MAR_Worm: Secure and Efficient Wormhole Detection Scheme through Trusted Neighbour Nodes in VANETs

Mahabaleshwar Kabbur, V. Arul Kumar

Abstract: ***VANET is an application and subclass of MANET's, in which nodes are mobiles and considered as moving, communicating vehicles in a wireless adhoc network. Vehicles communicate through dedicated short rage communication (DSRC) via IEEE 802.11p protocol. With the progress of wireless technology, vehicular ad hoc network has become emerging technology to support real-time traffic condition, safety, entertainment, enhance driver experience and emergency navigation in intelligent transport system (ITS). Core of VANETs application is the communication between vehicle to vehicle (V2V), vehicle to roadside unit (V2RSU) and securing the data messages from malicious activities and attackers in the network. Securing V2V and V2RSU communication has raised challenging issues in detecting and avoiding malicious attackers for secure communications. VANET's are exposed to different threats while routing data, wormhole attack is the most threatening routing attack which severely effects VANET routing data and causes incorrect routing by private tunnels and damages to VANET's communication in terms of data leakage, data dropping, and delayed delivery. However existing attack detection schemes have failed to meet secured VANETs communication leading to packet loss. In this paper we propose an efficient wormhole detection mechanism by creating potential and trusted neighbour nodes discovery (TNND) in VANETs, which can detect malicious nodes through enabling common forwarding neighbour nodes as witness to monitor data packets are forwarded by malicious nodes. Basically this mechanism is based on trust management. This scheme is resilient and resistant against attackers launching malicious nodes to corrupt entire network. Simulation is carried on event driven network simulator and results shows efficient detection of wormhole nodes, increases packet delivery and performs better than existing detection scheme.***

Keywords: Worm hole, data security, MANETS, VANETS, malicious, attacks.

I. INTRODUCTION

Intelligent transport system (ITS) has wide vehicular applications and supports direct communication between V2V and V2RSU [1]. Figure 01 shows architecture and components of VANETs. Basically vehicles are equipped with sensor nodes with dedicated short-range communication (DSRC) protocol [2-4]. Sensed messages are communicated through wireless access (WAVE) IEEE 802.11p standard specially developed for vehicles to adapt adhoc network, messages include real-time road condition, traffic congestion, weather condition and audio/video streams [5-8]. This message gives driver a better understanding of current traffic events for safe driving. Road side unit (RSU) additionally provides value added services like, nearby fuel station, restaurants etc, which significantly enhances V2RSU communications. RSU helps in better understanding the traffic network by gathering messages from vehicles.

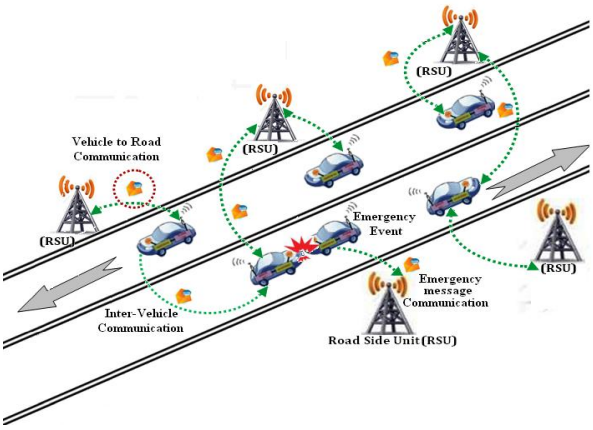

Figure 01: VANET architecture

Securing messages pose great challenging issues in VANETs due to wireless data exchange, frequent changing of topology and network size [9-11]. Malicious nodes indulge in various malicious activities like spoofing as legitimate user, modify data packets and interrupt the network. In order to detect and avoid malicious activities in VANETs, we propose efficient trusted neighbour node discovery mechanism to identify wormhole nodes through local trust monitoring between two nodes. The main contributions of this paper are:

- **a)** Propose secure and trusted neighbour discovery method to detect malicious nodes.
- **b)** Ensure massages confidentiality and availability for V2V and V2RSU
- **c)** Simulation results show better performance in detecting wormhole nodes.

The rest of this paper is organized as follows. In Section II describe the related work carried out. Section III describes the propose system model. In section IV the performance analysis and relative simulation are conducted. Finally we draw the conclusion on the proposed scheme in section V.

II. RELATED WORKS

Advancement of communication technology in ITS and VANETs is under research for past years, in securing the message exchange and providing better security against different threats.

Revised Manuscript Received on December 12, 2019.

Mr. Mahabaleshwar Kabbur, Research Scholar, School of Computer Science & Applications, REVA University, Bengaluru-64
mskabbur.reva@gmail.com
Dr. V. Arul Kumar, Assistant Professor, School of Computer Science & Applications, REVA University, Bengaluru-64, arulkumar.v@reva.edu.in

In this section we look into previous existing works done to eliminate frequency of attacks in VANETs. Greedy based detection for VANETs was proposed [12] in order to reduce greedy behaviour frequency in VANETs. This scheme detects multiple DOS attacks and assures enhance and safety travel for passengers and also authorize clients to access information. In [13] attack resistant trust management was proposed. In this management the algorithm was not only had a capable of detecting malicious activity and also had ability to deal with malicious attacks. Nodes trust evaluation was done of two factors: functional and recommendation trust, which reveal how node could accomplish its function and trust recommendations from nodes. In [14] author presented security model to prevent DOS attack on game theory and expressed two conditions on strategic and extensive type game. Also author analyzed DOS attacks by utilizing mobility models on actual map. In [15] VANET was regarded by experts to be a complex network in which all vehicle node moments were random. The node location varies in VANETs, so information dissemination was a concern; also, each time for data packet transmission, fresh links were established. So, an attack could end up all communication between vehicle nodes in such a scenario. In [16] sometime the cryptographic techniques of node authentication was not enough for data transmission, even authentic nodes gets compromised to attackers or disseminates fake information. To overcome these threats author proposed logistic trust which has the ability to detect and identify malicious false messages and nodes.

III. PROPOSED METHODOLOGY

a. System Model

As shown in Figure 2 the system model consists of vehicles, Trusted Authority (TA), RSU, application servers and on board units on vehicle. TA communicates with application servers and RSU through secure communication channels. TA recognizes vehicle's identity, RSU are placed along the road side and it is prone to attacks. In adversary model the communication between RSU and vehicles are not secure and adversary is capable of modify, diffuse legitimate vehicle to send wrong message and does malicious activities thus harming infrastructure of VANETs.

b. Trust Model

Trust of any nodes (vehicle) is evaluated by its neighbor node on its experience basis.

$$if\ A \geq B$$

$$T_{ei} = 1 - \frac{1}{\left(\frac{A-B}{A+B}\right)*W_s+2} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$if\ A < B$$

$$T_{ei} = \frac{1}{\left(\frac{B-A}{A+B}\right)*W_u+2} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Successful and unsuccessful transmission is represented as A, B and weights are represented as $W_s and\ W_u$. For successful transmission trust of nodes is range of (0.5-1) and for unsuccessful is less than 0.5.

The trust value of receiver *B* is computed based on the recommendation of sender *A*.

$$T_S = \frac{\sum_{i\neq A, i\neq B} T_A^i * T_i^B}{\sum_{i\neq A, i\neq B} T_A^i} \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

T_A^i representes trust of node i given by sensor A and T_i^B is B sensor trust from recommender sensor i.

A trust value compute for B in current time is given as

$$T_n = W_e T_{ei} + W_r T_s$$

where

$$W_e + W_r = 1$$

W_e and W_r are weights of experience and recommendation trust.

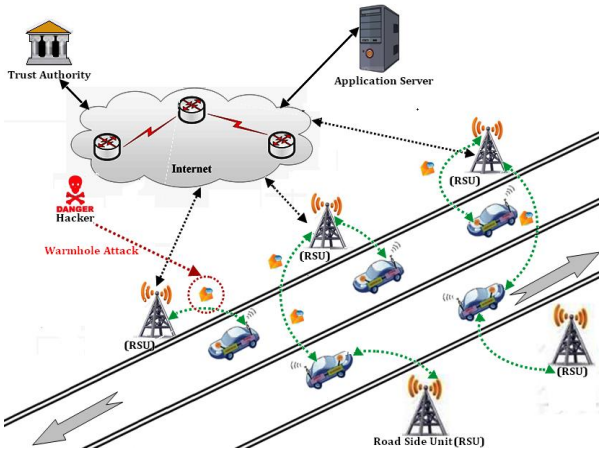

Figure 02: System Model of Wormhole Attack in VANET

c. Wormhole detection and avoidance mechanism

This type of malicious attack is launched by two or more nodes having private communication channel called tunneling and considered as severe threat in VANETs. These wormhole attacker uses out of bound channel medium from normal nodes and initiate attacks in hidden mode. Malicious nodes are hidden, on receiving packets they does not process any packet information and simply forwards it to next node. By doing this malicious activity they don't appear in routing tables making it right way to launch attacks and extract huge amount of traffic messages. Based on trust evaluation, the neighbour nodes successful and unsuccessful transmission is valuated. If the trust value of node is high, transmission is considered as safe and secure else if trust value is low it triggers for detection of malicious node.

Wormhole Detection Algorithm

Input : n_A : set of neighbour of node A; n_B :set of neighbour of B; T_n: trust value

Output: Between A and B pair there exist wormhole

Start :

- Let $E_A = n_A - n_A \cap n_B - \{B\}$ set of neighbour between two node links

- Let $e_A = |E_A|$ neighbour of node A
- $e_A \geq 0.5$ *then*
- for each node o_i in E_A do
- calculate the trust for unsuccessful transmission T_n
- if $T_n \leq 0.5$ Then triggers for detection of malicious node.

End.

There exists a wormhole between two vehicles

IV. RESULTS

Simulation of our proposed scheme is evaluated in discrete event driven simulation tool network simulator (NS2) and compared with existing trust scheme with logistic trust (LT). Performance evaluation metrics like trust computation error, end to end delay
and normalized routing overhead is compared and simulation results shows our scheme performs well in detecting malicious nodes and delivers trusted packets also achieves high successful transmission.

1. Trust computation error: is between successful and unsuccessful transmission on trust evaluation assessments of vehicles. Figure 3 shows the trust computation error graph, our scheme computes less root mean error trust calculation for all nodes. In logistic trust scheme performs optimal and occurs in errors.

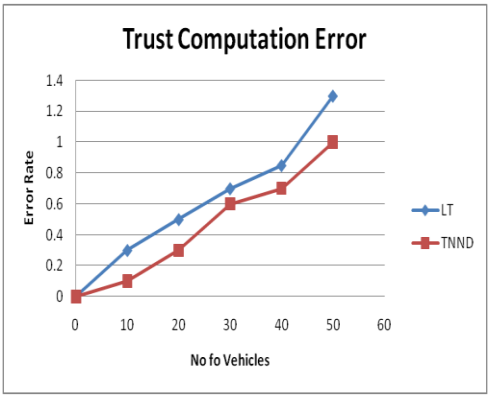

Figure 03: Graph of Trust computation

The enhancement in the performance TNND scheme is due to fact that our scheme evaluates trust values for all nodes randomly and malicious nodes are identified based on unsuccessful transmission. This scheme is resilient and resistant against attackers launching malicious nodes to corrupt entire network.

2. End to End Delay: Average end to end delay includes travelling of packets from source to destination buffered during routing process. Due to high mobility and frequent topology changes delay-tolerant networks are favoured to be use for higher packet delivery. Average delay is expressed as

$$\sum T_1 - T_2 / N$$

T_1 is first data packet received at destination and T_2 is time when the sender or source node transmitting first packet and N is number of packets sent. In the Figure 4 shows the delay graph of our proposed scheme, where the successful transmission rates are higher and the time required sending trusted packets are low compared to the logistic trust scheme. Our scheme achieves less average delay and delivers high packets.

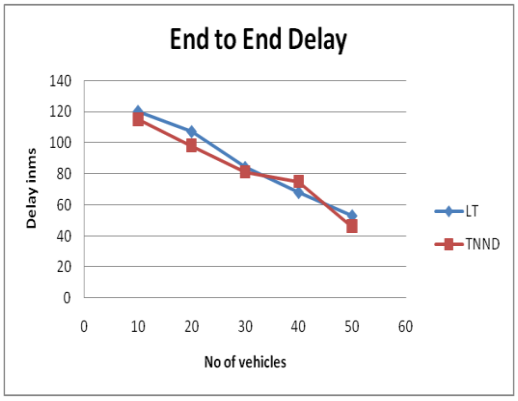

Figure 04: Graph of End to End Delay

Proposed methodology considerably needs less information about the behavior of the sensor nodes and trusted nodes route discovery process, which remarkably reduced the delay.

3. Transmission Overhead: Communication cost of proposed scheme is analysed and compare with logistic trust

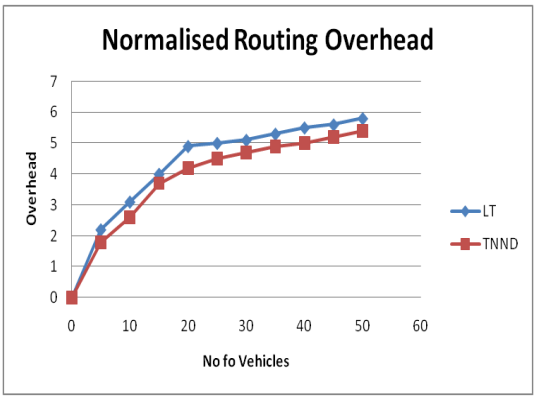

Figure 05: Graph of Routing overhead

scheme. The communication overhead incurred from V2RSU and V2V of sending data packets. In Figure 5 evaluation of transmission overhead focuses on evaluating trust values for nodes and detecting wormhole nodes before routing data packets which reflects in secure communication among vehicles.

V. CONCLUSION

VANET is an application of MANETs and basic building block of ITS, where the vehicle can communicate with V2V and V2RSU for real time messages. Securing these messages from various threats and avoiding hazardous circumstances is a challenging issue. In this paper we propose trusted neighbour nodes detection (TNND) scheme to detect wormhole nodes through enabling common forwarding neighbour nodes as witness to monitor data packets are forwarded by malicious nodes.

This creates tunnelling from authenticated nodes and redirects the messages to attackers. This scheme is secure and efficient in detecting malicious activities. Our scheme is compared with logistic trust scheme and performs better in terms of error rates, end to end delay and normalised routing overhead.

REFERENCES

1. K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, Y. Zhou, Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions. IEEE Commun. Surv. Tutor. 17(4), 2377–2396 (2015).
2. J. B. Kenney, Dedicated short-range communications (DSRC) standards inthe United States. Proc. IEEE. 99(7), 1162–1182 (2011)
3. D. Jiang, V. Taliwal, A. Meier, W. Holfelder, R. Herrtwich, Design of 5.9 GHzDSRC-based vehicular safety communication. IEEE Wirel. Commun. 13(5), 36–43 (2006)
4. J. Qian, T. Jing, Y. Huo, H. Li, Z. Li, Energy-efficient data dissemination strategy for roadside infrastructure in VCPS. EURASIP Wirel, J., Commun. Netw. 2016(1), 148 (2016). https://doi.org/10.1186/s13638-016-0650-0
5. Y. Liu, X. Weng, J. Wan, X. Yue, H. Song, A. V. Vasilakos, Exploring data validity in transportation systems for smart cities. IEEE Commun. Mag. 55(5), 26–33 (2017)
6. C. Chen, T. H. Luan, X. Guan, N. Lu, Y. Liu, Connected vehicular transportation: data analytics and traffic-dependent networking. IEEE Veh.Technol. Mag. 12(3), 42–54 (2017)
7. Y. Lu, Z. Zhao, B. Zhang, L. Ma, Y. Huo, G. Jing, A context-aware budget-constrained targeted advertising system for vehicular networks. IEEE Access. 6, 8704–8713 (2018)
8. J. Qiao, Y. He, X. S. Shen, Improving video streaming quality in 5G enabled vehicular networks. IEEE Wirel. Commun. 25(2), 133–139 (2018)
9. A. Boualouache, S. M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks. IEEE Commun. Surv. Tutor. 20(1), 770–790 (2018)
10. H. Li, R. Lu, J. Misic, M. Mahmoud, Security and privacy of connected vehicular cloud computing. IEEE Netw. 32(3), 4–6 (2018)
11. M. N. Mejri and J. Ben-Othman, "GDVAN: a new greedy behavior attack detection algorithm for VANETs," IEEE Transactions on Mobile Computing, vol. 16, no. 3, pp. 759– 771, 2017
12. S. Ahmed and K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in 2016 IEEE Wireless Communications and Networking Conference, pp. 1–6, Doha, Qatar, 2016, IEEE.
13. W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960–969, 2016.
14. M. N. Mejri, N. Achir, and M. Hamdi, "A new security games based reaction algorithm against DOS attacks in VANETs," in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 837–840, Las Vegas, NV, USA, 2016, IEEE.
15. Mujeeb Ur Rehman, Sheeraz Ahmed, Sarmad Ullah Khan, Shabana Begum, and Atif Ishtiaq, "ARV2V: Attack resistant vehicle to vehicle algorithm, performance in term of end-toend delay and trust computation error in VANETs," in 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pp. 1–6, Sukkur, Pakistan, 2018, IEEE.
16. Mr. Mahabaleshwar Kabbur & Dr. V. Arul KumarS, "Cooperative RSU Based Detection and Prevention of Sybil Attacks in Routing Process of VANET" in 2019 IJRTE ISSN: ISSN: 1742-6596
17. Mr. Mahabaleshwar Kabbur & Dr. V. Arul KumarS, "Detection and Prevention of DoS Attacks in VANET with RSU's Cooperative Message Temporal Signature" in 2019 IJRTE ISSN: 2277-3878.

AUTHORS PROFILE

Mr. Mahabaleshwar Kabbur, research scholar of Reva University**.** He has obtained his Master's degree in Computer Applications (MCA) and research degree in Master of Philosophy in computer science (M.Phil). He has 11 years of experience in teaching and 02 years of experience in research. He is pursuing his doctoral research on "Security on Wireless networking with respect to VANET". He is published 06 research articles in UGC approved international journals and presented 12 articles in various National and International conferences. His specializations and research interests include Network Security, Content-Based Image Retrieval Techniques & IoT.

Dr. V. ARUL KUMAR, Assistant Professor in School of Computer Science & Applications holds doctoral degree in Computer Science from Bharathidasan University-Tamil Nadu. He has completed B. Sc (Applied Sciences – Computer Technology), M.Sc (Applied Sciences – Information Technology) from K.S.R College of Technology and M.Phil in Computer Science from Bharathidasan University, Tamil Nadu. He has 5 Years of experience in teaching and 7 years of experience in research. He has qualified in State Eligibility Test (SET) conducted by Mother Teresa Women's University. He has published 18 research articles in the various International / National Journals and conferences. His Research area includes data Mining, cloud security and cryptography.