Gopikrishnan et al. 2018. *Int. J. Vehicle Structures & Systems*, 10(2), 85-88
ISSN: 0975-3060 (Print), 0975-3540 (Online)
doi: 10.4273/ijvss.10.2.02

International Journal of Vehicle Structures & Systems
Available online at www.maftree.org/eja

Reinforcing VANET Security using Ant Colony Optimization through Heuristic Approach

S. Gopikrishnan[a], C. Krishnaraj[b] and K. Kokilavani[c]

[a]*Dept. of Information Tech., Karpagam College of Engg., Coimbatore, India*
Corresponding Author, Email: gopikrishnanme@gmail.com
[b]*Dept. of Mech. Engg., Karpagam College of Engg., Coimbatore, India*
Email: krishna.kce@gmail.com
[c]*Dept. of Computer Engg., PSG Polytechnic College, Coimbatore, India*
Email: kkvkokila21@gmail.com

ABSTRACT:

Vehicular ad hoc network (VANET) is a novice technique which has drawn the attention of several industries and academics. Security parameters in VANET are now receiving popularity in the research community. A defensive mechanism provides a solution to control the attacks across the VANET security. However, a single defence mechanism is unable to provide solution to the attack models as more sophisticated method is required for VANETs. This paper proposed a method termed heuristic approach for ant colony optimization (HAAC) for improved security in addition to better transportation, reliability and management. The heuristic based ant colony optimization is used to reduce the problem in finding known and unknown opponents in providing security to VANET. The characteristic of real ant colonies is used in VANET security in order to solve attack problems with shortest path. The Reinforcing VANET security using vehicle mode analysis is evaluated in an efficient manner using NS2 simulator. The excellent outcomes are obtained by an HAAC approach combined with a dynamic heuristic.

KEYWORDS:

Collision avoidance; Data Aggregation; Delay efficiency; Energy efficiency; Security; Wireless sensor networks

CITATION:

S. Gopikrishnan, C. Krishnaraj and K. Kokilavani. 2018. Reinforcing VANET Security using Ant Colony Optimization through Heuristic Approach, *Int. J. Vehicle Structures & Systems*, 10(2), 85-88. doi:10.4273/ijvss.10.2.02.

1. Introduction

The quick development in wireless communication networks, recently has prepared Inter Vehicular Communications (IVC) and Road Vehicle Communications (RVC) in Mobile Ad Hoc Networks (MANET). IVC and RVC have given an origin to a new type of MANET known as the VANET. It aims to enable road security, well-organized driving, and infotainment. The basic idea from VANET is that each node in the network is portable, and move from one place to another inside the coverage area, but still the mobility is incomplete. VANET nodes are moving in elevated mobility, vehicles make connection throw their way with other vehicles that never faced before, and this connection lasts for few seconds only as each vehicle goes in its direction; these two vehicles may never meet again. So securing mobility challenge is tough problem. There are many researchers have addressed this challenge but still this problem is unresolved.

VANET is a part of MANET where every node travels generously within the network. It covers the entire network and keeps on connected. Each node communicates with other nodes in single hop or multi hop. Fig. 1 describes the VANET structure, where vehicular networks system consists of large number of nodes, approximately number of vehicles exceeds 800 million in the world today; these vehicles will require an authority to govern it. The improvement in wireless communications technology and the concept of car network has diverted the attention over worldwide.

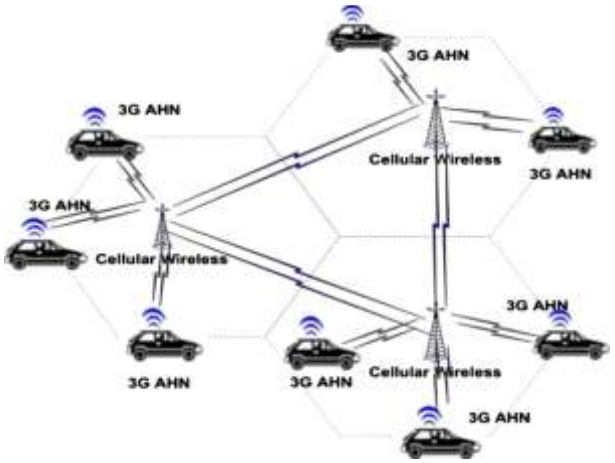

Fig. 1: VANET architecture

VANET is a subordinate class of MANET which provides wireless communication in the middle of vehicles and vehicle to road side equipments. The communication between vehicles is used for security, reassure and for activity as well. The performance of communication message depends on how improved the

routing acquired in the network. VANET routing information depends on the route protocols used in ad hoc system and chief aim of study is to recognize which ad hoc routing method has better performance in highly mobile environment of VANET. Routing protocols were chosen vigilantly after carrying out literature review and preferred protocols on VANET, then calculate the throughput and packet drop simulation in terms of experimental metrics. Due to high mobility, frequent change in topology and incomplete life time are such characteristics of this network that make routing decisions more demanding.

Security is always denoted with price regarding performance degradation and it should be determined carefully. Wireless ad hoc networks (WANETs) normally offer communication among the shared wireless channel, by not considering or not employing any preceding infrastructure. Creation of end-to-end secure paths in such WANETs is more demanding because of lack of central authorities. Its impact on network performance is not noticed [1] depending on common random network model, the asymptotic behaviours of secure throughput and delay with the common transmission range is determined. Even when the throughput is zero, because of the network size is randomly large; there is still a possibility to form throughput-order-optimal secure WANETs. Thus another author suggests a different way to provide security. In wireless networks, wandering of mobile users is high and authentication to be provided to them is difficult. He et al [2] designed a privacy-preserving universal authentication protocol, named Priauth. It provides authentication for eavesdroppers and foreign servers; authentication efficiency is high when session keys are authorized. In Priauth foreign servers can be verified based on the revocation list (RL) i.e., whether the roaming user moved from the home server is revoked or not. Koksal et al [3] presented a method to find the obtainable rate regions for the problem of single and multi-user systems that are to be attained by considering the nodes having full Channel State Information (CSI) of their neighbours.

Xu et al. [4] presented a plan and execution of a policy enforcing mechanism is done using Satem, a kernel-level trusted execution monitor was formed based on trusted platform module. Bu et al. [5] proposed a structural result method to crack the problem for a large network with a variety of nodes. The policies resulting from structural outcomes are simple to execute in practical MANETs. The system performance from the structural results method is equal to the value iteration algorithm which is calculated on the basis of lower computational complexity. Sepulcre et al [6] designed and estimated a contextual cooperative congestion control policy that utilizes the traffic context information of each vehicle to decrease the channel load, while satisfying the vehicular applications requirements. Niyato et al [7] examined the difficulty of accessing an optimal channel, basically to offer quality of service (QoS) for data transmission in cognitive vehicular networks. A hierarchical optimization model is also designed for the framework to attain the optimal policy. The hierarchical optimization method includes two constrained Markov decision process (CMDP) formulations for the above mentioned factors. To overcome this problem, Lu et al [8] proposed a valuable pseudonym changing at social spots (PCS) strategy to attain the provable location privacy. The current model tracks a vehicle in a spatial-temporal way; hence advanced technique is to be considered which should use more character factors to track a vehicle and to discover new location-privacy-enhanced techniques under such a stronger threat model. Still an enhanced method is needed to provide safety for vehicular communication.

2. Heuristic-approach for ant colony optimization (HAAC)

In the Heuristic-Approach for Ant Colony optimization (HAAC), vehicular nodes acting in a same manner with each other, send out ants depositing information i.e. pheromone concerning the maliciousness of further nodes. Then, a node generates the authenticity of the other node following a pheromone guideline process and hence collecting all information accessible to the network enchanting an informed choice in an optimized manner. In our work, a VANET security system supposes the Authority Certificate (AC) responsible for production and distribution of digital signatures to all nodes entering the network. Once a node becomes a part of the VANET, it examines the performance including authenticity of other nodes using all the accessible sensor data. Till the time it persists to be in touch with the RSU, it sends this information back to AC and makes it accountable for conducting non-repudiation and eliminating some nodes from the network. Fig. 2 shows the architectural diagram of secured VANET communication using heuristic based ant colony optimization.

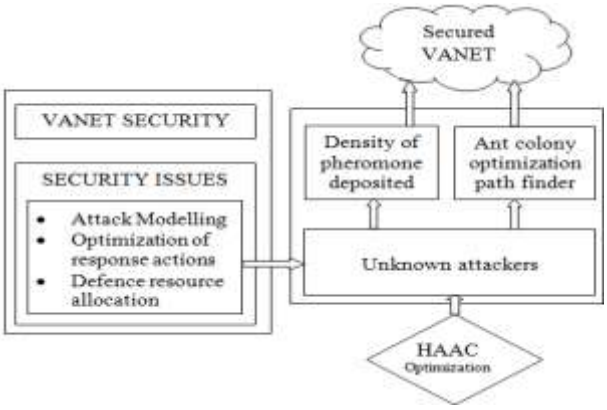

Fig. 2: Architectural diagram of secured VANET communication using Heuristic approach for ant colony optimization

The HAAC process is represented in the diagrammatic manner and is explained. In the Heuristic-approach for ant colony optimization passes ants depositing information where the vehicular nodes are acting in a same manner with each other. The node produces an authentication of the other node with the help of pheromone information. The work contains all the information accessible to the network. The VANET security system provides the Authority Certificate (AC) to all new nodes in the networks in producing digital signatures. The property of the node is evaluated after

the node becomes part of the VANET and also examines the authenticity of other nodes. The infrastructure environment is in connection with RSU. The RSU passes the information back to AC and makes it accountable for conducting non repudiation and rejecting some nodes from the network. Additionally in certifying ants also transmit out the all information regarding known or unknown nodes. Next every node depends on all information grouped through these ants, deciding next nodes. The algorithm describes the well distribution strategy of initial ants and dynamic updating of heuristic parameter and described as,

```
Step 1: Set parameters, begin with initializing pheromone trails
Step 2: Compute the highest entropy Loop
Step 3: Every ant is situated on a starting node consistent with distribution approach (every node has minimum one ant)
Step 4: For k = 1 to m do /*at this stage every loop is termed as a step */
Step 5: At the initial step moves every ant at diverse route
Step 6: Repeat [step 7 and step 8]
Step 7: Choose node j to be called next according to the subsequent node and must not be called by the ant.
Step 8: A heuristic is applied
Step 9: Until ant k finishes a tour repeat steps 7 & 8
Step 10: End for
Step 11: Local hunt are applied to progress explore
Step 12: Compute defensive measure of current pheromone trails
Step 13: Update the heuristic parameter
Step 14: Until End_condition
Step 15: End
```

3. Performance evaluation on HAAC optimization

A 1000 x 1000 grid of a map is considered on which nodes travel randomly, emulating a vehicular network environment (VANETS). Additional assignment in urban city-like scenario is made where the vehicle density is on the higher side. These nodes attempt and communicate with each other depends on another random set of connections of TCP or UDP. A simple maliciousness model is used to inject malicious behaviour into the system. A node marks one of its neighbours as malicious based on this maliciousness model. At this point heuristic based ant colony optimization comes into the action and drops pheromones. The following parameters and evaluation differ with the said metrics for the scenarios. Chen et al. [9] presented a simulation based on game theory in vehicular network. All simulations are run 20 times over and averaged. In a VANET, vehicles are set up with wireless networking environment permitting to communicate with other neighbouring vehicles passing on and to RSUs with the range specified. The communication taking place between the vehicles is multi-hop and similarly the RSUs are connected to each other. Vehicle density (vehicles/km) is defined as the number of vehicles per unit area of the roadway. The RSUs help vehicle-to-vehicle communication by tunnelling data. The vehicle density of the road network is presented with HAAC comparing to existing security games for vehicular network. The probability of vehicle density in different road network scenarios is presented according to the HAAC. Fig. 3 compares the strategies of CSI, PRIAUTH, PCS and the HAAC. The vehicles travel fast with high density in HAAC about 10-20% compared to security games. As the HAAC identifies both known opponents and unknown opponents recognizing the vehicles increasing the speed.

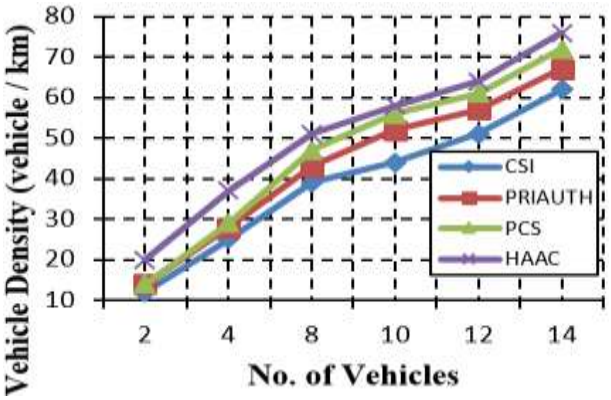

Fig. 3: No of vehicles vs. Vehicle density

The average speed indicates the data transmitted in the VANET network. The data transmitted requires an increased speed in delivering the data to the vehicle. Fig. 4 represents the average speed possibility rate of the proposed HAAC technique. Normally, in the urban scenario, there is a high possibility of speed. The average speed of vehicles is increased in HAAC around 20-25% compared to CSI, PRIAUTH and PCS. As the speed probability rate is high, the HAAC processes efficiently by identifying the known opponents based on the pheromone identified in the road path network and secure the vehicles moving on the road.

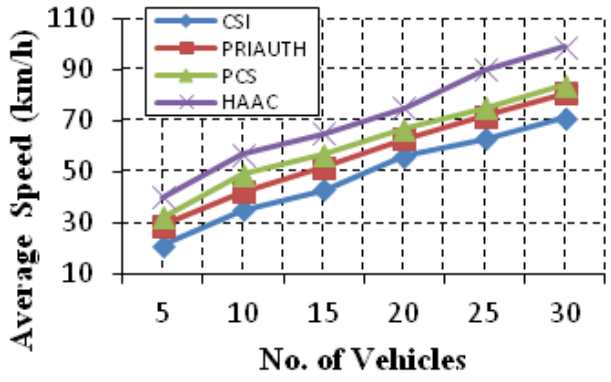

Fig. 4: No of vehicles vs. Average speed (km/h)

Centrality metrics are designed such that the highest value indicates the most central node. Fig. 5 specifies the centrality measures carried out depending on the vehicle density. The percentage of centrality measures is high in HAAC about 5-10 % compared to CSI, PRIAUTH and

PCS. The centrality provides a good measure as it relates to the expected role a node plays within the VANET communication. Betweenness centrality quantifies the probability of a node to be on the chosen shortest path between all the nodes of a given graph.

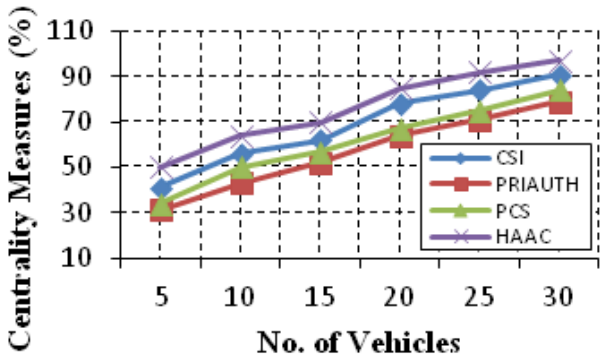

Fig. 5: Vehicle density vs. Centrality measures

In HAAC formulations, the data traffic model is essentially taken into account when characterizing the vehicular network and in deciding the payoff matrices. Fig. 6 describes the data traffic held between the vehicles. Data traffic denotes the data transmitted between the vehicles. Data traffic is measured in kbps. The data traffic is reduced in HAAC and the speed of data sending is increased around 20 - 25 % compared to CSI, PRIAUTH and PCS. The reason for reduced data traffic is due to a new road path explored with traversal of ants based on heuristic ant-colony optimization. Finally, the experimental conclusion of HAAC scheme works well and provides defensive measures to enhance an effective communication among the nodes in the network.

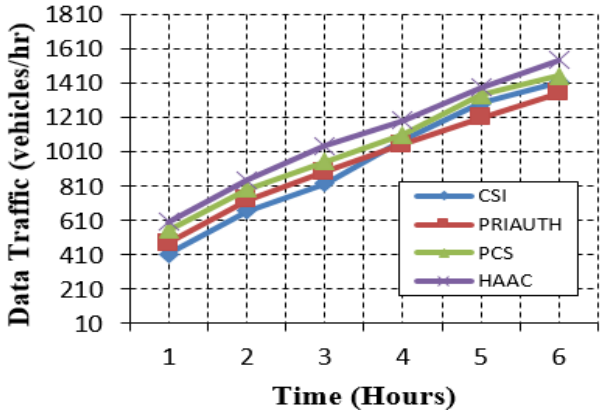

Fig. 6: Time (hr) vs. Data traffic (kbps)

4. Conclusion

The Heuristic-approach for ant colony optimization technique has efficiently implemented to improve the game theoretic approaches for VANET security. The factor centrality measure taken as input in security game is evaluated by aligning centrality metrics to the conventional road model derived by road segments. Analysis of VANET securities are made based on the simulation data determined from traffic engineering systems. The security method performs better when compared to the original strategy of shielding locations by ignoring behaviour of attacker. Globally best solutions are identified using Heuristic-approach for ant colony optimization which shares to the nodes that requires. Experimental evaluation performed using sample dataset shows performance improvement of 60% (with the increase in vehicle density (10-20%), average speed of (20-25%), high centrality measures (5-10%), and increased data traffic (20-25%), the defensive measures for mitigating malicious nodes in the network is improved to 60%.) of defensive measures for mitigating malicious nodes in the network.

REFERENCES:

[1] C. Zhang, Y. Song, Y. Fang and Y. Zhang. 2011. On the price of security in large-scale wireless ad hoc networks, *IEEE/ACM Trans. on Networking*, 19(2), 319-332. https://doi.org/10.1109/TNET.2011.2106162.

[2] D. He, J. Bu, S. Chan, C. Chen and M. Yin. 2011. Privacy-preserving universal authentication protocol for wireless communications, *IEEE Trans. on Wireless Communications*, 10(2), 431-436. https://doi.org/10.1109/TWC.2010.120610.101018.

[3] C.E. Koksal, O. Ercetin and Y. Sarikaya. 2013. Control of wireless networks with secrecy, *IEEE/ACM Trans. on Networking*, 21(1), 324-337. https://doi.org/10.1109/TNET.2012.2197410.

[4] G. Xu, C. Borcea and L. Iftode. 2011. A policy enforcing mechanism for trusted ad hoc networks, *IEEE Trans. on Dependable and Secure Computing*, 8(3), 321-336. https://doi.org/10.1109/TDSC.2010.11.

[5] S. Bu, F.R. Yu, X.P. Liu and H. Tang. 2011. Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks, *IEEE Trans. on Wireless Communications*, 10(9), 3064-3073. https://doi.org/10.1109/TWC.2011.071411.102123.

[6] M. Sepulcre, J. Gozalvez, J. Harri and H. Hartenstein. 2011. Contextual communications congestion control for cooperative vehicular networks, *IEEE Trans. on Wireless Communications*, 10(2), 385-389. https://doi.org/10.1109/TWC.2010.120610.100079.

[7] D. Niyato, E. Hossain and P. Wang. 2011. Optimal channel access management with QoS support for cognitive vehicular networks, *IEEE Trans. on Mobile Computing*, 10(4), 573-591. https://doi.org/10.1109/TMC.2010.191.

[8] R. Lu, X. Lin, T.H. Luan, X. Liang and X. Shen. 2012. Pseudonym changing at social spots: an effective strategy for location privacy in VANETs, *IEEE Trans. on Vehicular Tech.*, 61(1), 86-96. https://doi.org/10.1109/TVT.2011.2162864.

[9] C. Chen and M.A. Jensen. 2011. Secret key establishment using temporally and spatially correlated wireless channel coefficients, *IEEE Trans. on Mobile Computing*, 10(2), 205-215. https://doi.org/10.1109/TMC.2010.114.