communication capabilities among the vehicles, while RSUs are placed along the road and constitute the network infrastructure. RSUs work as a router between the vehicles. Communication is done in between the vehicle to vehicle, vehicle to road side unit and road side unit to road side unit.

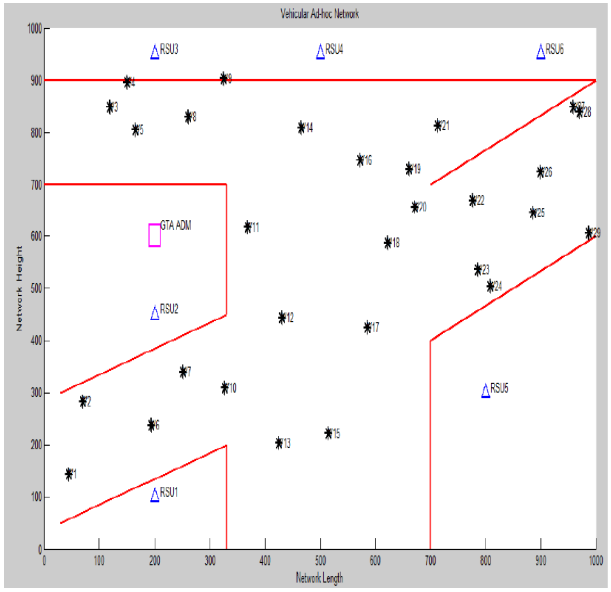
This paper is mainly focused on Security. Security is the main issue in VANET. The security issues must be addressed and solved by the successful deployment of VANETs. VANET requires security to employ the wireless environment and serves users with safety and non-safety approaches. Attacker produces distinct kinds of attack in the vehicular environment. The aim of the attacker is to establish issues for rest of users by modifying the message content in the network, so proper mechanisms need to be implemented for detecting and avoiding the malicious nodes. Therefore my work is mainly towards the detection of malicious nodes in Vehicular Ad-hoc networks and securing the VANET node and monitoring with trust based system and use of Ant bee colony optimization so, that packet drops and overhead reduced by this.

2. Objectives

1) Detecting the malicious vehicles using Trust based system.
2) Implementation of Ad-Hoc On-Demand Distance Vector routing and optimization of the approach with Ant Bee Colony algorithm.
3) Evaluation of parameters such as transmit, risk and the trust values.
4) To validate the proposed approach with the existing one.

3. Proposed Work

Selective forwarding attack in which malicious nodes acts as a normal nodes so we are finding the malicious nodes with trust based system. Firstly the deployment of vehicles in the networks then we performed the authentication of vehicles on the basis of GTA (Government transportation authority). By finding the source and destination nodes and coverage area then Ad-Hoc On-Demand Distance Vector routing is performed. Malicious nodes are detected on the basis of trust based system. Only trusted nodes carry the data. RSU (road side unit) are deployed in every block so that they communicate with the nodes and collect all the data of the malicious nodes. RSU transfer the collected data to GTA and send a report to GTA. Ant Bee Colony optimization is held on this process to improve the performance of the system. Evaluation of parameters on the basis of transmit, risk, packet delivery and the trust values are calculated.



Proposed System Architecture

Simulation Parameters	Values
1. Simulator	MATLAB 2013
2. Simulator Area	1000*1000
3. Number of Nodes	30
4. Simulation time	300 sec

Parameters for proposed architecture

4. Assumptions

The following underlying assumptions have been made to evaluate the efficiency of proposed approach for urban environment. This approach has been designed for security in case of urban scenario. If the overhead increases, then we have to go for optimization. The randomness of vehicle has to be

reduced, ie less is the randomness of vehicle, more stable is the state of vehicle, than the packet drop will be reduced. The mechanism attached with RSU and send report to the GTA.

1) RSU is used for monitoring the malicious nodes and recording the data and send to the GTA. RSU are set on every block in the network.
2) Implemented on highways where all the paths are already known.
3) Work is done in the low density area.
4) Amount of malicious nodes always less than the normal nodes in the network.

5. Performance and Evaluation

5.1. Computation parameters

Here we evaluate the four parameters in our proposed work by using Ant Bee Colony optimization:
1) **Transmit:** It shows the probability to delivery of packets.
2) **Risk:** It shows the risk rate methods in malicious nodes for the high speed and the low
speed.
3) **Trust:** Trust Based system is used for finding the trusted values.
4) **Packet delivery**: Successful delivery of a packet over the network.

5.2. Simulation Results

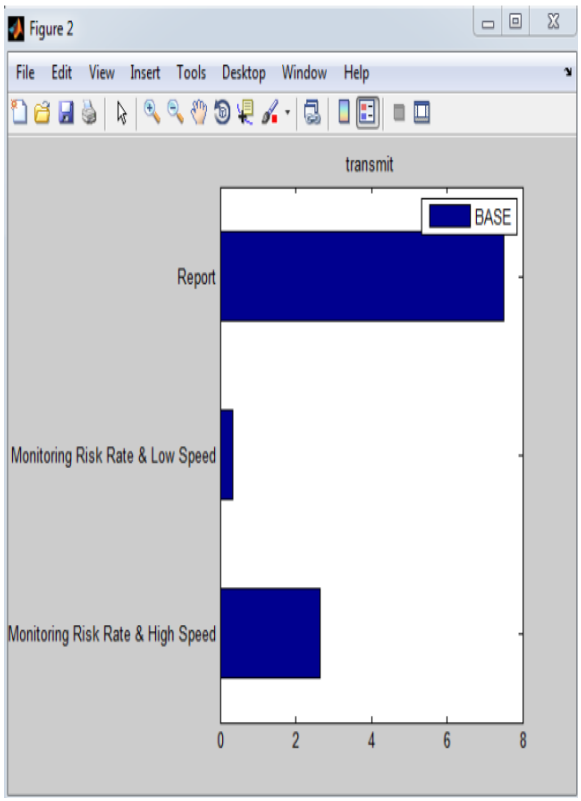
For determining the efficiency of the system by finding the malicious nodes from the trust based system, we improve the performance of the system. Here we compare the results with the existing system. Perceptions are made by considering different parameters and in this manner looking at them against the new parametric values on the Vehicular Ad-hoc networks.

By doing the proposed model with the current one, results are appeared for the vehicles in the system whose main motive is just drop the data packets and change the integrity of data. We are just improving the stability of the system. So, by this proposed system we can enhanced the security of the Vehicular Ad-hoc network. On the basis of trusted based model we are finding the highly trusted nodes. Firstly find the nodes for routing with Ad-hoc on demand distance vector protocol then we are focusing on finding the malicious vehicles, low trust vehicles, high trust vehicles and the common nodes vehicles. Malicious nodes are then communicate with the Road side unit and road side unit save the locations of the vehicles and send all the information to the Government transportation authority in the form of reports.

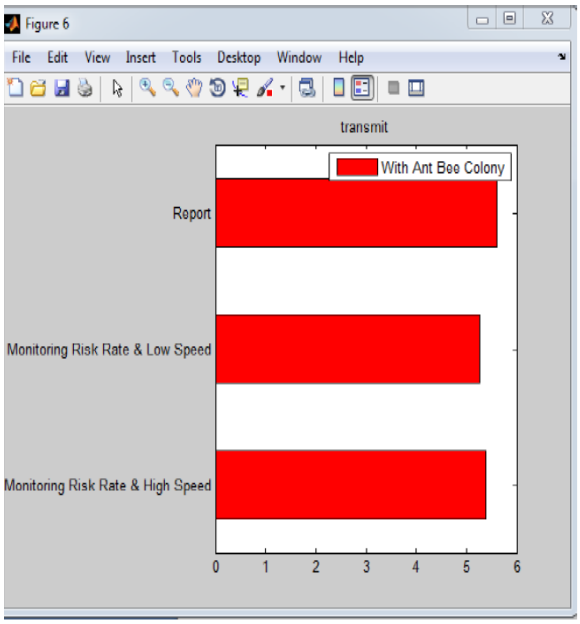
The Results are observed from different parameters. After studying the proposed model with the existing one four parameters are concluded that are: transmit, risk, trust and packet delivery.

Evaluation of transmit:

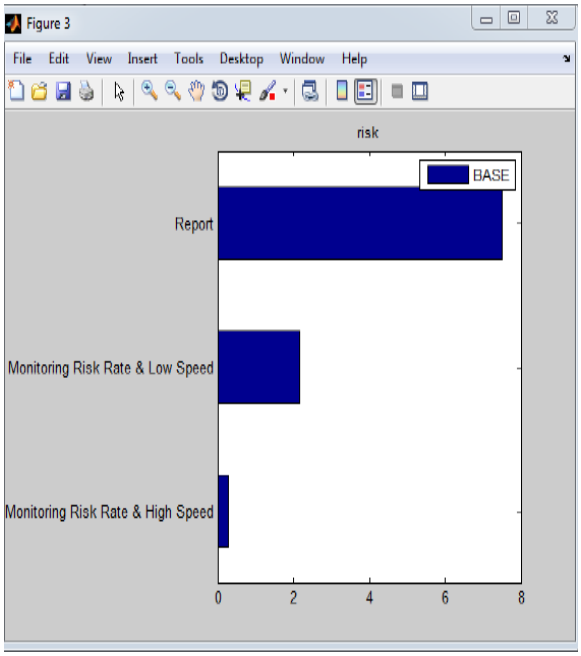
Here we are considering the two methods for comparison, first one is the report and second one is the detection of driving patterns. On comparing the results of existing approach and the proposed approach, proposed approach comes out as a better then the existing one. Here the optimization is being done with the Ant Bee Colony algorithm.



Transmit Parameter without optimization



Transmit Parameter evaluation after optimization

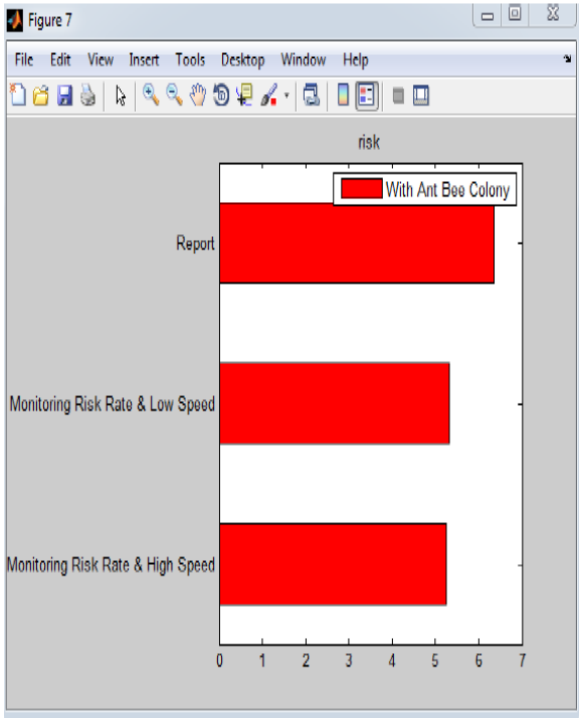


Risk evaluation without optimization

As the results are being compared when it comes to the monitoring risk rate, there is increase in detecting the risk for data transmission in case of proposed approach. When vehicles are moving at a high speed they are in the unstable state which is leading to increase in data transmission risk. So it depicts we should focus much more on monitoring the risk rate at higher speed as compared to the lower speed nodes.

Evaluation of Risk:

Here we are considering the two methods for comparison, first one is the report and second one is the detection of driving patterns. On comparing the results of existing approach and the proposed approach, proposed approach comes out as a better then the existing one. Here the optimization is being done with the Ant Bee Colony algorithm. When it comes to compare the average risk for various driving pattern, slower speed vehicles appear to have a higher risk rate, which is depicting slower speed vehicles are having higher risk while transmitting the messages. This further leads to the affect on wide area network as they are not monitored completely. With the help of optimization algorithm monitoring the risk rate at slower speed has been taken into consideration.

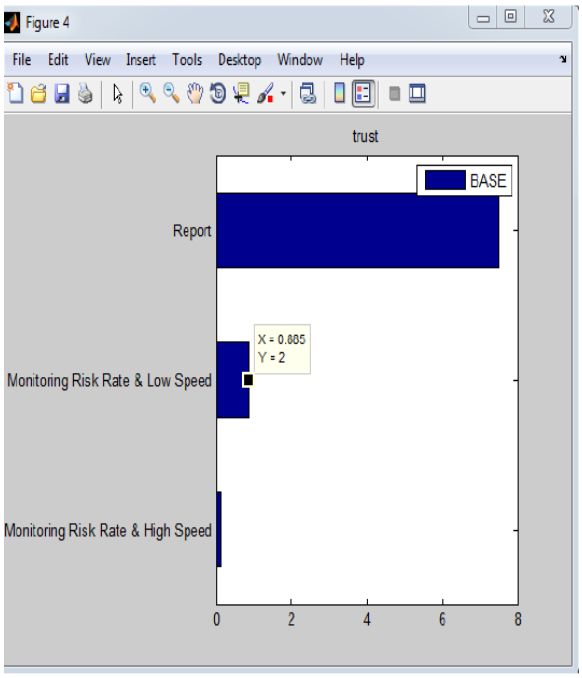


Risk evaluation with optimization

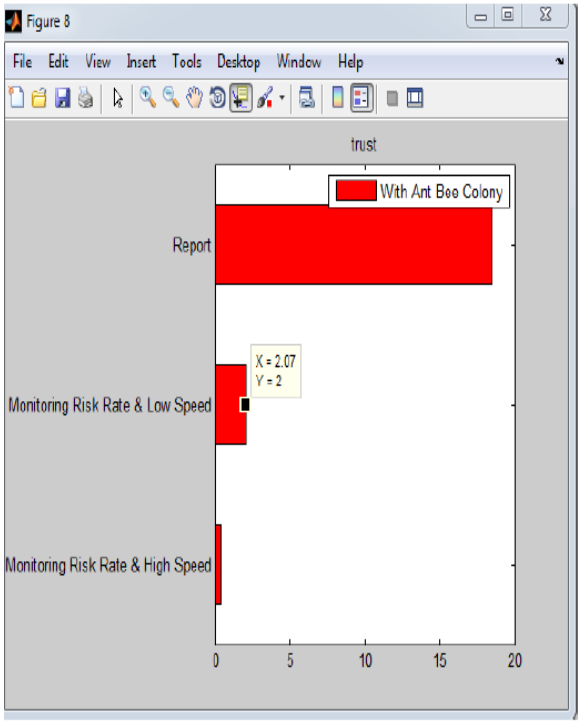
Evaluation of Trust:

The below is supporting the assumption of nodes with the higher speed are having the decreased trust value in comparison the report methods. So the risk

rate detection method is working accurately for the higher speed nodes in comparison of the slower ones.



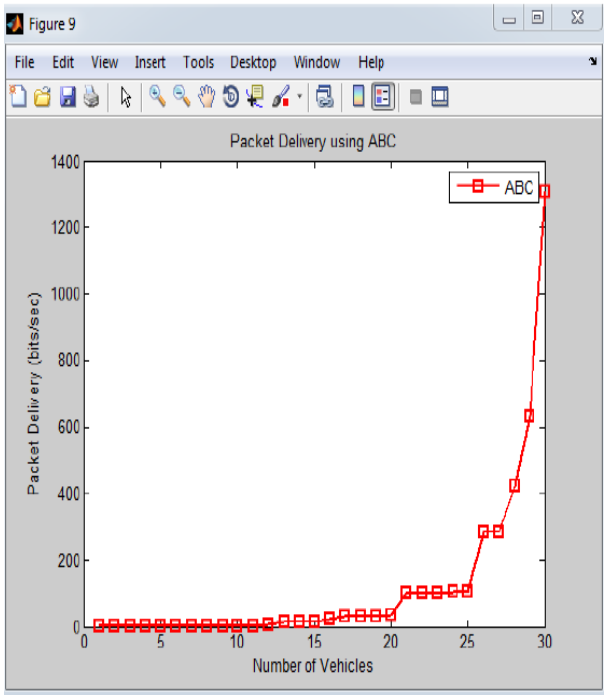
Trust evaluation without optimization



Trust evaluation with optimization

Packet Delivery Ratio:

Increase in the number of vehicles is leading to increase in the network connectivity which is further reducing the chances of encountering network partition. When the density of network is sparse, vehicles are scattered, connectivity of the network becomes bottleneck, which is restricting the improvement in case of routing performance. With increase in the number of vehicles there is a increase in packet delivery ratio.



Packet delivery ratio with ABC optimization

6. Conclusion

We have proposed a system which is detecting the malicious node which appears to be a normal node. By detecting these nodes in the Vehicular Ad-hoc network we are improving the stability and performance of the system. Our work is taking into consideration how to improve the packet delivery ratio by the detection of malicious nodes and further enhancing the security of our system. Simulation results have shown that the proposed approach is better in terms of transmit, risk and the trust value of the nodes. These parameters are compared on the basis of two methods such as Vehicle behavior

patterns and the Report. Our work is mainly focused on the compromised nodes and reducing the affect of these nodes in the Vehicular Ad-hoc networks. GTA (government transportation authority) is use as a admin for storing the locations of malicious nodes and capture process is done with the help of RSU. Therefore, by decreasing the malicious nodes and improving the routing with Ad-hoc on demand distance vector our network contribute to increased availability and performance of the system.

7. Future Work

Though our proposed work tried to introduce the model which is detecting the malicious nodes but still the work is pending. In this current scenario we are just detecting the malicious nodes and these nodes are storing in the GTA but further process is still remaining like blocking of the malicious nodes. We are not addressing any particular attack on general communication so in our further study we can redesigned the attacks also. Apart, from this we can also improve the Vehicle behavior patterns approach, for increasing the system performance and availability. For increasing the security of the whole network we can also work on the data security standards with AES and DES approach for encrypting the data packets. So, by adding some further steps or techniques we can easily enhance more security in the system.

8. REFERENCES

[1] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," *IEEE, 2007,* 2007 pp. 26–30.

[2] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, 2007, vol. 15, pp. 39–68.

[3] Y. Qian and N. Moayeri, "Design of Secure and Application-Oriented VANETs," *IEEE,* 2008, vol. 24, no.1, pp. 2794–2799.

[4] X. Lin, R. Lu, C. Zhang, H. Zhu, and P. Ho, "Security in Vehicular Ad Hoc Networks," *IEEE Communications Magazine* , 2008, vol.15, no. 4, pp. 88-95.

[5] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, 2008, vol. 16, no. 1, pp. 1–15.

[6] T. W. Chim, S. M. Yiu, and L. C. K. Hui, "SPECS : Secure and Privacy Enhancing Communications Schemes for VANETs," 2011, vol. 9, no. 2, pp. 189–203.

[7] Z. Baniasadi, A. Sanei, M. R. Omidi, and E. Eslami, "Modeling Composite Intrusion Detection Systems Using Fuzzy Description Logics," *International Symposium on Computer Networks and Distributed Systems (CNDS)*, 2011, pp. 1–6.

[8] A. Rawat, S. Sharma, and R. Sushil, "VANET : SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS," *Journal of Information and Operations Management***,** 2012, vol. 3, no. 1, pp. 301-304.

[9] B. Ding, Z. Chen, Y. Wang, and H. Yu, "An Improved AODV Routing Protocol for VANETs," *IEEE,* 2011, vol. 7, pp. 1-5.

[10] F. A. Ghaleb, "Security and Privacy Enhancement in VANETs using Mobility Patterns," International Journal of Electronics, 2013, vol. 5, pp. 184-189.