Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 03 Issue 01 - 2022 (January to June)

Page 56:61

Malicious Attacks Detection Using Trust Node Centric Weight Management Algorithm in Vehicular Platoon

Dr. Prakash Kumar Sarangi
Computer Science & Communication Engineering
Vardhaman College of Engineering Hyderabad
https://orcid.org/0000-0002-0070-1574?lang=en
prakashsarangi89@gmail.com

Article History

Received: 22 January 2022
Revised: 14 April 2022
Accepted: 19 May 2022

Abstract

For potential way of transmission people mostly use Vehicular Ad Hoc Networks (VANETs) by which they can generate secured consistent wireless communication networks (wagons, buses, traffic signs, cell phones, and additional devices). Even though they have these advantages, the network used for communication has to control vehicles that are unprotected to appropriate attack surface which could be make use of malignant attacks. In consideration with associated vehicles between trusts could enhance security while all active vehicles can create and proliferate that can be authentic, accurate also it could be content trusted inside the network. So, this paper propose a novel Node Centric Weight based Trust Management algorithm (NC-WTM) by considering badmouth attack. According to the performance study, the outputs of the NC-WTM are optimal in terms of precision (78%), recall (69.3%), F-score (60.4%), and accuracy (89%).

Keywords: Bad Mouth Attack; Platoon; Security; Trust Management; Vehicular Ad Hoc Network.

1 Introduction

The major concentration for humans is that they have interest in Communication. Therefore this result in constant effort has come into appropriate replacement from one communication channel through any other high speed communication in order to transmit and receive the information [1]. Those devices that are networked for communication are carried out through data link in group of hardware devices that can interchange data through computer networks. These links can be wired or wireless in between those nodes has been fixed [2].Since this network lacks infrastructure, its nodes can connect to mobile networks like Wi-Fi. VANET is the MANET application. The VANET is a wireless ad hoc network in which moving cars would function as mobile nodes and can link to one another using DSRC. IEEE 802.11p for Intra Ventricular Communication is the protocol anticipated for WAVEs (IVC). I2V, V2I, and V2V communication schemes can all be connected by this network [3].

2 Literature Review

The techniques that have already been developed and contributed by many researchers in the fields of VANET as well as vehicular platooning are covered in this part. Work [4] recommended a data-oriented trust management pattern utilizes trust measurements and a convent secure elements trust to

distinguish whether they got messages are genuine, or false data to create congestion in channel. In ([5], a Real-time Message Content Validation (RMCV) system remains projected which depends continuously with the data arranged trust method. Work [6] highlighted potential residual effects, such as using a lower time gap when driving physically after having used platooning, as well as the probability of worse human performance when guiding robotized frameworks than when driving physically.The pioneer subsequent-centered cooperative adaptive crusie control framework was created in [7]. Work [8-10] looked at drive-through Internet uplink performance under error-prone circumstances. A 4-D Markov tie was also kept in mind to illustrate the useful retransmission behaviour in the anticipated scheme.

3 Proposed Methodology

The proposed trust evaluation model, known as NC-WTM, is employed in VANET as an efficient mechanism, however there is no integration of the data and strategy provided by RSU, which is nearby and is shown in Fig 1.First, the sender node has identified the estimation for trustworthiness. It is carried out based on prior interactions, and adjacent automobiles have received a recommendation. When the centre node calculates trust, the data received is calculated in three stages: (1) the quality of the data, (2) the ability of each node to deliver messages, and (3) initial neighbour opinions. The data of the sender node is established once both of nodes in centreare evaluated. If not, data will not be accepted by the evaluator node.

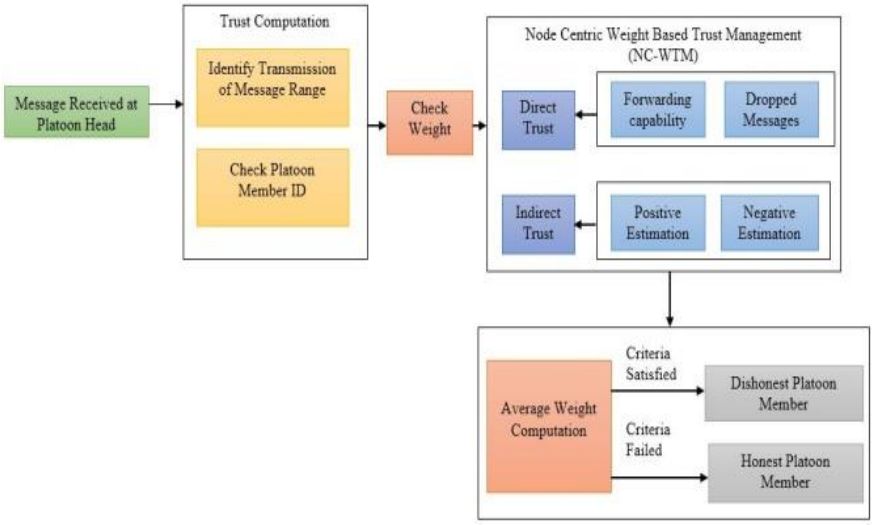

Fig. 1 Block Diagram of Proposed Methodology

Additionally, it includes the ID and location details for the nearby car. The arrival angle of CTB messages has been used to assess message arrival, allowing the source vehicle to estimate all mutual inter-vehicle distances between nearby vehicles. When several vehicles are relatively close to one another and their distance is below a threshold rate (in our study, Dmin assumes 15 km), they can be regarded as being accessible on the same platoon. The RSU identifies many platoons, chooses one of them as platoon commander, and only sends data messages to that one vehicle at each cluster.

3.1 Trust Model

Since there is uncertainty in relation to each other at first, the initial stage has been taken into consideration for new cars before communication with the network. Vehicles are not permitted to move in homogenous VANET structures without the consent of the platoon chiefs. However, they are free to move and connect to other lanes while waiting for the nearby neighbours to estimate their trust levels.

The trust computation is computed via Algorithm 1. Algorithm 2's harmful propensity and total average weight are used to discover malicious platoon members. The vehicle weights and direct and indirect trust computation are used to calculate the Algorithm 3 Node Centric Weight based Trust Management algorithm.

3.2 Proposed Node Centric Weight Based Trust Management Algorithm (NC-WTM)

According to node authority, nodes have been divided into three phases: high phase (marked by H), medium phase (indicated by M), and low phase (shown by L) (indicated by L).

$$W(N) = \begin{Bmatrix} 1, N = H \\ 0.7, N = M \\ 0.5, N = L \end{Bmatrix} \quad (1)$$

$$A^{x,y}(TotAvg) = \frac{U\,x,y\,(w)}{Ny(x)} \quad (2)$$

Due to the close relationship between a vehicle's malevolent impulse and the typical load of data that isn't forwarded, vehicle "x" can calculate the maliciousness of the vehicle by,

$$F\ y(w) = (U\,x,y\,(w) - S\,x,y\,(w)) / (Ny(x) - My(x)) \quad (3)$$

The platoon chief assesses the trust by examining the contents of the established data after the attack has been discovered in the network. Two methods of trust computation are obtained and are detailed below as a result of the subsequent information being transmitted to target either directly or via intermediate neighbours.

$$DDR = \sum_{i=1}^{n} \frac{A*MD}{(C*MD)+(D*DMC)} \quad (4)$$

$$\text{Direct trust (Dir)=avg(DDR)} \quad (5)$$

C represents car's weight when communicating data to another vehicle. Session of lost messages at vehicle is known as DMC. MD for the genuine automobiles, which are higher in reality as fewer messages are still being dropped at the vehicle. The weight of nodes that are unable to transmit and segment messages is represented by D.

$$\text{Indirect trust (IDir)} = [(\frac{A}{A+B} * \sum_{i=1}^{x} Y) + (\frac{A}{A+B} * \sum_{i=1}^{x} Z)]^{\frac{1}{x}} \quad (6)$$

Whereas,

The vehicle sending messages to other vehicles has a weight, A. B stands for the vehicle's overall weight, which prevents it from sending and receiving communications. The symbol x denotes a unicast message between neighbours.

4 Performance Analysis

In this part, our method is compared against the current method using a variety of parametric criteria, including precision, recall, F-Score, and accuracy. The graphs provided here demonstrate that our NC-WTM approach is more effective than the currently used methods. Here, we've selected Network Simulator 2 version 2.29 for simulation purposes. Table 1 details the general simulation environment for the suggested NC-WTM.

Table 1 Simulation Parameter

Parameter	Value
Area estimated for simulation	800m×800m
Number of lanes	20
Number of platoon members	700
Number of platoon head	20
Node placement	random
Number of malicious nodes	425
Number of RSUs	25
Simulation time	500s
Channel type	wireless

$$\text{Precision}=\frac{p(ln)}{p(mn)+p(ln)} \quad (7)$$

The likelihood value that the genuine vehicle will identify any vehicle as malicious is represented by p (ln). The cumulative likelihood that the particular malicious vehicle will identify the vehicle as being malicious is represented by p(mn).

$$\text{Rec} = \frac{P(ln)}{P(mn)+P(ln)} \quad (8)$$

$$\text{F(s)}= 2*\frac{Prec*Rec}{Prec+Rec} \quad (9)$$

Root mean square of expected trust calculated for all cars is another method for predicting TCE.

$$TCE=MSE[\frac{wrongly\ sent\ messages}{total\ number\ of\ messages\ in\ particular\ lane}] \quad (10)$$

$$E(delay)= \text{ queuing time + transmission time} \quad (11)$$

$$Avg(link)= Avg\ distance[\frac{source\ vehicle}{destination\ vehicle}] \quad (12)$$

Table 1 Comparison of Existing and Proposed NC-WTM

Node %	Attack Resistant Trust Management Scheme (ART) [19]	A Robust and Privacy-Preserving Reputation Management Scheme (RPRep) [29]	Node Centric Weight based Trust Management Algorithm (NC-WTM)(Proposed)
Accuracy	74%	84%	89%
Precision	71%	68%	78%
Recall	56%	43%	69.3%
F-score	56.2%	43.2%	60.4%
Trust Computation Error	70.6%	67.2%	78%
End to end delay	70.6%	78%	67.2%
Average link duration	56.2%	43.2%	69.2%

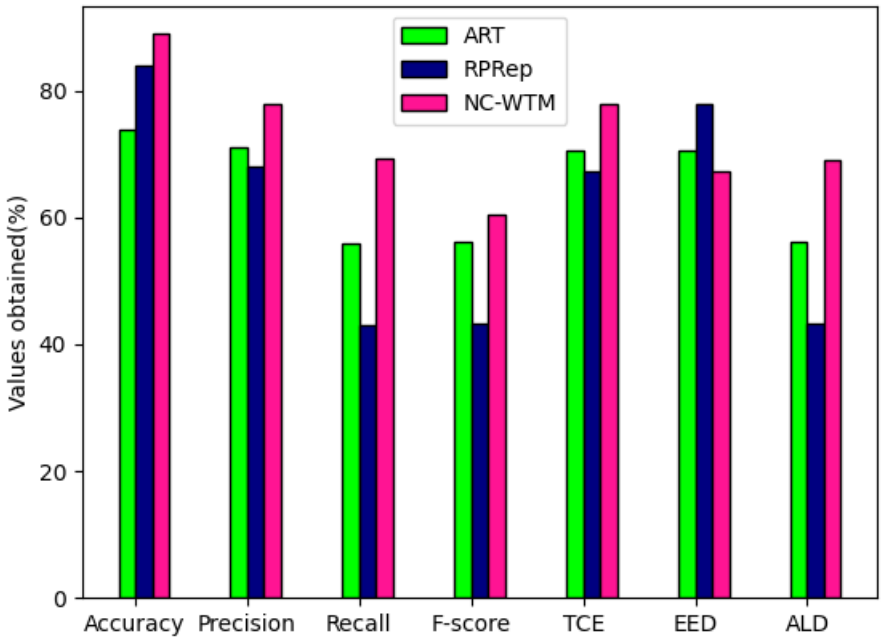

Figure 1: Comparison

Table 1 and figure 1 shows that suggested NC-WTM has a higher precision value of 78%, a higher recall value of 60.4%, and an F-score value of 89%. Precision in ART and RPRep is very low. The suggested NC-WTM technique offers the least amount of calculation error and end-to-end delay while also lengthening average links.

5 Conclusion

In this paper, we presented NC-WTM model in order to improve the overall platoon security by rapidly identifying and revoking deceitful vehicles along with its created message. Based on it, a network is created with badmouth attacks and put proposed algorithm in advanced to evaluate dependability of the data of each vehicle. The investigation designates that, node-centric trust method

is simple enough to encounter the requisite for fast trustworthiness assessment. Suggested NC-WTM is an attack-resistant trust method that offers excellent accuracy in identifying trusted information in the presence of negative word-of-mouth attacks. RPRep and an ART trust model are also used to assess NC-performance, WTM's and it is clear that NC-WTM outperforms them both in terms of obtaining high precision, recall, and F-score. Focus of future study is to create a resource allocation system that will result in high-quality platoon service.

References

[1] Farivar, F., Haghighi, M. S., Jolfaei, A., &Alazab, M. (2019). Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. *IEEE transactions on industrial informatics*, *16*(4), 2716-2725.

[2] Wu, M., Song, Z., & Moon, Y. B. (2019). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *Journal of intelligent manufacturing*, *30*(3), 1111-1123.

[3] Arif M, Wang G &Balas V. E (2018). Secure VANETs: trusted communication scheme between vehicles and infrastructure based on fog computing. Stud. Inform. Control. 27(2): 235-24

[4] O. Altintas, F. Dressler, F. Hagenauer, M. Matsumoto, M. Sepulcre, & C. Sommery (2015). Making cars a main ict resource in smart cities. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). pp.582-587.

[5] D. Patel, M. Faisal, P. Batavia, S. Makhija, & M. Mani (2016). Overview of routing protocols in vanet. International Journal of Computer Applications.136(9):4-7.

[6] D. Jia, K. Lu, J. Wang, X. Zhang, & X. Shen (2015). A survey on platoon based vehicular cyber-physical systems. IEEE communications surveys & tutorials. 18(1):263-284.

[7] M. Segata, B. Bloessl, S. Joerer, C. Sommer, M. Gerla, R. L. Cigno, & F. Dressler (2015). Toward communication strategies for platooning: Simulative and experimental evaluation. IEEE Transactions on Vehicular Technology. 64(12):5411-5423.

[8] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, & K. Levitt (2015).Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine. 53(6):126-132.

[9] Dong, Y., Zhang, Y., Ma, H., Wu, Q., Liu, Q., Wang, K., & Wang, W. (2018). An adaptive system for detecting malicious queries in web attacks. *Science China Information Sciences*, *61*(3), 1-16.

[10] Peng, C., Sun, H., Yang, M., & Wang, Y. L. (2019). A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(8), 1554-1569.