CHAPTER 3

HEURISTIC-BASED ANT COLONY OPTIMIZATION TO ENHANCE SECURITY IN VANETS

3.1 INTRODUCTION

To increase the security in VANET, heuristic ant colony optimization is introduced for application with few known opponents and with unknown opponent uncertainty using heuristic based ant colony optimization is designed. The heuristic based ant model evaluates both with known and unknown opponents. VANET is a promising profitable infrastructure framework used in diversified area of applications. Security parameters in VANET are now receiving popularity in the research community. In VANET environment, prescribed and quantitative decision format has to be quantified with the issues related to attack modeling, optimizing response and finally allocation of defense resources in a wide manner. The most important issue is to increase the security in VANET. Game theory approach handles the security related factor in an efficient manner.

Vehicular Ad hoc NETwork (VANET) is a novice technique which has drawn the attention of several industries and academics. Vehicular Communications (VC) lie down at the core of a several study initiatives aspire to improve safety and efficiency of transportation systems, with envisioned applications provided. For example, warnings on ecological exposures, traffic and road situations such as emergency braking, congestion, or construction sites and local information like tourist are vehicular communications. In fact, vehicular networks appear in addition to national communication systems, as
one of the most convincing factor. At the same time one of the most demanding instantiations of the MANET technology also appears in vehicular network. To implement vehicular communication applications with vehicles and Road-Side infrastructure Units (RSUs), network nodes are designed using on-board processing and wireless communication units. Relying on heterogeneous type of network it shows the only means to identify safety and driving support applications. While a universal infrastructure is not practical, it’s too expensive and also very slowly organized.

The below Figure 3.1 elaborates the VANET scenario. The Web server handles the instruction noted in the RSU through internet. A main central management station maintains the overall RSUs. RSU notices the accidents happening with vehicles and messages passed through vehicles which is a Vehicle to Infrastructure (V2I) communication. The V2V denotes the Vehicle to Vehicle communication taking place between the vehicles.

![Figure 3.1 VANET Scenario](image-url)
Applications of VANET vary in their requirements according to the timely data delivery. The reply time is for follow-up of accident avoidance in the instant neighborhood or barrier on the road which tolerate minimum delays for the route optimization models. A minimum delay is acceptable in non critical delay-tolerant activity mechanisms. The existing security games for vehicular network provides security with zero sum game techniques but less efficient in organizing nodes. With promising features, VANET is significantly used in large series of applications. In the modern vehicular communication VANETs security properties have expected to be of significant importance to investigate in 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 benefiting from the VANET security. Tansu Alpcan and Sonja Buchegger proposed a security games for vehicular network to avoid attacks. The security games involve zero sum game and fuzzy games.

Game theory approach address the problems of attack modeling, optimization of response actions and allocation of defense resources as it features are enriched to address the VANET security which is given below,

i) Numerous players with varied goal structure struggle and interact in a manner with each other

ii) The structures are used in different authority level i.e., finances, decision theory, and control.

Game theory provide mathematical framework for analysis, modeling, and decision processes for VANET security. Game theory provides authorization to extra modeling of attacker behavior and communication between two users, defense and attackers. Compared with the pure
optimization mechanisms, mathematical abstraction framework is extensively used for generalization of problems, merging existing ad hoc schemes in single window.

The game theoretic approach for the application cases involves settings with a small number of known opponents and others with opponent indecision. For handling known opponents and unknown opponents, a defensive method for the VANET security with Heuristic based Ant Colony Optimization (HACO) is proposed. The proposed heuristic-based ant colony optimization model provides solution with,

i) Known opponents, derived on basis of deposition of pheromone density

ii) Unknown opponents derived on basis of traversal of ants with exploration made on evolution of new path.

The motivation of work is to enhance the security using heuristic ant colony optimization, for application with few known opponents and with unknown opponent uncertainty. The heuristic based ant model evaluates both with known and unknown opponents. Known opponents are derived on basis of deposition of pheromone density and unknown opponents are derived on basis of traversal of ants with exploration made on evolution of new path. A game theory provides a solution to the problems of attack modeling, optimization of response actions and allocation of defense resources. In addition the heuristic ant colony optimization enhances the VANET security.

The experimental evaluation of VANET security is derived from the sample dataset using heuristics based ant colony optimization scheme. On
basis of evaluation, comparing results of HACO with the existing Security games for VANETS is demonstrated on observation.

3.2 VEHICULAR NETWORKS

The popularity of the vehicle communications is increasing due to the navigation of safety needs and by the establishment of various car manufacturers and public transport authorities. The idea of VANET (Vehicular Ad-hoc Network) is finalized with the important needs of vehicle grid components like spectrum, access points and standards. The vehicle grid components are responsible for the way of unconditional opportunities in car-to-car applications. Safe navigation is one of the most metrics responsible for car manufacturers and also municipal transportation authorities.

There are several properties involved in a VANET decision and arrangement. The most of the VANET nodes are vehicles; in addition to vehicles there are various entities involved in the behavior of basic operation performed in the network. The communication carried out between the nodes or vehicles are in many different ways. At first the frequent basic entities involved in the VANET communication is described. Secondly the VANET settings are analyzed differently which is seen in most vehicles explaining the remaining vehicles.

The common VANET entities are elaborated. VANET network commonly incurs various different entities in the communication. The core and certain security issues of the VANET network are recognized based on the analysis of entities and the relationships of entities. A typical VANET scheme is outlined below in a Figure 3.2.
Figure 3.2 given below outlines the simplified VANET model. Two different environments are generally considered in VANETs. The different environments are infrastructure environment and ad-hoc environment which are detailed below with the brief explanation.

Figure 3.2 Simplified VANET model

i) Infrastructure environment

The infrastructure environment generally contains entities that are permanently interconnected to each other. The entities are nothing but the traffic managing data or other external service offers. The vehicles are
distinctly identified in the manufacturing process rather considering the VANET model. The VANET model also contains the legal authority. Although each country follows different regulation in the network it is habitually connected to two major processes. The common tasks involved in the network are vehicle registration and offence reporting. Once manufactured every vehicle in an administrative region should get registered. The registered vehicle is issued with an authority of license plate. Simultaneously the traffic reports are processed.

Trusted Third Parties (TTP) is one of the entities involved in the infrastructure environment. TTP renders various services such as time stamping and credential management. For issuing electronic credentials TTP are required. The need of electronic credentials links both manufacturers and the authority to the TTP. The other important entity is the service providers in VANETs. Service Providers supports services. The services are accesses through the VANET. Location-Based Services (LBS) and Digital Video Broadcasting (DVB) are two examples of such services.

ii) Ad-hoc environment

An ad-hoc communication is provided among from vehicles in the ad-hoc environment network. Ad-hoc environment are from the VANET point of view, they are appointed with three different devices. Firstly, they are equipped with a communication unit called On-Board Unit (OBU). The OBU establish Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. At the same time a sensor is fixed on the vehicle to measure the status of its own. The sensor status measures fuel consumption and environmental status like slippery road and safety distance. The sensorial data is held in common with other vehicles to maximize their awareness and enhance road safety.
Finally, a Trusted Platform Module (TPM) is frequently fixed on vehicles. TPM mounted on the vehicles are specifically fixed for security purposes. TPM supports reliable storage and computation. The TPM storage of sensitive information such as pre-crash information or user credentials is reliable.

VANETs as communications network set various distinct needs. Vehicles travel in a high speed and the increase in vehicle on the roads leads to tremendous network attacks. The network information sharing involves a change in the data transmitted. A specific communication standard is required to negotiate the data attacks during communications. The standard with some communications devices located aside the roads, called Road-Side Units (RSU). The RSUs become gateways between the infrastructure and vehicles and vice versa.

iii) VANET Settings

Road safety of the vehicles is severely suffered by various attacks. The several applications enabled by VANETS are also affected by the attacks on road safety. The message exchanging over VANET are also affected by the attackers recognizing the data. With the attack natures a four different types of communication patterns are established.

1. V2V warning propagation

The message is transferred between particular vehicles or to a group of vehicles. Consider an accident is faced by a vehicle. The detection of the accident vehicle is identified and a message is delivered to avoid traffic providing increase traffic safety. If an emergency vehicle is arriving in speed the way is cleared by passing a message over VANET network.
The below Figure 3.3 illustrates the V2V warning propagation diagrammatically. The V2V warning propagation way of message transmitting is easier for the emergency vehicle to have a free way. A routing protocol is needed to forward the message to the destination.

![Figure 3.3 V2V Warning Propagation](image)

Figure 3.3 V2V Warning Propagation

2. **V2V group communication**

The V2V group communication part works with the vehicles containing features. So under this pattern, only vehicles having some features participate in the communication.

The below Figure 3.4 describes the V2V group communication. The vehicles are participated with features. The features of vehicle required to involve in the communication are either static or dynamic. The static features include vehicles of the same enterprise and dynamic features include vehicles on the same area in a time interval.
3. **V2V guiding**

Guide messages are transmitted periodically to nearby vehicles. The guide messages include the vehicles speed traveling, usage of brakes and headlights etc. of the sender vehicle.

The neighbor awareness is enormously increased with the use of V2V guiding. Guide messages are only forwarded to 1-hop communicating vehicles. The routing protocols are benefited with the guide message forwarding. The message permits the vehicles to identify the best neighbor to route a message.

The below Figure 3.5 demonstrates the V2V beaconing. The V2V beaconing allows vehicles to discover the neighbor routes for passing messages.
Warning messages are forwarded commonly through infrastructure environment with the help of RSUs. The warning messages are sent to vehicles when a difficulty is detected or noticed. The messages are efficient in enhancing the road safety. When a collision is faced, a warning message is sent from the infrastructure to vehicles for road safety.

The below Figure 3.6 elaborates the I2V/V2I warning diagrammatically. The messages are passed through RSU providing road safety on indicating collision warning.
In the modern vehicular communication VANETs security properties are strongly believed to be significantly important in investigating 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 benefiting from the VANET security.

### 3.2.1 Attacks in VANET

VANET faces many challenges more specifically the attacks in identifying the data during vehicular communication. The types of attacks against messages, is described as follows: False Information, fooling with Positioning Information, ID disclosure, Denial of Service and Masquerade. There are different classes of attacks like network, application, timing, monitoring, and social. The different type of attack are described below.

The Figure 3.7 describes the classification of attacks depending on Availability, Authentication or identification, Confidentiality, Privacy, Non-repudiation and Data-trust. Ghassan Samara et al (2010) presented a security analysis in vehicular network to negotiate the attacks.

**i) Attacks on availability**

Availability in VANET represents any information at any time of communication. This security needs are crucial in time varying environment. Availability in VANET is confirmed both in the nodes take part in communication and communication network.

A classification of these attacks, according to their target, is as follows. Black Hole Attack is one of the security disorder occur in VANET. The attacker in the black hole attack garbage the data or even drop the packet. Malware is mischievous attack which disrupts the normal basic operation.
Malware attack is performed by insider. This attack is found in the network when the software update is handled by car’s VANET units and roadside station. In broadcast tampering attack the attackers discovers bogus messages into the VANET.

Spamming is a non usage message particularly for users like advertisements. Greedy driver attackers normally attacks for their own benefit. These drivers cause overload problem for RSU. Denial of Service (DOS) is one of the most serious level attacks in vehicular network. In DOS attack, the attacker jams the main communication medium and network is no more available to legitimate users.
ii) **Attacks on Authentication/identification**

In Authentication types of attack the affected area is identification/authentication. The VANET security is provided with the basic needs of vehicles identification or authentication of nodes. The attacker identifies the vehicles identification or authentication, a trustworthy transmitter is required to communicate.

The different types of attack on authentication/identification are discussed as follows. Masquerading attack inserts false message instead of the original message during the communication by the attacker. The ways in which masquerading is performed are alteration changes, fabrication and replay of the message. Replay attack is carried out at the time of message sending as it’s the best way to attack the message by interrupting information. Global Positioning System (GPS) spoofing attack deals with reading in the GPS devices by leading a false message to other vehicles. Tunneling attack is seen when a link is introduced between two different ad-hoc networks with the help of extra communication as tunnel. Sybil attack an attacker acts like there are multiple identities in the network. Sybil attacker pretends like there are multiple nodes in the communication by showing multiple false identities. Message tampering attack the important essential values like traffic safety information is interrupted. The ID of targeted destination node is covered to recognize the origin of the node where messages are sent in the ID Disclosure attack.

iii) **Attacks on confidentiality**

Vehicular networks security is decided generally on the data confidentiality. The confidentiality of the data is promised as the message passed to person is read with an authority of that message. Confidential messages are most seen in the group communication where the authority is
provided only to group members for reading the message. VANET transfers
public information visible to all as the VANET mobility is greater than
MANET. Routing protocol ability in providing confidential message is more
difficult than Ad-hoc network. The messages shared between the nodes are
specifically susceptible with techniques like prohibited set of messages
through eavesdropping and collecting location messages seen in the
transmission of broadcast messages. The existing user information is gathered
by the attacker without their permission if a eavesdropping is discovered.
Later the information are gathered and used when the user is inactive.
Location privacy and invisibility are vital issues for vehicle users.

iv) **Attacks on privacy**

This type of attack is related with unauthorized accessing important
information about vehicles. There is direct relation between driver and
vehicle. If the attackers illegally access some data this directly affect the
driver’s privacy. Usually a vehicle owner is also its driver, so if an attacker is
getting the owner’s identity then indirectly vehicle could put its privacy at
risk; this type of privacy attack is called as identity revealing. Location
tracking is also one of the well known privacy attacks. In this attack the
location of vehicle or the path followed by that vehicle at particular period of
time is considered as a personal data.

v) **Attacks on non-repudiation**

Non-repudiation is occurred when two or more users exchange the
same key. Due to this, two users are unknown from each other and hence their
action is rejected. The use of identical key in different vehicles should be
eliminated with the help of reliable storage.
vi) **Attacks on data trust**

An inaccurate data collection, affected message recognition, and useless information calculation are compromised in data trust. The data trust is operated by the sensors in vehicles or by altering the sent information. The reliability of the entire system is affected. HACO provides a protection against such attacks in vehicular network.

The above all attacks are restricted in VANET to provide security to the message forwarded. Proper and quantitative result construction for VANET security desires to deal with problems of attacks. Game theory approach addresses the problems of attack such as modeling, optimization of response actions and allocation of defense resources as it features are enriched to address the VANET security.

The heuristic based ant model evaluates both with known and unknown opponents. A HACO provides a solution to the problems of above attack specifically modeling, data trust, optimization and allocation of defense resources. In addition the heuristic ant colony optimization enhances the VANET security.

### 3.2.2 Heuristic-based Ant Colony Optimization

In the Heuristic-based Ant Colony Optimization (HACO), 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.

The Figure 3.8 given below shows the architectural diagram of secured VANET communication using heuristic based ant colony optimization. The HACO process is represented in the diagrammatic manner and is explained. In the Heuristic-based Ant Colony Optimization passes ants depositing information where the vehicular nodes are acting in a same manner with each other. The node produces a 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.
Figure 3.8 Architectural diagram of Secured VANET communication using Heuristic Based Ant Colony Optimization
3.3 HEURISTIC-BASED ANT COLONY OPTIMIZATION WITH ENHANCED GAME THEORETIC APPROACH FOR VANET SECURITY

In VANET, Vehicles are considered to be very efficient to communicate with both the neighboring vehicles and roadside units. Neighbors of a vehicle are structured using the measure, limited-radius (e.g., 300 m) radio coverage. The range and data rates are modeled, comprising of circular and fixed. Roadside units link with servers and other roadside units by using Internet or other side channels. VANET consists of three layers: data traffic, vehicular traffic, and road network. The data traffic and vehicular traffic are dynamic whereas the road network is physically fixed.

3.3.1 Centrality Measure for Road Networks

Centrality measure for the road network is derived by mapping centrality values BC (p) of the nodes \( p \in N_v \) of the vehicular network V snapshot to the corresponding nodes \( m \in N_r \) of the underlying road graph R. The centrality values of the relevant vehicles on a road segment are considered as mean over a time window to achieve the value for that node of the particular 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 is defined as follows Equation (3.1).

\[
BC (p) = \sum_{m}^{k} \sum_{n=1}^{k} \frac{S_{m,n}(p)}{S_{m,n}}
\]  

(3.1)

where \( S_{m,n} \) is the number of shortest paths from m to n and \( S_{m,n}(P) \) is the number of shortest paths from m to n passing through the node p. For a
node \( m \in Nz \) and finite-time window \( T = 1, \ldots, t \), the centrality measure \( C(m) \) is defined as Equation (3.2).

\[
C(m) = \frac{1}{t} \sum_{T=1}^{t} \sum_{p} B(p) f(p, m, T), \ p \in Nz; \ m \in Nz
\]  

(3.2)

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

\[
VD(m) = \frac{1}{t} \sum_{T=1}^{t} \sum_{p} f(p, m, T), \ p \in Nv; \ m \in Nz
\]  

(3.3)

\( C(m) \) measure is compared and contrasted to vehicle density \( VD(m) \) on a road segment \( m \), which is computed in a similar way through the method of averaging.

### 3.3.2 VANET Security Game Model

For HACO model, an attacker attacks one road segment with a certain expectations in comparison to various methodologies. In response, the defender node, assigns defense resources to the same or another road segment on the basis of its own strategy. The outcome of a particular game is obtained by the game matrix, which consist of the cost or payoff values for each possible action-reaction combination. The game matrix access is a function of the significance of every road segment, the risk of detection i.e. gains from capture for the attacker as well as further factor. Accordingly, the game matrix \( G \) is defined as Equation (3.4)

\[
G = G(p, m) = \begin{cases} 
C(m), & \text{if } p \neq m \\
R, & \text{if } p = m, \ \forall \ p, m \in N_r 
\end{cases}
\]  

(3.4)
where $C(m)$ is defined in Equation (3.2) 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 of 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 Equation (3.3, 3.5 and 3.6). Every such two-player game declares a solution in mixed strategies and the solution is obtained by solving the following pair of primal-dual linear programming problems

$$\begin{align}
\text{Max}_x v &= \begin{cases} 
\sum_p G(p,m), & \text{if } x_p \geq v, \forall m \in N_r \\
\sum_p X_p = 1, & \text{if } x_p \geq 0, \forall p \in N_r 
\end{cases} \\
\text{Min}_y w &= \begin{cases} 
\sum_m G(p,m), & \text{if } y_m \geq w, \forall p \in N_r \\
\sum_p Y_p = 1, & \text{if } y_p \geq 0, \forall m \in N_r 
\end{cases}
\end{align}$$

Since both problems are reasonable and equally dual, by duality theory, the most 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.

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 /* at this stage each loop is called iteration*/

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

The above algorithm describes the process of heuristic-based ant colony optimization to improve the game theoretic approach and the next section describes the performance evaluation of the proposed work.
3.4 PERFORMANCE EVALUATION ON HEURISTIC-BASED ANT COLONY OPTIMIZATION ON GAME THEORETIC APPROACH

The performance of the proposed heuristic-based ant colony optimization on game theoretic approach for secure communication without interruption is evaluated on Pentium IV 2.5 GHz Processor with 2GB RAM in an efficient manner using NS2 (Version No. 2.3.4) simulator. The game theoretic approach in VANET competently communicates with the network with low overhead and the game model has been created efficiently based on traffic conditions on par with threats and attacks. It is considered a 1000x1000 grid of a map on which nodes travel randomly, emulating a vehicular network environment (VANETS). It is additionally 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.

All simulations are run 20 times over and averaged. Initially the experiment is evaluated with 100 nodes in a flat area of 100 * 100 m². The nodes’ incoming time measured in terms of seconds is noted as t1, t2….tn. Imagine a 1000x1000 grid of a map where nodes are able to pass through arbitrarily for VANET environment based game theoretic approach. In VANET environment, these nodes endeavor and correspond with each other depends on another arbitrary set of connections of TCP or UDP. All simulations are run 25 times over and averaged.

The 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 evaluated: first one rural and the other 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 parameters which are taken into consideration for our simulation are listed below.

i. Vehicle Density

ii. Average Speed

iii. Centrality Measures

iv. Data Traffic

3.4.1 Vehicle Density

The number of vehicles per km denotes the vehicle density. The parameter is differed 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 non-peak hours.

3.4.2 Average Speed

The average speed with which nodes travel in the simulation setting makes a decision of the average active communication time i.e. the average amount of time two nodes reside in communication area. 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.

3.4.3 Centrality Measures

Centrality metrics are developed in social network analysis to quantify the importance of particular individuals in social networks. The objective is to find people who are central to communication and important for information dissemination. The highest value is indicated by the central node for the design of centrality metrics. If every node is participating in the communication with each other the betweenness centrality is measured with the calculated routing service appeals.

3.4.4 Data Traffic in Vehicular Network

The data traffic occurred and scattered on a VANET rely upon the particular scenario and applications disposed. Evaluation parameter for a time crucial accident warning events happening is handled by sending a warning message distributed over all cars around the broadcast range. Hence, data traffic places an important parameter in evaluating the HACO techniques in vehicular traffic network nature.

3.5 RESULTS AND DISCUSSION

A 1000x1000 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 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. The following parameters and evaluation differ with the said metrics for the scenarios. Tingting Chen et al (2010) presented a simulation based on game theory in vehicular network. All simulations are run 20 times over and averaged.

3.5.1 Vehicle Density

In a VANET, vehicles are set up with wireless networking environment permitting to communicate with other neighboring vehicles passing on and to RSUs with the range specified. The communication taking place between the vehicles is multihop 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 tunneling data. The vehicle density of the road network is presented with HACO comparing to existing security games for vehicular network.

The below Table 3.1 describes the action of vehicles with density to enhance game theoretic approach for VANET. The probability of vehicle density in different road network scenarios is presented according to the HACO.

<table>
<thead>
<tr>
<th>No. of Vehicles</th>
<th>Vehicle Density (vehicles/km)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Games</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>25</td>
</tr>
<tr>
<td>8</td>
<td>39</td>
</tr>
<tr>
<td>10</td>
<td>44</td>
</tr>
<tr>
<td>12</td>
<td>51</td>
</tr>
<tr>
<td>14</td>
<td>66</td>
</tr>
</tbody>
</table>
Figure 3.9 given below compares the strategies of both the security games [65] and the HACO. The vehicles travel fast with high density in HACO about 10-20% compared to security games. As the HACO identifies both known opponents and unknown opponents recognizing the vehicles increasing the speed.

![Graph of No. of Vehicles vs. Vehicle Density](image)

**Figure 3.9 No. of Vehicles vs. Vehicle Density**

### 3.5.2 Average Speed

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.

The below Table 3.2 describes the average speed involved in vehicle traveling in vehicular network. Based on the above Table 3.2 a graph is depicted as follows
Table 3.2 Tabulation for Average speed

<table>
<thead>
<tr>
<th>No. of Vehicles</th>
<th>Average Speed (km/h)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Games</td>
</tr>
<tr>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>10</td>
<td>35</td>
</tr>
<tr>
<td>15</td>
<td>43</td>
</tr>
<tr>
<td>20</td>
<td>56</td>
</tr>
<tr>
<td>25</td>
<td>69</td>
</tr>
<tr>
<td>30</td>
<td>71</td>
</tr>
</tbody>
</table>

The below Figure 3.10 represents the average speed possibility rate of the proposed Heuristic Based Ant Colony Optimization technique. Normally, in the urban scenario, there is a high possibility of speed. The average speed of vehicles is increased in HACO around 20-25% compared to security games [65]. As the speed probability rate is high, the HACO 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.

Figure 3.10 No. of Vehicles vs. Average Speed (km/h)
3.5.3 Centrality Measures

Centrality metrics are designed such that the highest value indicates the most central node. The vehicle density and betweenness centrality values comparison are depicted below.

The below Table 3.3 describes the vehicle densities over a certain period of time for days of the week. Based on the above Table 3.3, a graph (Figure 3.11) is depicted. The below graph (Figure 3.11) centrality indicates how long the parallel communication to all other nodes would take at most.

<table>
<thead>
<tr>
<th>Vehicle Density</th>
<th>Centrality Measures (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Games</td>
</tr>
<tr>
<td>5</td>
<td>41</td>
</tr>
<tr>
<td>10</td>
<td>56</td>
</tr>
<tr>
<td>15</td>
<td>62</td>
</tr>
<tr>
<td>20</td>
<td>78</td>
</tr>
<tr>
<td>25</td>
<td>89</td>
</tr>
<tr>
<td>30</td>
<td>91</td>
</tr>
</tbody>
</table>

The below Figure 3.11 specifies the centrality measures carried out depending on the vehicle density. The percentage of centrality measures is high in HACO about 5-10 % compared to security games [65]. The betweenness 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.
3.5.4 Data Traffic

In HACO formulations, the data traffic model is essentially taken into account when characterizing the vehicular network and in deciding the payoff matrices.

The data traffic of vehicles in vehicular network is illustrated in below Table 3.4 based on which a graph is depicted as follows.

Table 3.4 Tabulation for Data Traffic

<table>
<thead>
<tr>
<th>Time (Hours)</th>
<th>Data Traffic (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Games</td>
</tr>
<tr>
<td>1</td>
<td>416</td>
</tr>
<tr>
<td>2</td>
<td>667</td>
</tr>
<tr>
<td>3</td>
<td>828</td>
</tr>
<tr>
<td>4</td>
<td>1083</td>
</tr>
<tr>
<td>5</td>
<td>1296</td>
</tr>
<tr>
<td>6</td>
<td>1417</td>
</tr>
</tbody>
</table>
The below Figure 3.12 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 HACO and the speed of data sending is increased around 20 - 25 % compared to security games [65]. The reason for reduced data traffic is due to a new road path explored with traversal of ants based on heuristic ant-colony optimization.

![Figure 3.12 Times (hr) vs. Data Traffic (kbps)](image)

**Figure 3.12 Times (hr) vs. Data Traffic (kbps)**

Finally, the experimental conclusion of HACO scheme works well and provides defensive measures to enhance an effective communication among the nodes in the network.

### 3.6 CONCLUSION

The Heuristic-based 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 behavior of attacker. Globally best solutions are identified using heuristic-based 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.