed model and its future directions.

DOI: 10.48175/IJARSCT-3390

II. Literature Survey

This section presents reviews of existing techniques by stating their merits and demerits. Message suppression and false message attacks are the two recent novel attacks that prevail in the VANET communication process. In VANET communication architecture, messages are converted into packets. Each packet composes source id, destination id, and the data. The goal of the message suppression attacks is to prevent the traffic and collision of information from reaching its authorities. Likewise, false message attacks are to eliminate the injection of false data from reaching its authorities [10]. Trust and reputation mechanisms have been widely suggested by the researchers to detect the misbehaviour of the nodes.

In [11], the authors suggested short-lived certificates that generate secret keys periodically based on the instruction given by the cluster heads and Regional Authority (RA). It aimed to reduce the size of CRL by improving the Central Certificate Authority (CCA) and the Local Certificate Authority (LCA). Here, RSU has two units, one for revocation list received from LCA, and has been inserted into every incoming vehicle of a cluster. The second is to generate the Neighbors Cluster Certificate List (NLCCL) [12] which checks the status of the vehicle at different zones. Every LCA updates the local certificates periodically and then transmits them to RSUs. Though data secrecy is achieved, the efficiency of the vehicles is lowered and idle until issuing the certificates. In [13], the authors presented a validation scheme for revocation status, to enhance the verification speed. Here, each CRL is embedded with credibility and issued date. It helped the RSUs for periodic checking of issued certificates. Every time, the vehicles enter the new region, then its certificates are checked. If any vehicle is revoked, then the RSU broadcasts the revoked data to all the vehicles except the relevant vehicles. It helped to secure the VANET systems from malicious behaviours.

Authors in [14] & [15] presented regional broadcast methods to ensure secure certificate evaluation models. Here, each CRL issued by CA is split into N pieces and then transferred via RSUs. The efficiency of broadcasting services of each node is analyzed by evaluating the transmission rate. Both the schemes aimed for reducing the network load by reducing CRL size. But, the methods bring challenges for On Boards Units (OBU). In [16], the authors presented short-lived anonymous certified keys in OBU. It aimed for preserving the privacy of sensitive data. Here, depending on the location of vehicles, the Region Authority (RA) is assigned. The assigned RA communicates with OBU via RSU and then verifies the validity of the sender. In cases OBU misbehaves, then its group signature from RA alerts the members in a group by facilitating the group user key and then revokes the misbehaving certificate if key constraints are not satisfied. Then, the Group Manager (GM) takes responsibility for the revoked users. In a realistic environment, it is vulnerable to many attacks.

The author in [17] discussed the effects of a lifetime with reduced CRL size. Here, pseudonyms are generated for each vehicle which ensured the node's security and reduces network overheads. Pseudonyms are also temporarily validated until successful data transmission is achieved. It is observed that there is a higher chance of message suppression attacks. In [18], the author discussed the linking of certificates and storing with bloom filters to minimize the searching complexity. The system proved that the CRL lists minimized the efforts of RSUs. If pseudonyms are compromised, then the privacy of the data is not assured. The single hop fast certificate revocation process was designed by [19]. It introduced a fixed number of RTOs presented in the RSU zone which shares the workload of CA and RSU. The behavior of each vehicle is monitored by RTO, if any misbehaves, RTO updates its network. Then, CA verified the validity of the vehicles [20]. Since the revocation list is maintained from the guidance of trusted vehicles, network attacks are reduced. The drawback is mishandling of RTO failure is not discussed.

In [21], cloud technologies are combined with the VANET, to reduce the distribution time of CRL and Ticket Transient (TT) between certificate issuing and revocation lists. In general cases, CA sends the CRL by RSU. A new entity, Traffic Police Controlled Vehicular Cloud (TPCVC) [22] was introduced which issued the CRLs instead of RA. It also takes control over the pseudo-id of the node. In real-time, it is not possible due to road safety constraints. A lightweight pseudonym with trapdoor model was suggested by [23] which removed the CRL. Here, CA takes responsibility for tracking the current position of the vehicles. Vehicle density determined the efficiency of the vehicular nodes. If the behaviour of a node in the region is altered, immediate alerts are sent to the respective RSUs. This system developed a cryptographic overhead. In [24], they presented a certificate revocation model using hash tree algorithms. Revocation lists are composed of the root of all vehicular units using Merkle Hash Tree (MHT). It is maintained for extending the CRL if it is not valid. It reduced the overheads of security primitives. Message Authentication Acceleration (MAAC) protocols were suggested by [25] that replaced the CRL verification time. With the help of message authentication code, revoked and non-revoked vehicles are distinguished for the confidentiality of the issued certificates. Trust among the nodes is not assured for the long-term communication process.

An adaptive threat detection model [26] was studied from the concepts of cloud systems with IoTs. It gears the industrial control systems. Here, two kinds of training models were designed namely, disjoint training and testing models and the disjoint labeled and unlabeled data. These two models were inserted into the different units of recurrent layers. It was trained under 30 and 100 epochs of training and testing data. An automatic database module recognized the 967 malwares with 379 features. However, the computational complexity is increased in disjoint unlabeled data models. Similar IDS model was designed by following the rules of genetic algorithms [27]. The selection of hidden layers and the activation units were optimized using GAs. Again, it was re-tuned using a backpropagation algorithm. Each hidden layer makes use of GAs bits before classifying the malwares. Initially, the datasets were normalized under optimal genetic generations and detected the malwares such DoS, R2L, Probe, and U2R. It achieved 97% accuracy by consistently following the optimal structure.

A similar hybrid model was extended by exploring with the Probabilistic Neural Network (PNN) [28]. The malware features were discovered by DBN and PNN employed for classification purposes. Along with that, the optimum number of the hidden layer was defined using Particle Swarm Optimization. It was tested in 10, 000 data that included classes, namely normal and four attacks. The designed model achieved an accuracy of 99.14% with reduced false alarm rate. Convolutional Neural Networks (CNN) was formulated with the help of DBN systems [29]. Here, three layers of RBM was designed for 122 input layers with 100 dynamic features. The iterations level of each layer was fine-tuned with the training and testing iteration sets. It has achieved 95% accuracy from the hybrid model.

A detailed architecture of DBN for IDS was still in the developmental stage because less analysis proceeded in dynamic features [30]. By the help of NSL-KDD datasets, the author described the role of static and dynamic features in designing the training classifiers. Due to the class imbalance issue, the results were not remarkable. The real-time applications of DBN with Artificial Neural Networks (ANN) [31] were studied by tuning the hidden layers and the number of features. It was tested using 5-cross validation training models with 30 epochs. The designed model detected 3000 benign and 3000 malicious files. It achieved 96.1% accuracy with 400 features. Then, hybrid anomaly detection models of DBN and one-class SVM [32] were introduced to resolve the dimensionality reduction issues. With the help of DBN, the dimensionality of the data was removed and then fed into the one-class SVM, so as to identify the malware on the collected data. It was tested on the 6 real-life datasets and achieved better performance than the DBN-SVM model.

In [33], a monitoring system was introduced to collaborate the sensor nodes deployed in the intra-clustering techniques. It was tested in beehive applications. The symptoms like Co2, O2, temperature, and others were considered for the analytic purposes. These parameters transferred into the base station and determined the states of hives. By means of a decision tree algorithm, the classification accuracy of 95% was achieved. It was tested on large scale sensor nodes. An intelligent recognition model was designed to connect the objects via a decision tree. It was tested on the remote control indoor farming environment. Initially, the states of the plant and grass were analyzed using connected sensors. All parameters related to the farming fields were studied and then the plants were classified [34].

III. RESEARCH METHODOLOGY

This section presents the working model of an enhanced k-Nearest Neighbor to detect the malicious node in VANETs. The primitives of the algorithm are explained as follows:

3.1 Adhoc On Distance Vector (AODV) Routing Protocols

AODV routing protocols are a type of reactive protocol. When the packets initiate the transmission process, then the appropriate routing path is selected. The below fig. 2 presents the message communication process in AODV protocol. The deployed nodes are monitored by sending hello messages. Active nodes in the network reply back to hello messages based on their availability. These messages are communicated periodically in a network. If any node fails to reply back, then the behaviour of the node is monitored and the communication link is disconnected. Consider a scenario, the source node has a packet to transmit to an unknown destination node, then the source node broadcasts a Route Request (RREQ) packet to all nodes in the network. Active nodes reply back to the RREQ packets by acknowledging with Route Reply (RREP) packets. Here, RREP packets, unicast model i.e hop by hop analysis takes place. When RREP packets initiate to transmit, then the routing path is formed by all intermediate nodes. An appropriate source node monitors the formed route path and then the

DOI: 10.48175/IJARSCT-3390

data transmission process begins. Here, nodes with a minimal hop count are considered as the shortest path. Each packet is embedded with the timer that assists the source and destination nodes, to maintain the current information about the active nodes using the routing table. If the route is idle for a long period, then the route is labeled as an 'invalid route'. In case, the valid route is in idle state, then the Route Error (RERR) message is broadcasted to all subordinate nodes. Again, re-initiates the route discovery process.

	Source Node	Intermediate node 1	Destination node
Hello	----> < ----	< --- ------ >	----> < ----
RREQ	----- >	------- >	
RREP	< ----	< ----	
Data	----> ----- >	---- > ----- >	----> ---- >
RERR	< -----	< ----	

Figure 2: Message exchange process in AODV protocols

3.2 VANET - Architecture

In a realistic environment, the VANET oriented applications are embedded with roadside sensors. Here, an equipped vehicle should have a WiFi card, and some on-board units (OBU). In this work, we have considered both Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication models. Likewise, Road Side Units (RSUs) are also installed and administered properly. It is assumed that the RSUs are not communicated directly with each other under a similar communication range. This decision is made to eliminate the vehicle's traffic. If there is no proper associativity among the network entities, then the information is not shared. Instead, an alert message is forwarded to all its subordinates.

3. 3 Working of k- Nearest Neighbor

Once the VANET architecture and its communication process are defined, then the enhanced k- Nearest Neighbor technique is employed for detecting the misbehaving nodes in the network. Initially, the trace files are collected, aligned, and coordinated with the AODV routing protocols and the VANET communication architecture.

A. Measurements of VANET Entities

The density of each vehicle is measured by its coordination with neighboring vehicles and their respective vehicle's identity ($Density_{Vehicle}$). As we know, each vehicle is equipped with the GPS, to know its present position which is given as, X_{pos}, Y_{pos}. The average traffic flow of each vehicle is computed as $Avg.Traf.Flow_{Vehicle}$. The traffic flow of neighboring vehicles is estimated as $AvgFlow_{neigh}$. Maximum speed ($Max_{speed}$and maximum density ($Max_{Density}$of the vehicles are calculated by using the below equation.

$$AvgSpeed_{own} = Max_{speed} \quad - \frac{Density_{vehicle}}{Max_{Density}} Max_{speed}$$

$$Trafficflow_{Vehicle} = AvgSpeed_{vehicle} * Density_{vehicle}$$

$$Avg.Traff.Flow_{vehicle} = \frac{1}{n}(\sum_{i=1}^{N-1} AvgFlow_{neigh} + Trafficflow_{vehicle}$$

B. Format of the Nessages

The vehicles continuously broadcast with the RREQ packets under the same interval until the required neighboring vehicles data is collected. Generally, the format of the message is given as,

$$RREQpackets_{sourceID.Avg.flow.Position}$$

Like the above message format, each vehicular node and its neighboring nodes are calculated.

C. Maintenance of Routing Tables

The messages are stored within their communication window that contains three table, neighboring tables, a routing table, and the position table. Here, the neighboring table stores the neighboring information, the routing table stores the request messages, and the position table stores the response messages. The lifespan of these tables is assessed by a Trusted Authority (TA) in each zone. Once the session ends, all the tables are then re-initiated. The current neighbor information is moved into the next session. By doing so, we shall eliminate the computational overheads and reduce the chance of information leaking to the attackers.

D. Misbehavior Node Detection Model:

The fig. 3 illustrates the workflow of the proposed k-nearest neighbor algorithm. The steps involved in enhanced k-nearest neighboring models are as follows:

1. Initialize the number of vehicles, RSUs and OBUs,
2. Initialize the Trusted Authority (TA)
3. Computing Euclidean Distance between the nodes.
4. Find the average traffic flow
5. Updating the neighboring table, routing table, and position table
6. Finding the nearest neighbor node for communication by continuously observing its behavior.
7. Finding the number of route requests taken by each node.
8. If any node violates the threshold value of route requests, then it is considered as misbehaving nodes
9. If the node satisfies the threshold value of route requests, then it is considered as a normal nodes.

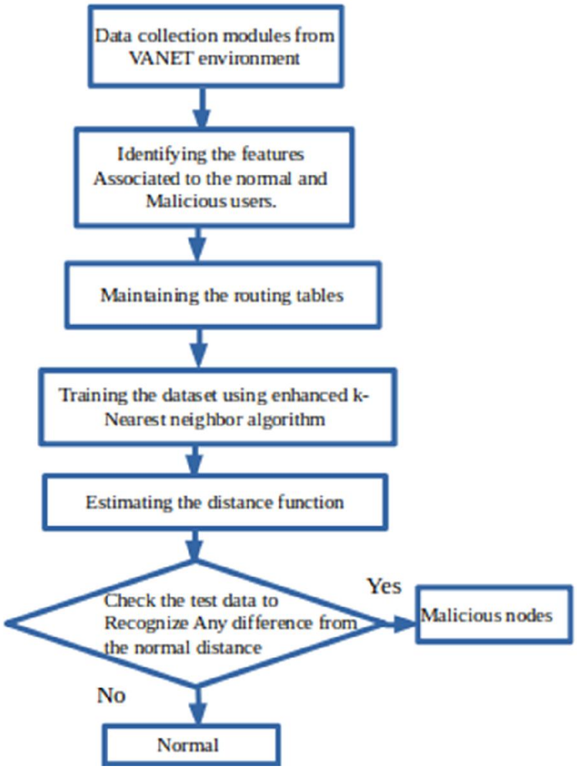

Data collection modules from VANET environment
Identifying the features Associated to the normal and Malicious users.
Maintaining the routing tables
Training the dataset using enhanced k-Nearest neighbor algorithm
Estimating the distance function
Check the test data to Recognize Any difference from the normal distance
Yes
Malicious nodes
No
Normal

Figure 3: Proposed workflow

DOI: 10.48175/IJARSCT-3390

Pseudocode for enhanced k- Nearest Neighbor classifier:

```
Input:   n*n distance matrix D, sensor nodes s
Output: The path taken by sensor nodes maintained in list A
for i←1 to n
do
visited[i]←false
visited[s]←true
current←s
for i←2 to n do
find the lowest element in row current and unmarked column k containing the element
current←j
visited[k]←true
Estimate the distance between the trained sensor data points and the testing sensor data points
Sort the distance and determine nearest neighbors based on the k-th minimum distance.
 Majority of the category of nearest neighbors as the prediction value of the query.
```

IV. Experimental Results and Analysis

This section presents the experimental analysis of the proposed enhanced k-nearest neighboring techniques. Here, NS2, a simulated programming language, is used for experimental purposes. Performance measures such as end-to-end delay, throughput, packet delivery function, and communication overhead are examined. The existing technique is taken from [35].

4.1 End-to-End Delay

It is defined as the time taken for successful transmission of packet delivery without any interruption. The below table & fig. 4 presents the computational analysis between existing and proposed framework.

Delay rate (kB)	Existing (ms)	Proposed (ms)
0	0	0
3	3.5	1
4	4.0	1.5

Table 1: End-to -End delay computational analysis in ms.

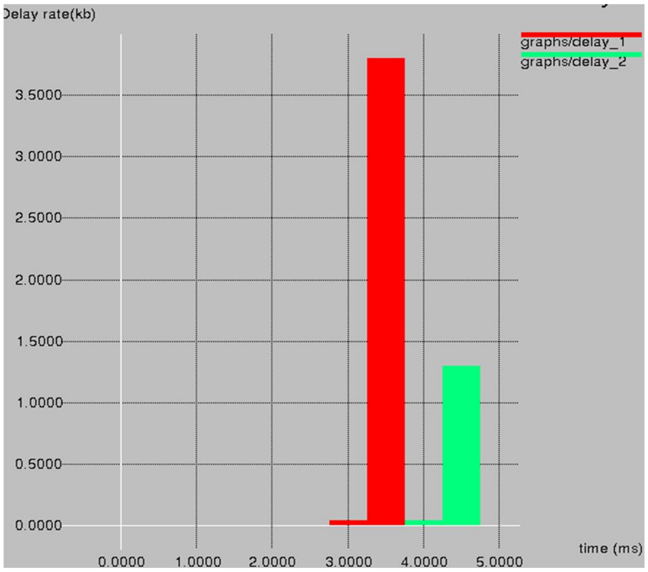


Figure 4: End-to -End delay -computational analysis in ms

4.2 Packet Delivery Function

It is defined as the time taken for transmitting the packets without any obstacles. It ensures the success rate of the proposed framework. The fig. 5 presents the computational analysis of the packet delivery rate.

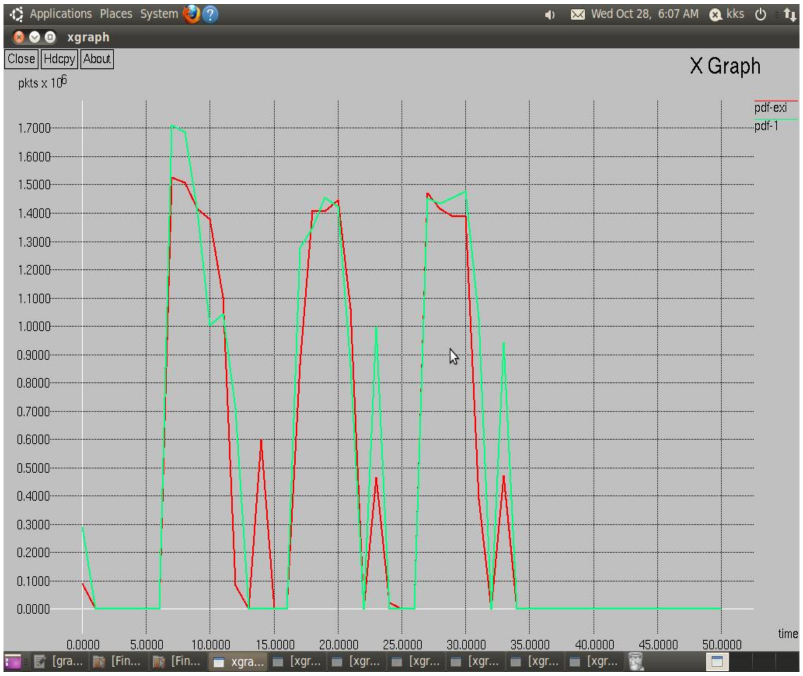


Figure 5: Computational analysis of the packet delivery rate

4.3 Throughput

It is defined as the amount of packets passed to the network in a given amount of time. The below table 2 & fig. 6 presents the computational analysis of the throughput rate.

Table 2: Computational analysis of the throughput rate

Time (ms)	Existing	Proposed
0	0	0
20	90000	90000
30	110000	160000
40	150	800
45	130	180
50	180	150
60	30	50

DOI: 10.48175/IJARSCT-3390

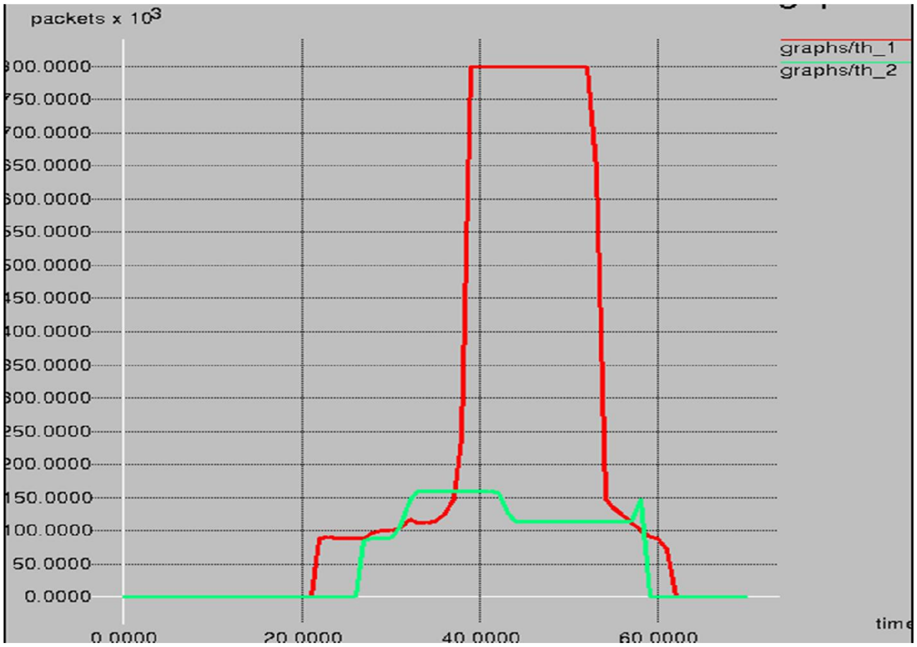


Figure 6: Computational analysis of the throughput rate

4.4 Communication Overhead

It is defined as the computational load taken, when the size of the node increases. The fig. 7 represents the computational analysis of the communication overhead. It is inferred that the proposed techniques eliminate the vehicles with malicious behavior and thus, overhead issue is significantly reduced.

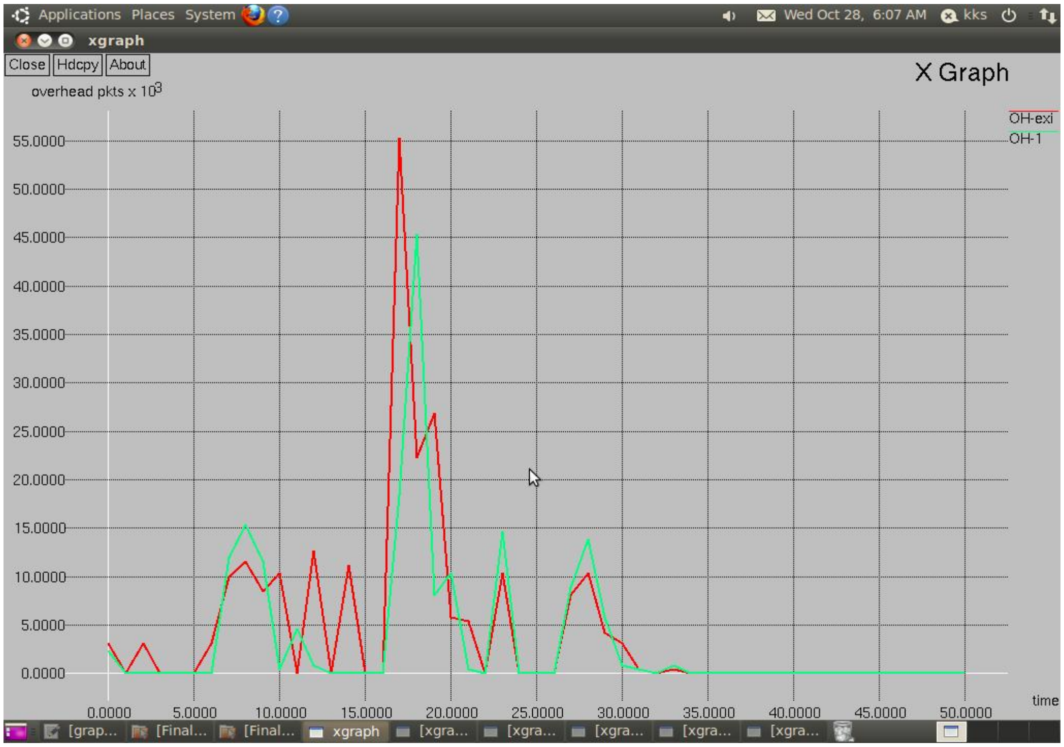


Figure 7: Computational analysis of the communication overhead.

DOI: 10.48175/IJARSCT-3390

4.5 Packet Loss Analysis

It is defined as the packet missed during the transmission process. It determines the reliability of the network. The fig. 8 presents the comparative analysis of the packet loss. Compared to the existing technique, the proposed technique has lowered the rate of packet loss by approaching the nearest vehicles.

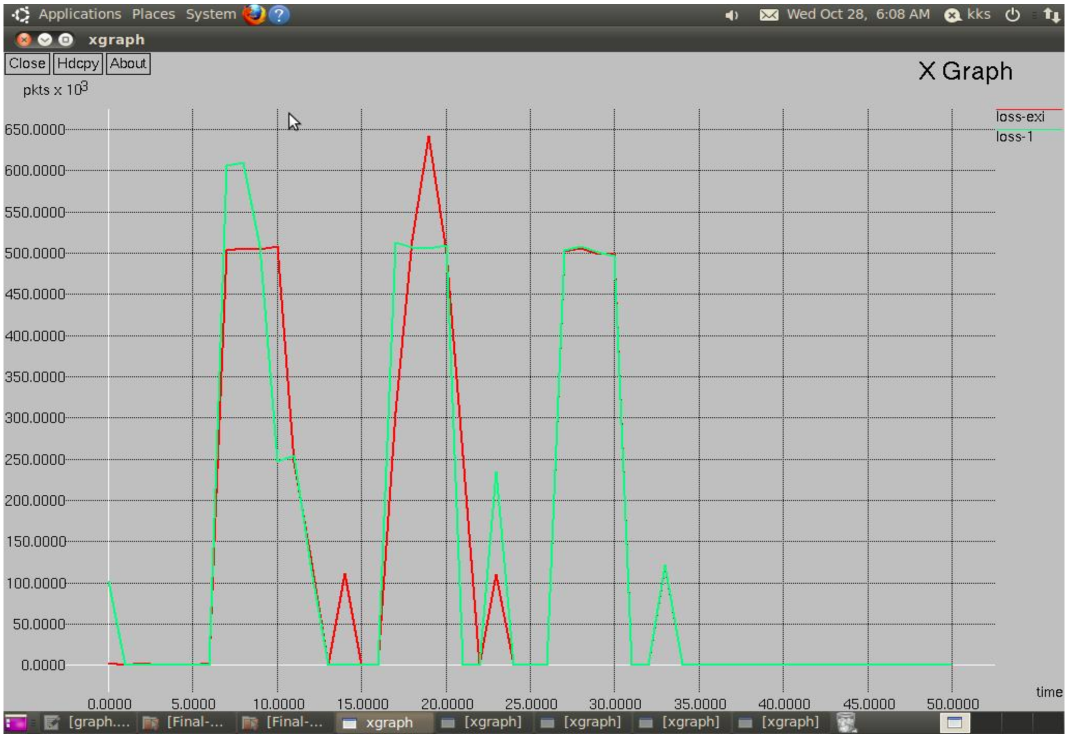


Figure 8: Comparative analysis of the packet loss.

V. Conclusion

In this paper, we proposed an enhanced k-Nearest Neighbor algorithm for an accurate detection of misbehaving nodes in VANETs. Initially, the vehicular nodes are deployed using AODV protocols. Then, the collected trace files are analyzed for predicting the behavior of the nodes. Here, three tables are maintained, viz, position, routing and neighboring tables. The lifespan of these tables are assessed by Trusted Authority (TA) in each zone. Once the session ends, all the tables are then re-initiated. The current neighbor information is moved into the next session. By doing so, we shall eliminate the computational overheads and reduce the chance of information leaking to the attackers. Finally, k- Nearest neighbor algorithms detected the attacks based on received number of route requests. If the observed value of route requests violates the threshold value of route requests, then it is considered a ‘malicious node’. The detected node was removed from the VANET network. Performance metrics like end-to-end delay, throughput, communication overhead and packet delivery are examined using NS2 programming language. It is observed that the increased packet delivery and throughput analysis proved the efficient detection process. Similar to lowered communication overhead and end-to-end-delay proved that the enhanced k- nearest neighbor has minimized the storage cost.

References

[1]. A. M. Abdullah, M. B. Alsolami, and M. H. Alyahya ‘‘Intrusion, detection of DoS attacks in WSNs using classification techniques,’’ J. Fundam. Appl. Sciences., vol. 10, no. 4, pp. 298–303, 2018.

[2]. N. Savarimuthu, ‘‘An investigation on security attacks in wireless sensor network,’’ J. Pure Appl. Math., vol. 119, no. 15, pp. 925–927, 2018.

[3]. G. Kaur and P. Agrawal, ‘‘Detection of LDoS attacks using variants of CUSUM and Shiryaev—Roberts’s algorithm,’’ in Proc. 4th Int. Conf. Parallel, Distrib. Grid Comput., Dec. 2017, pp. 363–369.

[4]. S. Patel and A. Sharma, ''The low-rate denial of service attack based comparative study of active queue management scheme,'' in Proc. 10th Int. Conf. Contemp. Comput. IEEE Comput. Soc., Aug. 2017, pp. 1–3.

[5]. X. Yang et al., ''A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems,'' IEEE Trans. Comput., vol. 64, no. 1, pp. 4–18, Jan. 2015.

[6]. N. Singh et al., ''Explicit query based detection and prevention techniques for DDOS in MANET,'' Int. J. Comput. Appl., vol. 53, no. 2, pp. 19–24, 2013.

[7]. D. Yin, L. Zhang, and K. Yang, ''A DDoS attack detection and mitigation with software-defined Internet of Things framework,'' IEEE Access, vol. 6, pp. 24694–24705, 2018.

[8]. A. K. Nain et al., ''A secure phase-encrypted IEEE 802.15.4 transceiver design,'' IEEE Trans. Comput., vol. 66, no. 8, pp. 1421–1427, Aug. 2017.

[9]. J. Lin et al., ''A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications,'' IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[10]. Samara G, Al-Salihy WAH, Sures R. Security issues and challenges of vehicular ad hoc networks (VANET). In: Proceedings of the second international conference on network applications, protocols and services; 2010.

[11]. Zhang Q, Almulla M, Ren Y, Boukerche A. An efficient certificate revocation validation scheme with k-means clustering for vehicular ad hoc networks. In: Proceedings of the IEEE symposium on computers and communications (ISCC); 2012.

[12]. Nowatkowski ME, Owen HL. Certificate revocation list distribution in VANETs using most pieces broadcast. In: Proceedings of the IEEE southeastCon; 2010. p. 238–41.

[13]. Papadimitratos P, Mezzour Gh, Hubaux J-P. Certificate revocation list distribution in vehicular communication systems. In: Proceedings of the 5th ACM international workshop on VehiculAr Inter-NETworking, VANET '08; 2008. p. 86–87.

[14]. Studer A, Shi E, Bai F, Perrig A. TACKing together efficient authentication, revocation, and privacy in VANETs. In: Proceedings of the 6th Annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks, SECON'09; 2009. p. 484–92.

[15]. Nowatkowski ME, Wolfgang JE, McManus C, Owen HL. The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS. In: Proceedings of the IEEE southeastCon; 2010.

[16]. Haas JJ, Hu Y-C, Laberteaux KP. Efficient certificate revocation list organization and distribution. In: Proceedings of the IEEE journal on selected areas in communications, 29; Mar. 2011. p. 594–604

[17]. Samara G, Al-Salihy WAH, Sures R. Security issues and challenges of vehicular ad hoc networks (VANET). In: Proceedings of the second international conference on network applications, protocols and services; 2010

[18]. Mallissery S, Pai MM M, Ajam N, Pai RM, Mouzna J. Transport and traffic rule violation monitoring service in ITS : a secured VANET cloud application. In: Proceedings of the 12th annual IEEE consumer communications and networking conference (CCNC); 2015

[19]. [19] Rajput U, Abbas F, Eun H, Oh H. A hybrid approach for efficient privacy preserving authentication in VANET. IEEE Access published in 2017;5:12014–30.

[20]. Martín-Fernández F, Caballero-Gil P, Caballero-Gil C. Managing certificate revocation in VANETs using hash trees and query frequencies. In: Proceedings of the 15th international conference on computer aided systems theory – EUROCAST. Springer; 2015. p. 57–63

[21]. Wasef A, Lu R, Lin X, Shen X. Complementing public key infrastructure to secure vehicular ad hoc networks. IEEE Wirel Commun 2010;17(5):22–8

[22]. T. D. S. Keerthi and P. Venkataram, ''Confirmation of wormhole attack in MANETs using honeypot,'' Comput. Secur., no. 76, pp. 32–49, Jul. 2018.

[23]. P. Liu et al., ''Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET,'' IEEE Access, vol. 6, pp. 20795–20806, 2018.

[24]. H. Chen et al., ''Design and performance evaluation of a multi-agent-based dynamic lifetime security scheme for AODV routing protocol,'' J. Netw. Comput. Appl., vol. 30, no. 1, pp. 145–166, 2007.

[25]. J. Han et al., ''Do you feel what i hear-enabling autonomous IoT device pairing using different sensor types,'' in Proc. IEEE Symp. Secur. Privacy (SP). San Francisco, CA, USA, Sep. 2018, pp. 836–852.

DOI: 10.48175/IJARSCT-3390

[26]. Huda, S., Miah, S., Yearwood, J., & Alyahya, S. (2018). A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network. Journal of Parallel and Distributed Computing, 120, 23-31

[27]. Zhang, H., Li, Y., Lv, Z., Sangaiah, A. K. & Huang, T. (2020). A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. IEEE/CAA Journal of Automatica Sinica, 7, 790–799.

[28]. Zhang, H., Li, Y., Lv, Z., Sangaiah, A. K. & Huang, T. (2020). A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. IEEE/CAA Journal of Automatica Sinica, 7, 790–799.

[29]. Qu, F., Zhang, J., Shao, Z., & Qi, S. (2017). An intrusion detection model based on deep belief network. In Proc. of ICNCC, 97-101.

[30]. Alom, Z., Bontupalli, V., & Taha, T.M. (2015). Intrusion detection using deep belief networks. In Proc. of IEEE NAECON, 339-344

[31]. Ding, Y., Chen, S., & Xu, J. (2016). Application of Deep Belief Networks for opcode based malware detection. In Proc. of IJCNN, 3901-3908

[32]. Erfani, S. M, Rajasegarar, S., Karunasekera, S., & Leckie, C. (2016). High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. Pattern Recognition, 58, 121-134.

[33]. M. Hasan, M. M. Islam, M. I. I. Zarif, M. Hashem, Attack and anomaly detection in iot sensors in iot sites using machine learning approaches, Internet of Things 7 (2019) 100059.

[34]. Zhang, H., Li, Y., Lv, Z., Sangaiah, A. K. & Huang, T. (2020). A real-time and ubiquitous network attack detection based on deep belief networks and support vector machines. IEEE/CAA Journal of Automatica Sinica, 7, 790–799.

[35]. Chunhua Zhang et al, “Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs”, IEEE access, 2017.

DOI: 10.48175/IJARSCT-3390