ANT COLONY OPTIMIZATION TO ENHANCE GAME THEORETIC APPROACH FOR VANET SECURITY

Prabhakar M[1] Dr. J.N. Singh[2] Dr. Mahadevan[3]

[1] Research Scholar, Anna University Of Technology Coimbatore, Tamilnadu, India,

[2] Director/IT, Sambhram Institute of Technology, Bangalore, India,

[3] Professsor , AMC Engg. College, Bangalore, India,

e-Mail: laxmi.prabakar@gmail.com

Abstract

With promising features, VANET is potentially used in extensive variety of applications. In the current vehicular communication VANETs security properties have established more awareness in research community. Prescribed and quantitative decision structure for VANET security wants to address the issues of Attack modeling, Optimization of response actions, Allocation of defense resources which may benefit. Game theory approaches address these problems as its features are able to handle VANET security.

In this paper, we plan to improve the game theoretic approaches for the application cases having a scenarios with few known opponents and others with opponent uncertainty. To handle this type of issues, which is not addressed in the literatures, we introduce a defensive mechanism for the VANET security with heuristic based ant colony optimization. Our heuristic based ant model, work with i) Known opponents based on the density of pheromone deposited in the road network path and ii) Unknown opponents with new road path exploration with traversal of ants.

Keywords: ***VANET security, Game theory, Ant Colony Optimization***

1. Introduction

Vehicular ad hoc network (VANET) is a fresh technique which has newly drawn the notice of the industry and academia. Vehicular communications (VC) lie down at the core of a several study initiatives that aspire to improve safety and efficiency of transportation systems, with envisioned applications providing, for example, warnings on ecological exposures, traffic and road situations (e.g., emergency braking, congestion, or construction sites), and local (e.g., tourist) information. In fact, vehicular networks appear, along with national communication systems, as one of the most convinces and yet most demanding instantiations of the MANET technology. To allow such applications, vehicles and road-side infrastructure units (RSUs), network nodes, will be prepared with on-board processing and wireless communication units. Relying on mixture networking shows to be the only means to recognize safety and driving support applications, as a universal infrastructure cannot be a practical; it is too expensive, and thus very slowly organized.

Applications of VANET vary in their necessities of timely data delivery. Earlier reply time is for follow-up of accident avoidance in the instant neighborhood or barrier on the road. Tolerate little delays for the route optimization applications. Substantial delay is sufficient in non critical delay-tolerant activity situations. With promising features, VANET is potentially utilized in large series of applications. In the modern VC, Vehicular Networks security properties have expected more consideration in investigate society. Proper and quantitative result construction for VANET security desires to deal with problems of Attack modeling, Optimization of response actions and Allocation of defense resources could benefit.

Game theory approach address these troubles, as it features are capable to hold VANET security which is listed below.

1. Several players with different goals struggle and interact with each other and
2. They are used in several authority i.e., finances, decision theory, and control. Game theory provide mathematical framework for analysis, modeling, and decision processes for VANET security.

Game theory authorizes extra modeling of attacker behavior and communication between defense and attackers Compared with a pure optimization approach. Mathematical abstraction (framework) is useful for generalization of problems, merging existing ad hoc schemes in single window.

In this paper, we enhance the game theoretic approaches for the application cases having settings with a small number of known opponents and others with opponent indecision. For handling above concerns, we propose a defensive method for the VANET security with heuristic based ant colony optimization. The proposed ant colony optimization model, effort with i) Known opponents based on the pheromone density deposited in road network path and ii) Unknown opponents with new road path exploration with traversal of ants.

2. Related Works

VANET Security and a variety of countermeasures have been outlined in [11] which discussed security necessities for VANETs and proposed a set of design principles. VANET risk analysis and a set of security protocols are examined and evaluated quantitatively in [13]. As a precursor to this work, placement approaches for roadside divisions in vehicular networks have been examined through evaluating different metrics such as density, centrality [13], and connectivity [12]. In a related work, several centrality indexes have been calculated for urban streets and studied their sharing [12]. In contrast, in this work, we see at the traffic dynamics rather than the static road system and use centrality metrics of the traffic in all elements of the map.

Security games, which detain the interaction of attackers and defenders under imperfect observations, have been investigated in [12]. Security game between the attacker and the intrusion detection system has been investigated both in finite and continuous kernel versions, where in the latter case, players are associated with specific cost functions [11]. This security game has been extended in [6] to a stochastic and dynamic one by modeling the operation of a sensor network as a finite Markov chain.

In contrast to this paper, where there is one defender strategically dispensing a fixed amount of resources, the scenario involves several defenders whose varying willingness to invest impacts the vulnerability of the whole system [12]. Revocation games in ephemeral networks (which encompass vehicular networks) have been studied in [7], where players jointly decide whether to revoke credentials of potentially malicious players [9]. It differs from the security games in this work by focusing on credentials of players rather than allocation of defensive resources.

3. Ant Colony Optimization to Enhance Game Theoretic Approach for VANET Security

In VANET, Vehicles are considered to be capable to communicate with neighboring vehicles and roadside units. Neighbors of a vehicle are deployed by its limited-radius (e.g., 300 m) radio coverage. The range and data rates will be modeled, for example, as circular and fixed. Roadside units link with servers and other roadside units by way of the Internet or other side channels. VANET comprises of three layers: data traffic, vehicular traffic, and road network. While the earlier two are dynamic, the final one is physically fixed.

3.1 Centrality Measure for Road Networks

A centrality measure for the road network is explained by mapping centrality values BC(p) of the nodes p € Nv of the vehicular network V snapshot to the corresponding nodes m € Nr of the underlying road graph R. the centrality values of the relevant vehicles on a road segment are taken as mean over a time window to attain the value for that node of the road graph. Betweenness centrality BC(p) quantifies the probability of a node p to be on the chosen shortest path s between all the nodes of a given graph. It can be defined as follows:

$$BC(p) = \sum_{m=1}^{k} \sum_{n=1}^{k} \frac{Sm,n(p)}{Sm,n}$$

where $S_{m,n}$ is the number of shortest paths from m to n and $S_{m,n}$ is the number of shortest paths from m to n passing through the node p. For a node m ∈ Nr and finite-time window T = 1, 2, 3, . . . , t, the centrality measure C(m) can be defined as

$$C(m) = \frac{1}{t}\sum_{T=1}^{t}\sum_{p} BC(p)\ f(p,m,T),\ p \in Nv,\ m \in Nr$$

where BC(p) denotes the betweenness centrality of a vehicle p ϵ Nv and f(p, m, T) is an indicator function.

$$VD(m) = \frac{1}{t}\sum_{T=1}^{t}\sum_{p} f(p,m,T),\ p \in Nv, m \in Nr$$

C(m) measure can be compared and contrasted to vehicle density VD(m) on a road segment m, which can be computed in a similar way through averaging.

3.2 VANET Security Game Model

For security game, an attacker jams (attacks) one road segment with a few probabilities according to its mixed attack strategy. In response, the defender assigns defense resources to the similar or another road segment corresponding to its own strategy. The outcome of a particular game is determined by the game matrix, which contains the cost (payoff) values for each possible action-reaction combination. The game matrix access can be a function of the significance of every road segment, the risk of detection (gain from capture) for the attacker (defender), as well as further factor. Accordingly, the game matrix G is defined as,

$$G = G(p, m) = \begin{cases} C(m), & \text{if } p \neq m, \\ R, & \text{if } p = m, \text{ for all } p, m \in Nr, \end{cases}$$

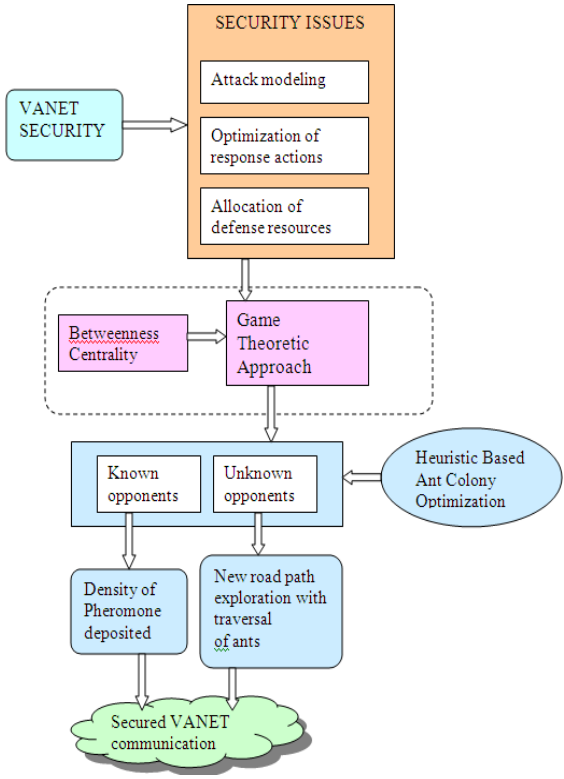
where C(m) is defined in (2) and r is a permanent scalar which indicates the risk or penalty of capture for the attacker (benefit for defender), if the defender allows resources to the position of the attack, i.e., the same square on the map.

The game matrix (cost and payoffs) is assigned to be known to both the defender and the attacker. The attacker's gain is equal to the defender's loss, and vice versa. The game has the matrix which is defined in eqn. (3). Every such two-player game declares a solution in mixed strategies and the solution (saddle point) will be attained by solving the following pair of primal-dual linear programming problems

$$\begin{cases} \sum G(p, m)\, x_p \geq v, & \text{for all } m \in Nr \\ \sum_{p} Xp = 1,\ Xp \geq 0, & \text{for all } p \in Nr \end{cases} \quad \text{Max}_x\ v$$

$$\begin{cases} \sum_{m} G(p, m)\, y_m \geq w, & \text{for all } p \in Nr \\ \sum_{p} Xp = 1,\ Xp \geq 0, & \text{for all } m \in Nr \end{cases} \quad \text{Min}_y\ w$$

Since both problems are reasonable and equally dual, by duality theory, the maximum of v will be equal to the minimum of w. Hence, the value v = w is the value of the game, that corresponds to the equilibrium gain and loss for the attacker and defender respectively. Here, the vector x is the equilibrium strategy of the attacker. The vector y is the defense strategy.



3.3 Heuristic Based Ant Colony Optimization

In our Heuristic Based Ant Colony Optimization, vehicular nodes acting together with each other send out ants depositing information (i.e. pheromone) concerning the maliciousness of further nodes. Then, a node develops the authenticity of another 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 model of a VANET security system we suppose the authority certificate (AC)

responsible for production and distribution of digital signatures for all nodes entering the network. Once a node becomes the part of a 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 banishing of some nodes from the network.

Additionally, to seem to be for certificates, ants can also be Transmit out to allocate information regarding known (or unknown) of particular nodes. Then every node, depends on all information grouped through these ants, will take a decision of that node. The above process is represented in the diagrammatic manner which is given as figure 1.

4. Performance Evaluation on Ant Colony Optimization on Game Theoretic Approach

Effectiveness of security game solutions and heuristic based ant colony optimization is evaluated using realistic simulation data obtained from traffic engineering systems. In the simulations, two particular scenarios are studied: first one rural and the other

Fig 1: Architectural diagram of Secured VANET communication using Heuristic Based Ant Colony Optimization

urban, which vary from each other in road and traffic density. The traces recommend snapshots in 1-second intervals about the identity of a vehicle, its x- and y-axis on the map, and a time stamp. Mobility models sort from random way point, where vehicles choose a random target and drive there with randomly changeable speed, to further difficult models including traffic lights and vehicle following, where the speed not only based on external constraints but also on the distance to the vehicle in front.

The game matrix (cost and payoffs) is defined in (3), and off-diagonal elements are centrality measures as in (2). The diagonal values, that quantify the penalty for the attacker when both players decide the identical road segment, are initally set to r = 0.2 approximately interpreted as 20 percent loss. From penalty, the equilibrium value of the game amounts to v = w = 0.4145. If the penalty is decreased to 0.01, the value raises to 0.6560, i.e., a gain for the attacker as predictable. Furthermore, a big penalty for the attacker directs to diversification in attack probabilities instead of narrowly meeting point on most valuable places to attain the most injure. The parameter which is taken into consideration for our simulation is listed below.

Vehicle Density: The number of vehicles per km, we differ this parameter by changing the number of nodes in the similar grid. This parameter also allows us to regard as time of the day as the vehicle density differs based on peak and no-peak hours.

Average Speed: The average speed with which nodes travel in the simulation setting make a decision the average active communication time i.e. the average amount of time two nodes can reside in communication variety of each other. This is significant parameter in our case as the pheromone dropping only concerns the nodes within the communication series of the node that has now recognized a malicious node. Hence intuitively, more the average speed, more the active time, more the number of nodes getting the pheromone containing information, greater the number of at first aware nodes.

5. Results and discussion

We consider a 1000x1000 grid of a map on which nodes travel randomly, emulating a vehicular network environment (VANETS). We have additional assigned an urban city-like scenario where the vehicle density can be on the higher side. These nodes attempt and communicate with each other depends on another random set of connections of TCP or UDP. We use a simple maliciousness model to inject malicious behavior into the system. A node marks one of its neighbors as malicious based on this maliciousness model. At this point heuristic based ant colony optimization comes into the action and drops pheromones. We differ the following

parameters and evaluate the said metrics for these scenarios. All simulations are run 20 times over and averaged.

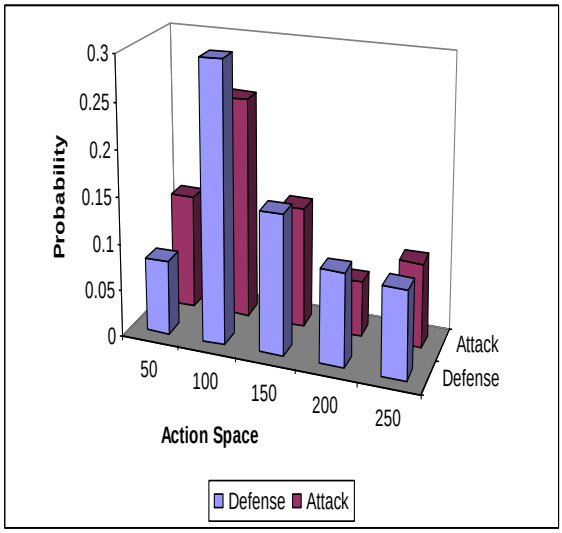


Fig 2: Nash equilibrium attack and defense probabilities of the zero sum Game in the rural scenario

Figs. 2 and 3 compare the mixed strategies of both the attacker and the defender in the rural and urban scenarios. The action space is the set of alternative moves offered to the player, in our specific case, the squares of the map (road segments) to either attack or defend. The probabilities represent attack and defense attempts by the respective players.

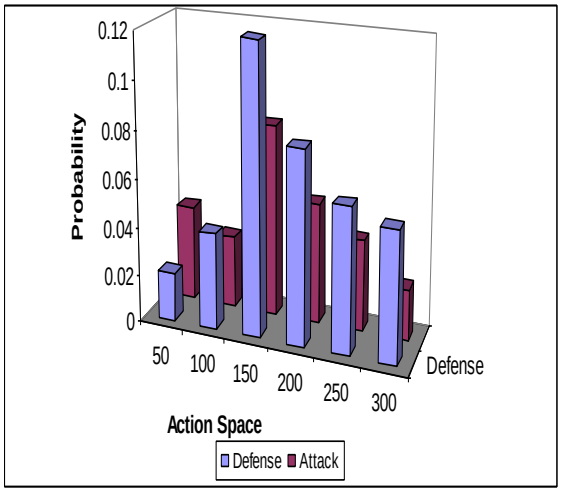


Fig 3: Nash equilibrium attack and defense probabilities of the zero sum game in the urban scenario

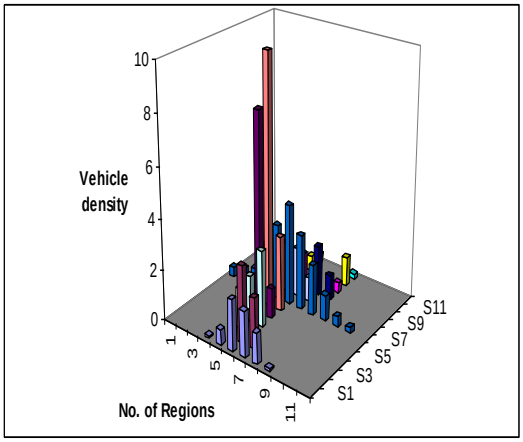


Fig 4: Vehicle density on the urban region map

The vehicle density and betweenness centrality values (over a certain time period) on example rural and urban region maps are depicted in Figs. 3 and 4 respectively**.**

6. Conclusion

In this paper, we have presented Heuristic Based Ant Colony Optimization to improve the game theoretic approaches for VANET security. The security game takes input as the centrality measures which are computed by mapping centrality metrics of the vehicle

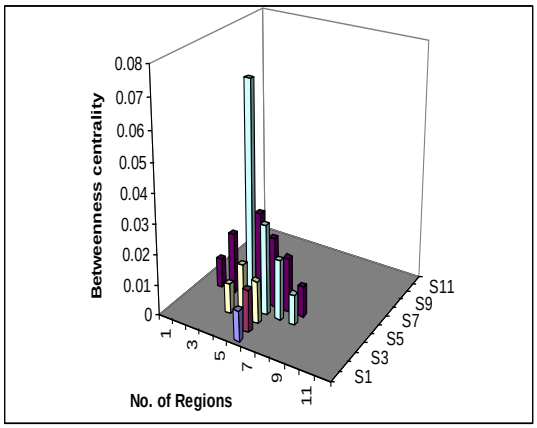


Fig 5: Betweenness centrality values on the quantized rural region map

networks to the fundamental road structure indicated by road segments. The numerical analysis is based on the sensible simulation data attained from traffic engineering systems. The security game outperforms the naïve strategy of shielding locations corresponding to their methods neglecting attacker behavior. Then we use the Ant colony optimization as a heuristic optimization to discover a globally best solution for share out certificate information to the nodes that require it most. Our simulation results shows that lesser latencies for prevention of malicious nodes from the network.

References

[1] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M. Gerlach, R. Kroh and T. Leinmuller, ”Attacks on Inter-Vehicle Communication Systems – An Analysis” in Proceedings of the 3rd International Workshop on Intelligent Transportation (WIT 2006), March 2006

[2] B. Parno and A. Perrig, ”Challenges in Securing Vehicular Networks,” in Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV), 2005

[3] G. Marfia, G. Pau, E. Giordano, E. De Sena, and M. Gerla, “Vanet: On Mobility Scenarios and Urban Infrastructure. A Case Study,” Proc. 2007 Mobile Networking Vehicular Environments, 2007.

[4] J. Grossklags, N. Christin, and J. Chuang, “Secure or Insure? A Game-Theoretic Analysis of Information Security Games,” Proc. 17th Int’l Conf. World Wide Web (WWW ’08), pp. 209-218, 2008.

[5] J. Grossklags, N. Christin, and J. Chuang, “Predicted and Observed User Behavior in the Weakest-Link Security Game,” Proc. First Conf. Usability, Psychology, and Security (UPSEC ’08), pp. 1-6, 2008.

[6] M. Backes and T. Gross ”Tailoring the Dolev-Yao abstraction to web services realities - a comprehensive wish list” Proceedings of SWS’05, Nov. 2005

[7] M. Raya, A. Aziz, and J.-P. Hubaux. Efficient secure aggregation in VANETs. In VANET ’06: Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc
Networks, pages 67–75, Sept. 2006.

[8] Marco Dorigoa,Christian Blum, “Ant colony optimization theory: A survey”, Theoretical Computer Science 344 (2005) 243 – 278

[9] R. Pucella and J. Y. Halpern, ”Modeling adversaries in a logic for security protocol analysis,” Proceedings of Formal Aspects of Security, 2003

[10] T. Basar and G.J. Olsder, Dynamic Non cooperative Game Theory, second ed. SIAM, 1999.

[11] Tansu Alpcan, and Sonja Buchegger, “Security Games for Vehicular Networks”, IEEE transactions on mobile computing,vol.10,no. 2, Feb 2011.

[12] U. Brandes. On variants of shortest-path betweenness centrality and their generic computation. Social Networks, 2008.

[13] Y. Do, S. Buchegger, T. Alpcan, and J.-P. Hubaux, “Centrality Analysis in Vehicular Ad-Hoc Networks,” technical report, EPFL/ T-Labs, 2008.