CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

VANET is largely measured to present security associated information, traffic association, and infotainment services. The VANET security is reinforced using vehicle mode analysis enhancing the Heuristic based ant-colony optimization of game theory with improved Nash equilibrium integrated Markov chain. The existing technology - security games for vehicular network improves game theoretic approach. The limitation of security games is more attacks are unsolved in providing VANET security.

A Heuristic Based Ant Colony Optimization is presented to improve the game theoretic approaches for VANET security. The security game is computed by mapping centrality metrics where the numerical analysis is based on sensible simulation data obtained from traffic engineering systems. Ant colony optimization used as heuristic optimization, discovers the globally best solution. To improve game theoretic approach in VANET security, MC (Markov Chains) and NE (Nash Equilibrium) are used and NE is computed based on the game model. A new defensive mechanism is then presented to improve the game theoretic approaches for VANET security.

A novel scheme for reinforcing security level of game theoretic approach for VANET is presented which consists of skeleton for mode
analysis modules using which the effectiveness and trust of the vehicle is determined in road network path. This novel scheme differentiates between three statuses: reliable, unreliable and impartial vehicles. Simulation results have been conducted to evaluate the performance of the proposed security measures in game theoretic approach in VANET and the security level of the network environment.

To start with the security of VANET is improved using the proposed Heuristic based ant-colony optimization (HACO). HACO provides high security to VANET by solving the problems of attack modeling, optimization of response actions and allocation of defense resources. The attacks on availability, authentication, driver’s confidentiality, privacy, non-repudiation and data trust are detected by HACO based on the centrality betweenness of game theory. In addition, known and unknown opponents of game theoretic approach are evaluated. The heuristic based ant model evaluates both known and unknown opponents. The performance of HACO is estimated with parameters such as trustworthiness, probability of attacks, security and time-sensitive communication. Experimental evaluation is performed with merits using sample dataset which shows performance improvement of 60% defensive measures for mitigating malicious nodes in the network.

Further, Game theoretic approach pay attention on VANET security using Nash Equilibrium integrated with Markov Chains (NEIMC). The security related issues in VANET block the protection against secured communication. The security issues such as DoS attacks, bottlenecks and intruders are solved by NEIMC. Markov Chains are chosen to evaluate the appropriate model for security related issues in VANET. An efficient game model is implemented based on the issues related to VANET environment using Markov Chain.
Based on the game model, the Nash Equilibrium is computed efficiently which reduces the issues related to security over VANET. The better performance of NEIMC is showed with parameters like vehicle density, performance rate, privacy conservation and vehicle speed both in upward and downward direction. Numerical analysis is executed depending upon simulation data obtained from traffic engineering systems which showed 40% improvement in game theoretic approach for VANET security using NEIMC.

Finally, HACO and NEIMC are combined to reinforce the security across VANET. The heuristic ant colony optimization based Game theory with Nash Equilibrium integrated Markov Chain for Reinforcing Security is presented. The security of VANET is reinforced using vehicle mode analysis. The vehicle mode analysis determines the effectiveness and trust of the vehicle in road network path. The reinforcing security using vehicle mode analysis (RSVMA) differentiates the status of reliable, unreliable and impartial vehicle.

The misbehavior of the opponents played in the game is determined. The performance of RSVMA is determined with attributes such as trustworthiness, probability of attacks, security and time sensitive communication. The simulation results have been conducted to evaluate the performance of the reinforcing security measures in game theoretic approach in VANET. The security level of the network environment is comparably 78% high in the reinforcing security using vehicle mode analysis.

7.2 FUTURE WORK

A Heuristic based Ant-colony Optimization (HACO) is performed in forwarding message across vehicular network similar to the action of ants overcoming attacker knowledge. The HACO technique does not consider the
fault tolerance issues faced by the information. The addition of fault tolerance issues in the future researches is required.

The Markov Chain model characterizes the hackers on basis of two criteria to classify them viz., motivations and skills. If the attacker is highly skilled then Markov chain consumes more time in evaluating the motivation of attackers. So, time consumption for transition rate is high along with the increased computation cost. The transition rate is evaluated on the basis of categories of hackers and skill distribution.

Reinforcing security for VANET using vehicle mode analysis provides a trusted communication over V2V or vehicle to road side units. The limitation of RSVMA technique is that it is more efficient if cluster is formed across network in VANET communication. So, the research work is proceeded to implement the total information communication in cluster mode for a complete VANET environment.