Vehicular ADHOC Network Based Safety Improvement

M. Karpagam¹, M. Shyam Kumar¹, A Monikavishnuvarthini¹, M. Sowmiya¹
¹Department of Electronics and communication, Sri Krishna College Of Engineering and Technology, Coimbatore, India
karpagam@skcet.ac.in, 19epae002@skcet.ac.in, 19epcm001@skcet.ac.in, 19epcm002@skcet.ac.in

Abstract. As the development of processing power and communication speed increasing the possibilities of many thing which where thought impossible things are possible like communication between vehicles often referred as VANET -Vehicular networking. The possibilities of intruders even like even they can bypass through normal firewalls in industries now we have a problem in our VANET as the rate of speed increases with increase in processing speed it gives a good way to manipulate and get away details very fast. So we want ensure the robustness of our system, starting from the dashboard to the server. I had used the guidelines for modelling a application that will be used in dashboard in way that it will not provide any access to unauthorised data. I had used many technologies from traditional to implemented modified method to get accurate results with less nodes and less bandwidth. As we are working on a real time network here speed of decision making should be high with accuracy. We are going to discuss about practical system setup.

1. Introduction

Development of technology is like knife with two sides we want to be safe from same technology that we use to make good stuffs, as it is also available for all, few use them for bending the technologies to use it or to use the flaws in the system, often referred as bugs [1]. We are going the build a system with less possibilities to be bended and to improve the accuracy of the trust cascading with less number of node and fast prediction as in old method if we predicting with less number of data there will be possibilities of trusting false message and acting according to it may cause minimum of small traffic issue to maximum of chaos(an accident) and if the vehicle waits for more data for more perfecting the message then there will be no time for reacting to message this may also cause issue. We are going to use the CA getting the certificate of the vehicle from the RSU updated often with timestamp to avoid use of old certificate usage [2]. We are going to introduce a system that maintains the on/off status of vehicle with MAC address this may avoid MAC address duplication with MAC spoofing as it can pave a path for normal to be accused for malicious message passing or using a highly trusted vehicle CA for passing wrong message that can be trusted by all as the algorithm increase the trust of message with trust worthiness of a vehicle with its CA certificate

Eg: case 1:
if $\sum(C(E^+)) < \sum(C(E^-))$: 
return False
(no accident or obstacle road is clear to go and it was a false message)
case 2:
if $\sum(C(E^+)) > \sum(C(E^-))$:
return True
(accident or obstacle in the path so reduce speed)
Σ(C(E+)- total of vehicles accepting

C – trust value of the vehicle
E+ – Accepting issue

this means according to majority voting we will get result which is highly influenced by trust certificate of each of the vehicle so there will be flaw in result calculating so we need to prevent duplication or identity theft for avoiding false accuse also [3]. We had introduced a buffer time for the new vehicles and at this time they can use their trust certificate but will along with a warning as default trust value not verified . So this allows drives a warning but this should not affect the calculation as all the cars will have this as a new car and if we make them dummy then they affect the whole system and the mathematical design will not work correctly as the new driver can also have a valuable information to avoid accident in correct scenario [4]. The main motive of this paper is we need to validate message but the time of validating should not grab their time till the end as after though the system gave a validated result they will not have time for reacting to it and the whole idea will become waste as the vehicles are mobile and we need to consider that they will be travelling in independent speed so we want take speed into consideration and we want to calculate the distance between vehicle that messaged us and divide it with speed and so we can get the time so we can divide it in two one for validating and other half for reacting. Recommended the validating speed should be less than reaction [5]

Speed as reaction is done by human which needs more time than computer calculating and the extra time can also help them with extra time for observing the situation themselves. We use MV(Majority voting) and also we can have the accidental car to transmit a key which help us in increasing trust value. The concept is increase in resource decrease the time of verification [6].

2. Security measure starts from the dashboard:
The dashboard is the first weapon for the beginner level to expert level intruder [7]. According to guidelines for creating a dashboard with less ability to hack will start with the options available for the person if the dashboard have option like enter your name in the dashboard to get details from the database to check then the hacker use their knowledge in the language to make the database to fetch a name by itself from the database this can lead to identity theft so the main advise for designing frontend like dashboard is to use graphical button to the extend which you can use as they come under our limitation if control we are giving to the dashboard user, if this is secure then the first level of security is secure [8]. I had designed a small dashboard with options to perform which works on background Python code

3. The dashboard:

Figure 1. Dashboard
Here in the above Figure 1 we had give only button options to the user and a display [9]. If we are given with the blacklist to list and whitelist to list then we want to block all in blacklist of a system like ports and in white list we want to list the only port that is necessary as port are the main source of attack and avoid blacklisting few use white list to enable necessary things and block all other than the one in whitelist [10].

To block all the services the server command is:

\[
\text{deny all/any} \\
\text{deny- will be denying the following} \\
\text{all- all sorts of connection} \\
\text{any/any – any source IP or port to any destination IP or port}
\]

Next we can add the services to be whitelisted

4. Prevention of time delay in verification with accident car message:

4.1. Accidental Car beacon:

The accident car will transmit emergency signal along with a unique key that identifies the car and the car which tries to message all other behind him about the issue catch the key and add it to his message this adds weightage to the message, there may be a situation where the driver cant on the beacon, but if it is on then the verification process can be made less time consuming [11]. The RSU can also help us in this situation as the vehicle which is now in damaged would have crossed the nearest RSU this can help us in verifying the car was in same spot or a fake message with previously catch key from an accident. With our old formula for comparison we can add this key a element and this will be present only there is a accident, so found only on the E+ side this will make E+ extra weightage and so verification can be made with this as additional comparison too. The scope of main paper and this modified paper both based on straight road and complex road like this is out of the scope of the paper [12]. Figures 2 and 3 shows the trail.

**Figure 2. Linear trail**

**Figure 3. Closed complex trail**
the graph of a single node coming and stopping due to message and after moves from the place as shown in Figure 4

5. Case Study
If no beacon and we compare $\Sigma(C(E^+)$ and $\Sigma(C(E^-)$ if both have one car each saying opposite suggestions a and they both are new car so having trust value full in this situation nothing will verify the message easily in time so they need to wait for another car to message about the situation and add to my of the one category. This waiting time put pressure on the driver and this also makes the possibility of escaping from a bad situation with less time to be slim. So when we add a message option by accident car and which can be caught by the car which want to spread the message ,when it sends the message the unique key of the accident car helps way more to in increasing the reaction speed as the verification speed took very less time $B(C(E^+)$ - 'B' represents the message from the accident car. So a vehicle which send a message will have the code and this will be also transferred to all other cars and they too will transfer the same message with code as echo [13-16].so if $\Sigma(C(E^+)$ = $\Sigma(C(E^-)$ the there will be a verification delay that might cause zero verification time so we can use less number of resource to get verification easily as there will be increase in the weightage in side of the accident occurrence make the cars to accept the accident fast, the first graph show the delay took by three cars for waiting many cars to send data and after they want to process them and that will add a delay in whole thought we can get accurate output the time for reacting according output will be lost. Figures 5 and 6 shows the graph.

1.Old method for three cars to judge in period of time

\[ \begin{align*}
\text{i) Graph for number of vehicle(Y-axis) vs time(X-axis)} \\
\text{Methods used for trust building normally uses} \\
\bullet \text{Majority voting method(MV)} \\
\bullet \text{Certificate Authorisation copy(CA)} \\
\bullet \text{Trust Certificate(TC)} \\
\bullet \text{Entity Oriented data}
\end{align*} \]
\( \Sigma(C(E^+)) - \) Total messages for accident occurred

\( \Sigma(C(E^-)) - \) Total messages for accident not occurred/cleared

Comparing the result \( \Sigma(C(E^+)) < \Sigma(C(E^-)) \) and we can verify and the comparison justify the result but if the counts are same then the verification will happen for infinite amount of time, especially if all are new cars and starting the drive and there was a situation, so we want the guidance also from RSU the unit that communicate with all vehicles to get detail from accident car or nearby car use its ID to transfer along with message for fast judging which I referred as constant B, so the equation will be for a single car

\( B(C(E^+)) \) so when we get total with the message from accident car though the trust value is same the group with accident cleared will not have extra weightage to prove their part this disappears the confusion and enables faster verification and more reaction time

\( \Sigma(C(E^+)) - \) Total messages for accident occurred

\( \Sigma(C(E^-)) - \) Total messages for accident not occurred/cleared

Comparing the result \( \Sigma(C(E^+)) < \Sigma(C(E^-)) \) and we can verify and the comparison justify the result but if the counts are same then the verification will happen for infinite amount of time, especially if all are new cars and starting the drive and there was a situation, so we want the guidance also from RSU the unit that communicate with all vehicles to get detail from accident car or nearby car use its ID to transfer along with message for fast judging which I referred as constant B, so the equation will be for a single car

\( B(C(E^+)) \) so when we get total with the message from accident car though the trust value is same the group with accident cleared will not have extra weightage to prove their part this disappears the confusion and enables faster verification and more reaction time

\[ \Sigma(B(C(E^+))) > \Sigma(C(E^-)) \]

Modified method uses less time to verify and have more reaction time

![Figure 6. Graph](image)

ii) Graph for number of vehicle (Y-axis) vs time (X-axis)

Method used for verifying

- Modified Majority voting (MV)
- Certificate Authorisation copy (CA)
- Trust Certificate (TC)
- Road Side Unit (RSU)
- Onboard Unit (OU)

6. Conclusion

We have network constructions. Three aspects of vehicle ADHOC networks research issues: route, security, and privacy, and applications are discussed. We also focused on vehicle ADHOC networks
research methods and other travel models and simulator tools. Finally, an analysis of vehicle ADHOC networks research challenges and future practices were done. This paper introduces an automotive communication network from a research perspective which incorporates basic constructions, critical research issues and standard to vehicle ADHOC networks and research methods which provides a complete reference.

References

[1] M. Karpagam, *Analysis of EMCA, EFNR and HEFRN Algorithms in wireless sensor Networks*, Applied Mechanics and Materials, **550** May 2014, pp 102 - 109

[2] VanDung Nguyen; Thant Zin Oo; Pham Chuan; Choong Seon Hong *An Efficient Time Slot Acquisition on the Hybrid TDMA/CSMA Multichannel MAC in VANETs* Vol: **20**, Issue: 5, 2016

[3] H. Hu, R. Lu, Z. Zhang, and J. Shao, *REPLACE: a reliable trust-based platoon service recommendation scheme in VANET*, IEEE Trans. Veh. Technol., **66**(2), pp. 1786-1797, Feb. 2017.

[4] M. Karpagam, *ACO enhanced RILoD-IN scheme for WSN*, 2020 International Conference on Smart Electronics and Communication, pp 744 – 749.

[5] J. Li, H. Lu, and M. Guizani, *ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs*, IEEE Trans. Parall. Distr., **26**(4), pp. 938-948, Apr. 2015

[6] M. Karpagam, *Underwater Wireless Sensor Network Based Marine Environment Monitoring System*, International Journal of Oceans and Oceanography, volume- 13, Number 2, 2019.

[7] J. Li, H. Lu, and M. Guizani, *ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs*,

[8] Haldorai, A. Ramu, and S. Murugan, Social Aware Cognitive Radio Networks, Social Network Analytics for Contemporary Business Organizations, pp. 188–202. doi:10.4018/978-1-5225-5097-6.ch010

[9] R. Arulmurugan and H. Anandakumar, Region-based seed point cell segmentation and detection for biomedical image analysis, International Journal of Biomedical Engineering and Technology, vol. **27**, no. 4, p. 273, 2018

[10] F. F. Hassanzadeh and S. Valae, *Reliable broadcast of safety messages in vehicular ad hoc networks*, in Proc. 28th INFOCOM, 2009, pp. 226-234.

[11] M. Karpagam *Effective Queuing Model Based Bandwidth Allocation Scheme for Fair QoS Provisioning in LTE Systems*, Journal of Theoretical and Applied Information Technology, **65**(2), pp. 504 – 514

[12] O. K. Tonguz, N. Wisitpongphan, F. Bai, P. Mudadige and V. Sadekar, *Broadcasting in VANET*, Proc. IEEE INFOCOM MOVE Workshop 2007, Anchorage, USA, 2007

[13] F. Lyu, H. Zhu, H. Zhou, W. Xu, N. Zhang, M. Li, and X. Shen, *SS-MAC: A novel time slot-sharing MAC for safety messages broadcasting in VANETs*, IEEE Trans. Veh. Technol., **67**(4), pp. 3586-3597, Apr. 2018.

[14] O. A. Wahab, H. Otrok, and A. Mourad, *A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles*, Comput. Commun., **41**, pp. 43–54, Mar. 2014

[15] D. B. Rawat, B. B. Bista, G. Yan, and M. C. Weigle, *Securing vehicular ad-hoc networks against malicious drivers: A probabilistic approach*, in Proc. IEEE CISIS, Seoul, South Korea, Jun. 2011, pp. 146–151

[16] 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., **41**(3), pp. 407–420, May 2011.