Volume 6, Issue 12, December 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Adaptive Clustering Mechanism with Trust Enabled Data Propagation for Realization of Secure VANETs

Heena Goyal
CGC, Department of Information and Technology
Landran, Mohali, Punjab, India

Amitabh Sharma
CGC, Department of Information and Technology
Landran, Mohali, Punjab, India

Abstract— In this paper, the proposed model has been designed with the security model based upon the trust values for the establishment of the connection between the two vehicular nodes. The proposed model has been designed to provide the authentication level for the data being propagated during the decongestion mechanism based upon the trust factor level, which guide the data during the communications between the vehicular nodes. The proposed model has been aimed at resolving the issue related to the vehicular traffic decongestion mechanism. The proposed model is aimed at solving the issues related to the performance of the vehicular data propagation in the vehicular nodes. The proposed model also providing information about hurdle and collision and avoid collision. The result shows that the performance of purposed model is better than existing model.

Keywords: collision detection, collision avoidance, collision bypass, color vise data selection.

I. INTRODUCTION

Vehicular ad-hoc network (VANET) is Associate in nursing ad-hoc network that is recognized as a taxonomic group of the mobile ad-hoc network (MANAET). It is one amongst the auspicious approaches of the intelligent transit (ITS) [2]. VANET provides various methods like fast changes within the constellation, high quality, repeated or periodic portioning etc. transport ad-hoc network enable inter-vehicle communication to reinforce driving expertise and road safety [12]. Communication within the transport ad-hoc network depends on the transfer of messages between many nodes within the network. It helps to reinforce the protection, driving effectiveness and relief on the course for the travellers [1] within the transport network, the messages collected from alternative nodes create use of to create the foremost of the choices.

Still, a node could perform as malicious or stingy so as to require the like alternative transport nodes. Security of the VANET has been known as an enormous challenge. The applications of the VANET compromise with life crucial information and support the period communication to try it properly, it's essential to follow some security needs like integrity, non-repudiation, authentication and privacy across assaulters and malicious attacker nodes [4]. There are a unit the no. Of attacks like part, timing, illusion, DOS [10], Sybil that not solely influences the vehicles and deriver's privacy however additionally affects the traffic safety [1][13]. In some cases, it's going to ends up in loss of life to confirm the traffic safety the VANET wants some appropriate security techniques that may assure protection across distinct misbehaviours and malicious nodes that influence the protection of the VANET [5][7].

Information distribution within the VANET takes place through the joint behaviour of the transport nodes. The messages that area unit broadcast hold the essential info like road condition, holdup, inclemency condition, emergency break events and accidents notifications etc. Therefore, In this when message will be alter the result will go on risk. Hence it is necessary to concern with actus reus within the network. Generally , misbehavior will be indicated by actus reus.Thus, the detection of the misdeed and malicious nodes includes a misconducts i.e. greatly crucial plenty of labour has been lugged dead set determine the actus reus and malicious node within the transport ad-hoc network. Generally, the actus reus detection methods may be of 2 types: knowledge central and node central actus reus detection strategy [6] [8][9][11].

To spot the actus reus the information given by data centric theme will be broadcast between the nodes. It is fascinated by relationship among messages instead of the identities of single node. In the network , data given by every node will be determined and after that this data will be compared with data collected from alternative nodes. Therefore when any node will give some wrong information related to many events within the VANETs like wrong location, road conditions, faux traffic messages, faux emergency events, accidents etc. will be consider as misbehaving. And these type of behaviours can be set with knowledge central actus reus schemes [1] [3].

Non-centric techniques area unit accustomed characterize between the nodes victimization authentication. Digital signatures, security credentials area unit accustomed validate the node that transmittal the messages [3]. Such techniques area unit specialize in the node that transmittal the messages instead of the inforamtion transmits. Non-centric schemes may be any classified as activity and trust based mostly non-centric schemes. The node's behavior are watched for the work of activity techniques with metric which will helpful for determining the speed and efficiency of node works. Non –Centric techniques are based on trust that commonly choose the nodes by its behaviour. This behaviour will commonly access the habitual behaviour within the future [9].

Transport ad-hoc network have achieved plenty of concentration because it will improbably enhance the protection on the roads and therefore the driving conditions. Within the VANET, it is necessary to discover the actus reus because it may be dangerous. To create VANET more reliable and safe, number of problems that found in node central and knowledge central actus reus detection techniques will eliminate. When validation will be accept non-centric techniques may be increased by choosing the node as observer . To find the abnormal actus reus these techniques gives nice observations.Therefore this nice observation will help to create the choices earlier and properly for high speed computation and process hardware on board unit(OBU). For the results of short term actus reus some actus reus detection techniques are used.In knowledge central schemes, the actus reus is detected by victimization the protection alert messages, beacons etc. To reduce the overburden associated within the communication of the messages. It is observe that nobody actus reus find theme will detect all kinds of the actus reus expeditiously within the VANETs.

II. LITERATURE REVIEW

1. Ghaleb F. et.al. proposed "Security And Privacy Enhancement In VANETs Using Mobility Pattern"(2013).This paper is presenting a mobility pattern based misbehavior detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions (Misbehavior), such as modify, fabricate, drop the messages in addition to, impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse ordenial of the communications among VANET's nodes. Misbehavior in VANETs can be viewed two perspectives:(i) physical movement and (ii) information security perspectives. Anonymous Location-Aided Routing for MANET (ALARM) is used for vehicular network which relies on the location information and corresponding time. This paper includes algorithms by which the misbehavior can be detected

2. Samara G. et.al proposed "Security Analysis Of Vehicular Ad Hoc Network(VANET)"(2010). In this paper various type of security problems and challenges of VANET been analyzed and discussed; author of this paper also discuss a set of solution to solve these challenges and problems. According to this paper each vehicle has OBU(On Board Unit).this unit connects vehicles with RSU via DSRC. and another device is TPD(Tamper Proof Device),this device hold the vehicle secrets like keys, drivers identity, trip detail, route, speed etc. Various attacks discussed are DOS, Fabrication Attack, Alteration Attack, Replay Attack and various attackers are Selfish Driver, Malicious Attackers, Pranksters. According to this paper. Various vehicular network challenges are Mobility, Volatility, Privacy VS Authentication, Privacy VS Liability, Network Scalability and various security requirements are Authentication, Availability, Non repudiation, Privacy, Integrity , privacy, Confidentiality

3. Seuwou.P et.al. proposed " Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".He stated vanet as technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst themselves (V2V communications) and with road-side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range. In this paper he proposed various issues of effective security in VANET. He discussed various attacks in vanet , according to him the attacks are classified into two broad categories first one is physical attack which further occure due to two problems ,tamper proof device and event data recorder and another attack is logical attack which occure due to the virus , Trojan horse and protocol weak spot.

4. Qian.yi et.al. **proposed** "Performance evaluation of a secure MAC Protocol for vehicular network". In this paper he proposed an overview on a priority based secure MAC Protocol for vehicular networks and he assume that the MAC Protocol can achieve both QOS and security in vehicular networks. In this paper he proposed that the MAC Protocol is having massages with different priority for different application to access DSRC(Dedicated short range communication channel) chanel .The proposed secure MAC Protocol will use a part of IEEE 1609.2 .Security infrastructure including PKI and ECC, the secure communication message format of vehicular networks, and the priority based channel access according to the QOS requirement of the applications.

III. EXPERIMENTAL SETUP

The proposed scheme is specially proposed for wireless platform mesh networks. The wireless user nodes are battery operated devices, Hence, having limited power sources. The platform vehicular nodes or mesh networks sends data to the platform record management services via long distance wireless communication channels such as cellular networks or radio networks. The communication between the wireless body mesh and VANET based platform service passes from many insecure network ingress or egress points, where there is higher risk of the communication data being exposed to the hackers. To protect the communication we are proposing a novel key exchange methods based upon the randomized key generation and management policy as the major improvement for the diffie-hellman scheme.

Our scheme does not rely upon the key reversal or re-computational process, but is robust and rigid in nature, which does not allow any of the key guessing attacks. Such attacks do not let the vehicle device to become hostile to the hackers and do not expose any information to the hackers. **More over our algorithm also provide hazard related information to all nodes from RSU and to RSU from nodes**. Our key scheme has been described in detailed below:

Key Generation Policy: Key generation policy under the proposed model is using the following mathematical algorithmic flow to populate the key table which is saved and being exchanged between the user nodes in the working cluster.

Algorithm 1: Randomized Function to generate random number

1. A number is generated randomly by using expression with in a range of 0 to 3.
2. $f(x) = 3 * \int_{1}^{1000000} random * \frac{1}{3}$
3. Randomly use coordinates or number to make OTP.
4. Return OTP

Key Management Policy:

Algorithm 2: Proposed VANET based Multi-Level Authentication Protocol (Fig 4.2 VANET M-LAP)

1. The user nodes powers up
2. The vanet node start data sending process.
3. The Vanet node request the RSU for channel allotment
4. The key is send to Vanet node called verification key
5. After accepting this key a key called acknowledgement key is send back to RSU
6. After accepting acknowledgement key this key is verified by RSU by matching it with verification key
7. If it matched with verification key
   a. Vanet node is informed through acknowledgement to send data and counter is started
8. Else
   a. Vanet node is refused to send data .
9. When secure counter time will expired then steps from 4-8 is initiated again
10. These steps are repeated until communication ends.

Furthermore to receive the more important data one more algorithm is used in this proposed model by name packet priority visualization model.

Algorithm 3: Packet Priority Visualization Model

1) Obtain the priority data
2) Runt the iteration equals to the array size
   a. Give red color to the highest priority node
   b. Give orange color to second highest priority node
   c. Give green color to lowest priority node.
3) Check the node color which is sending data
4) Process the data according to color.
5) If in between communication to lower priority nodes a higher priority node come than first process the data coming from higher priority node.
6) Else
   a. Keep receiving from that node
7) Repeat these steps

IV. RESULTS

Delay

Fig 1 shows that the delay of existing work is 1.7sec and delay of proposed work is 1.3 sec. Which is less than existing work

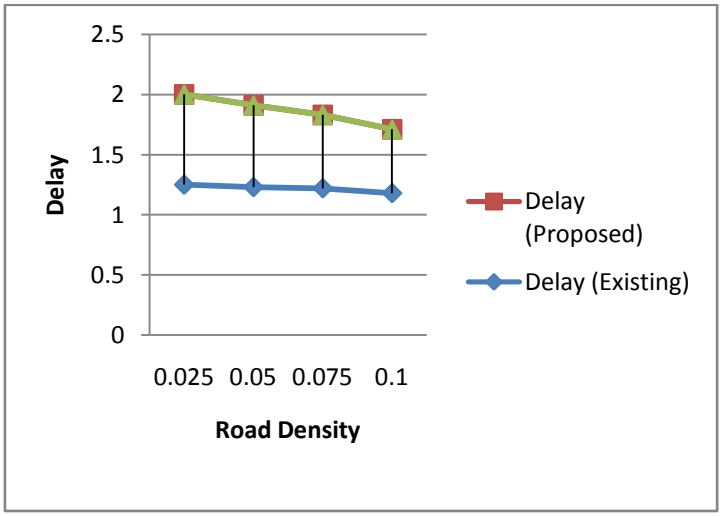

Figure 1 Delay

Number of Sent Packets

Fig 2 shows that the packet send of existing work is 271 and delay of proposed work is 284. Which is more than existing work

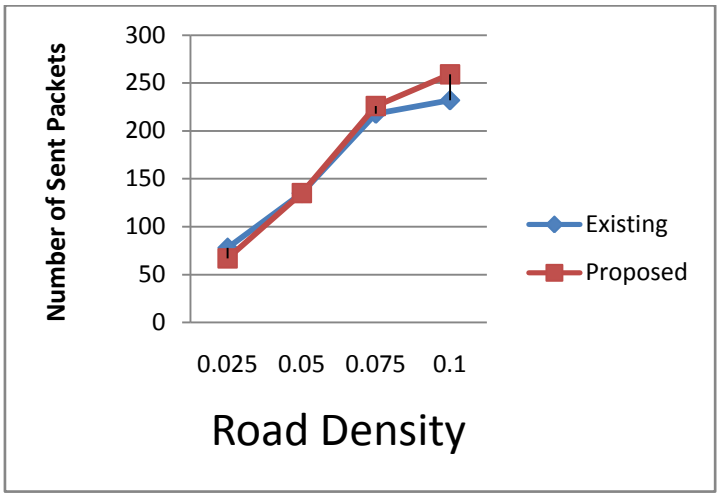

Figure 2 Number of Sent Packets

Accuracy Under Congestion Level

Fig 3 shows that the Accuracy Under Congestion Level is same as existing modela which is 100

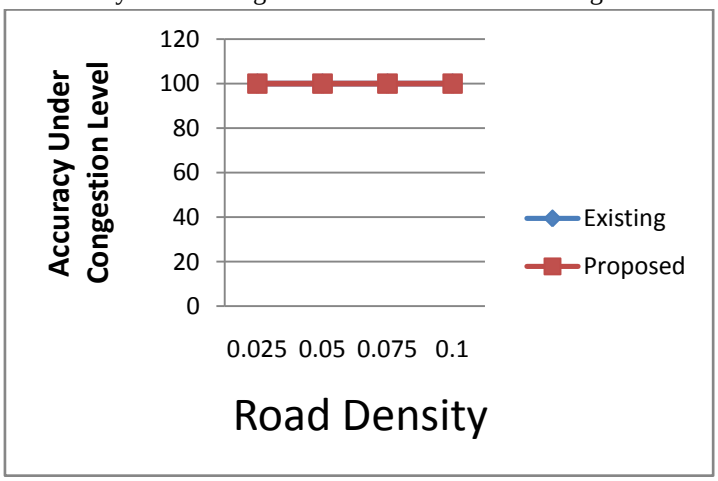

Figure 3 Accuracy Under Congestion Level

Accuracy Under Congestion Level with malicious nodes

Fig 4 shows that the Accuracy Under Congestion Level with malicious nodes is same as existing modela which is 100

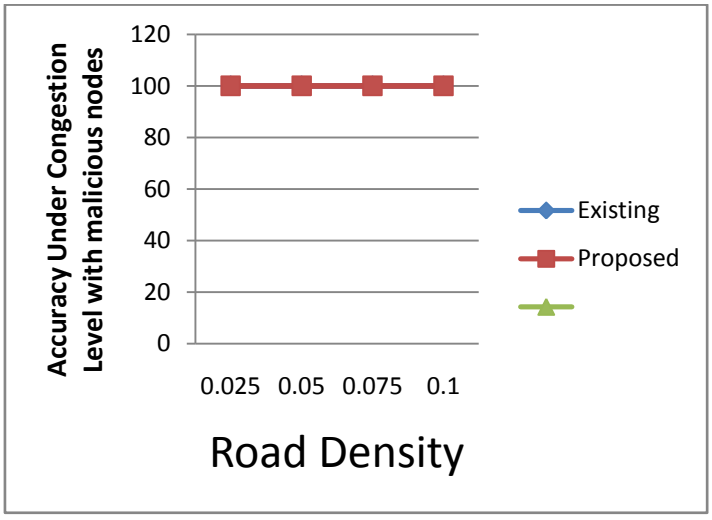

Figure 4 Accuracy Under Congestion Level with malicious nodes

V. CONCLUSION

We are proposing the new model to overcome congestion problem and it also detect and send information about hurdle and also avoid collision by sending information about prevention of collision. The proposed model will use a pre-shared trust information based trusted source evaluation with higher level of nodal integrity for selection of trusted source's data only. The proposed model will use the dynamic information exchange scheme for the highly trusted

communication between the VANET nodes and the region Road Side Unit using the concept of trusted source aware regional anomaly detectors (RADs) implemented over the RSUs. The RAD nodes will form the secure RAD network in order to control the security in the VANET clusters. The RAD nodes will be the nodes with the multiple connections with the other RAD nodes. The RAD nodes will be indulged into the well connected formation for the highly trusted data propagation methods along with the pre-propagation analysis to prevent the malicious data from entering the malicious data for exploitation. Then the results are compared with existing model. The result shows that the performance of purposed model is better than existing model.

REFERENCES

[1] Younes, MaramBani, and AzzedineBoukerche. "Scool: A secure traffic congestion control protocol for VANETs." In *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*, pp. 1960-1965. IEEE, 2015.

[2] Sepulcre, Miguel, Javier Gozalvez, OnurAltintas, and HarisKremo. "Integration of congestion and awareness control in vehicular networks." *Ad Hoc Networks* 37 (2016): 29-43.

[3] Ghaleb, Fuad A., M. A. Razzaque, and Ismail FauziIsnin. "Security and privacy enhancement in vanets using mobility pattern." In *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*, pp. 184-189. IEEE, 2013.

[4] Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." In *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*, pp. 393-398. IEEE, 2010.

[5] Seuwou, Patrice, Dilip Patel, Dave Protheroe, and George Ubakanma. "Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs)." In *Road Transport Information and Control (RTIC 2012), IET and ITS Conference on*, pp. 1-6. IET, 2012.

[6] Javed, Muhammad A., and Jamil Y. Khan. "A geocasting technique in an IEEE802. 11p based vehicular ad hoc network for road traffic management." In*AustralasianTelecommunication Networks and Applications Conference (ATNAC), 2011*, pp. 1-6. IEEE, 2011.

[7] Hung, Chia-Chen, Hope Chan, and EH-K. Wu. "Mobility pattern aware routing for heterogeneous vehicular networks." In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pp. 2200-2205. IEEE, 2008.

[8] Dias, João A., João N. Isento, Vasco NGJ Soares, FaridFarahmand, and Joel JPC Rodrigues. "Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks." In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pp. 51-55. IEEE, 2011.

[9] Moser, Steffen, Simon Eckert, and Frank Slomka. "An approach for the integration of smart antennas in the design and simulation of vehicular ad-hoc networks." In *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 36-41. IEEE, 2012.

[10] Sumra, Irshad Ahmed, HalabiHasbullah, J. A. Manan, MohsanIftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. "Trust levels in peer-to-peer (P2P) vehicular network." In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pp. 708-714. IEEE, 2011.

[11] Sumra, Irshad Ahmed, HalabiHasbullah, and J-L. A. Manan. "VANET security research and development ecosystem." In *National Postgraduate Conference (NPC), 2011*, pp. 1-4. IEEE, 2011.

[12] Chen, Lu, Hongbo Tang, and Junfei Wang. "Analysis of VANET security based on routing protocol information." In *Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on*, pp. 134-138. IEEE, 2013.

[13] Khabazian, Mehdi, and M. K. Mehmet Ali. "A performance modeling of vehicular ad hoc networks (VANETs)." In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 4177-4182. IEEE, 2007.

[14] Qian, Yi, Kejie Lu, and Nader Moayeri. "Performance evaluation of a secure MAC protocol for vehicular networks." In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1-6. IEEE, 2008.

