International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A LITERATURE REVIEW ON VEHICULAR AD-HOC NETWORKS

Nivedita Kalia[1], Navjot Kaur[2]
[1]Deptt. of CSE, Chandigarh Engg. College,
Mohali, Punjab, India.
[2]Associate Professor
Deptt. of CSE, Chandigarh Engg. College,
Mohali, Punjab, India.
[1]niveditakalia@gmail.com, [2]cecm.cse.navjot@gmail.com

Abstract: *Vehicular ad hoc network is a rising new technology that integrates ad-hoc network, wireless local area network and cellular technology to achieve intelligent inter-vehicle communications and get better road travel security and efficiency. VANETs are illustrious from other kinds of ad hoc networks by their hybrid network architectures, node movement individuality, and new application scenario. Therefore, VANETs pose many unique networking research challenges, and the design of an able routing protocol for VANETs is extremely vital. In this expose, we converse the research challenge of routing in VANETs and review recent routing protocols and related mobility models for VANETs [2].*

I. INTRODUCTION

VANETs are particular kind of Mobile Ad Hoc Networks that are shaped between moving vehicles on an as-needed basis. VANET is a rising technology, which enables a wide range of applications, including road security, passenger expediency, infotainment and intelligent transport. They help to create safer roads by disseminate information regarding the road situation and traffic scenario among the participate vehicles in a timely manner. Along with the safety application, VANETs broadcast valuable, real-time information to the user such as transfer systems, weather information, mobile, internet access and other multimedia applications [3]. VANETs enable computerized highway applications, where the vehicles are able to sail without the help of their drivers, even though such applications have not yet become realistic. VANETs inherit some of the individuality such as mobile nodes and self-organizing behavior from MANETs. However, VANETs possess certain unique individuality such as high mobility of nodes, time varying density of nodes, frequent disconnections, highly partitioned network and vigorously changing topology, which makes them more demanding. It is a confront to construct networks between vehicles and guarantee reliable, continuous and secure communication among the vehicles in motion. Routing in VANETs is a key issue. This paper focus on the issues connected to routing in VANET environment and presents a detailed review of various routing protocols for vehicular ad hoc networks [4].

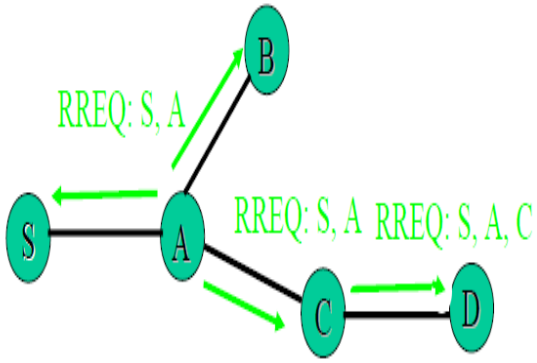
II. DSR PROTOCOL EXPLANATION

Dynamic Source Routing is a routing protocol for Ad-HOC networks. It is comparable to AODV in that it forms a route on-demand when a transmit computer requirements one. However, it uses source routing in its place of relying on the routing table at each middle device. This protocol is truly based on source routing where by all the routing information is maintain at mobile nodes. The DSR protocol is collected of two mechanisms that work together to allow Route Discovery and Route Maintenance of source routes in the ad hoc network.

2.1 Route Discovery in DSR

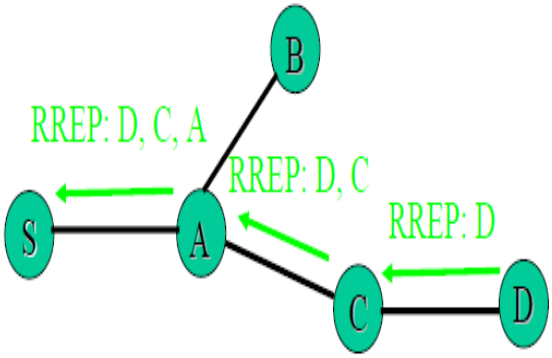
When node S wants to send a packet to node D, but does not know a way to D, nodes S initiate a route finding. Source node S floods the network with route request packets. Both nodes append its own address in the packet description when forward RREQ. End D on getting the first RREQ sends a path Reply. RREP is sent on a route obtained by reversing the route appended to receive RREQ.RREP includes the reverse

route from S to D on which RREQ was received by node D.



2.2 Route Maintenance in DSR

The path maintenance method assures that the routes saved in the path cache are validated. We assume that all nodes wishing to converse with other nodes within the ad hoc network are ready to participate fully in the protocols of the network. Every node participate in the network should also be willing to forward packets for other nodes in the network. If the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route preservation indicates a source path is busted, S can challenge to use any other route it happens to know to D, or it can appeal to Route Discovery again to find a new route for following packets to D. Route preservation for this route is used only when S is actually sending packets to D.



III. SECURITY ATTACK

Securing wireless ad-hoc networks is an extremely demanding issue. Kindly possible form of attacks is always the first step towards rising good security solution. Security of communication in MANET is important for secure transmission of information. Nonexistence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital or cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be secret into two types:

3.1 Passive Attacks

Passive attacks are the attack that does not disturb proper operation of network .Attackers snoop data exchange in network without changing it. Requirement of privacy can be violated if an attacker is also able to interpret data gathered through inquisitive .Detection of these attack is difficult since the operation of network itself does not get precious.

3.2 Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to execute the attacks. Energetic attacks involve some alteration of data stream or creation of false stream. Active attacks can be two parts:
1. Internal
2. External.

3.2.1 External attacks are carried out by nodes that do not belong to the network.

3.2.2 Internal attacks are from compromised nodes that are part of the network. Because the attacker is by now part of the system, interior attacks are more cruel and hard to detect than exterior attacks. Energetic attacks, whether carried out by an external advisory or an internal compromised node involves actions such as imitation, alteration, production and duplication.

3.3 Mobile vs. Wired Attackers

Mobile attackers have the same ability as the other nodes in the ad hoc networks. Their capabilities to harm the networks operations are also limited because of defective resources. With the limited transmit ability and battery powers; mobile attackers could only jam the wireless links within its region but not the whole networks operations. Wired attackers are attackers that are capable of gaining access to the external resources such as the electricity. Since they have more resources, they could commence more severe attacks in the networks, such as congestion the whole networks or breaking expensive cryptography algorithms. Survival of the wired attackers in the ad hoc networks is always possible as long as the wired attackers are able to locate themselves in the communication range and have access to the wired infrastructures.

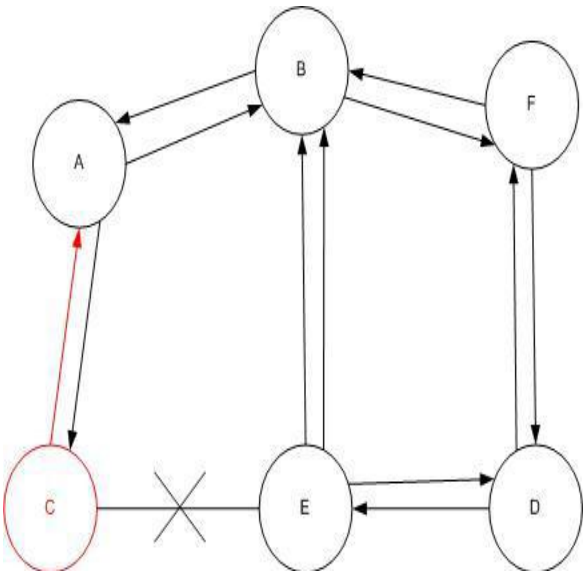
3.4 Single vs. Multiple Attackers

Attacker might choose to begin attacks against the ad hoc networks separately or by collude with the other attackers. Single attackers typically generate a reasonable traffic load as long as they are not competent to reach any wired services. Since they also have similar ability to the other nodes in the networks, their limited capital become the weak points to them. If several attackers are collude to launch attacks, distrustful the ad hoc network against them will be a good deal harder. Collude attackers could easily close behind any single node in the network and be capable to degrading the efficacy of network's dispersed operations including the security mechanism.

IV. BLACK HOLE ATTACK

VANETs face different securities coercion i.e. attacks that are approved out against them to upset the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Vehicular Ad-Hoc networks. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to interrupt.

This unfriendly node advertises its availability of fresh routes irrespective of checking its direction-finding table. In this way invader node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the nasty node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is set up, now it's up to the node whether to drop all the packets or forward it to the unknown address.



Black hole attack is a kind of Denial of Service attack possible in wireless ad-hoc network. In this attack, a mean node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to interrupt. The attacker absorbs transmitted data from source to destination and drops all this data or forwards it to unidentified address. As a consequence, the start and the end nodes become unable to communicate with each other this attack can be classified according to the source of attack, the behavior of attack and the group of work. External Black hole: it is outside the network and when it gets access to the network it will deny the access in the direction of the network. It causes denial of service in order to disturb the presentation of the whole network. [6] [7].

Internal Black hole: it is a node being part of the network that impersonates and starts its malicious behavior. Internal attack is more dangerous than external attack.

Active attack: it steals important information and modifies it and fabricates the messages to destroy the performance of the network. The active attack can be an internal or an external attack.

***Passive attack*:** it listens to the network in order to know and understand how the nodes communicate with each other. So the attacker has enough information about the entire network to easily hack the network. Black hole attack can be done by single or cooperative malicious node, where Cooperative Black hole means the cruel nodes act in a group.

V. OPTIMIZATION ALGORITHM

In optimization of a design, the design objective could be simply to minimize the rate of production or to maximize the competence of manufacture. An optimization algorithm is a procedure which is executed iteratively by compares various solutions till an optimum or a satisfactory explanation is established. With the advent of computer, optimization has become a part of computer-aided design activities.

5.1 Bacterial Foraging Algorithm (BFO)

Bacteria Foraging Optimization algorithm is a novel class of in nature certain stochastic global search method based on imitate the foraging actions of E.coli bacteria. This method is used for locate, conduct, and ingesting the food. Through foraging, a bacterium can

exhibit two unlike events: dropping or swim. The topple action modify the direction of the bacterium. During swim means the chemo taxis step, the bacterium will move in its recent direction. Chemo taxis society is continuous until a bacterium goes in the way of positive-nutrient gradient. Following a sure number of complete swims, the best halve of the population undergo the simulation and eradicate the rest of the population. In order to run off local optima, an ending dispersion event is carried out where some bacteria are clear up at random with a very small opening and the new stand-in are initialized at random locations of the search space. The Chemo taxis activities of E. coli bacteria making an allowance for the foraging behavior of E. coli, it has a common type of bacteria with a diameter of 1µm and a length of about 2µm and which under suitable conditions can replicate in 20 min. It is the ability to move comes from a set of up to six rigid 100–200 spinning flagella, each driven by a biological motor. The E. coli bacterium alternates between running and tumbling. When the flagella are rotate in clockwise, they work as propellers and hence an E.Coli may be run or fall. The Chemo taxis Actions are below:
(A1) If in impartial medium, the rotate tumbles and the runs ⇒ search.

(A2) If swim up in a nutrient of the rise or out of the noxious substances, swim longer ⇒ seek all the time more positive environments.

(A3) If swim down the nutrient of the ramp, then search ⇒ to keep away from adverse environments.

5.2 Genetic Algorithm

Genetic algorithms have been used in skill and manufacturing as adaptive algorithms for solve sensible harms and as computational models of normal evolutionary systems. This brief, easy to get to foreword describe a little of the majority attractive investigate in the field and also enable reader to apply and trial with genetic algorithms on their have. It focus in deepness on a small set of vital and attractive topics -- mainly in mechanism learning, systematic modeling, and artificial life -- and review a large extent of discover, including the work of Mitchell and her generation [8] . The images of application and model project widen outside the harsh borders of computer science to include dynamical systems premise, game theory, molecular ecology, ecosystem, evolutionary biology, and populace genetics, underscore the stirring "general purpose" nature of genetic algorithms as search method that can be working across discipline. A preface to Genetic Algorithms is available to students and researchers in any methodical discipline [9]. It includes many thinking and computer movements that build on and strengthen the reader's kind of the text. The first chapters introduce genetic algorithms and their terms and describe two challenging application in feature. They look at the use of genetic algorithms in machine learning (computer programs, data analysis and neural networks) and in scientific models (interactions among learning, evolution, and culture; ecosystems; evolutionary activity). Several approaches to the premise of genetic algorithms are discussed in depth. The next takes up implementation and the last chapter poses some currently unanswered questions and surveys prospects for the future of evolutionary calculation.

Basically, Science arise from the very human know and control the world. We human can slowly build up a grand structure of information that enables to predict and to vary extents. More recently we have even come to understand some basic limits to our abilities to predict. The goals of creating reproduction intellect and artificial life can be traced back to the very foundation of the computer age.

Given a clearly define a problem to be solved and a bit string symbol of applicant solutions, A simple Genetic algorithm work as follow:

1) Start with an arbitrarily generate population of n l-bit chromosomes.
2) Analyze the fit f(x) of each chromosome x in the populace.
3) Repeat subsequent steps until n offspring have been created.

5.3 ACO Algorithm

The combinatorial optimization problem is applied to various production fields. There is the shortest path problem in one of such the combinatorial optimization problems. It can be classified into two categories [13]. One is the problem for the search on the grid. The other is that for the search on the graph. Maze algorithm which was proposed by Lee is the routing algorithm for the former category, and it is applied to VLSI CAD problems. On the other hand, Dijkstra algorithm is the routing algorithm for the latter category, and it is applied to route guidance problem such as car navigation system. These routing algorithms find the shortest path, whenever the path exists. However, they have the inherent processing time on the searching process. Recently, many researchers study the meta-heuristics which can find the sub-optimal solution at small time. In these meta-heuristics, it is reported that Ant Colony Optimization, which is stimulated by

feeding performance of ants, show the better ability than Genetic Algorithm and Simulated Annealing when it is applied to Traveling Salesman Problem. In this paper, we propose a new routing algorithm using Ant Colony Optimization. The proposed algorithm deals with the route searching problem represented by the graph representation. In the route searching problem, the moving destination has been incomplete unlike TSP. Therefore, there is a possibility that the ant agent is trapped in the blind alley. Thus, the proposed algorithm combines Tabu search algorithm with ACO to overcome this problem. Moreover, experiment compared with Dijkstra algorithm proves the validity of the proposed algorithm [14].

5.4 BCO Algorithm

A great number of traditional engineering models and algorithms used to solve complex problems are based on control and centralization. Various natural systems lecture us that very simple personality organisms can create systems able to perform highly complex tasks by dynamically interacting with each other. Bee swarm behavior in scenery is, first and primarily, characterized by autonomy and dispersed functioning and self-organizing. In the previous pair of years, the researchers started studying the behavior of social insects in an attempt to use the Swarm Intelligence concept in order to develop various Artificial Systems. The Bee Colony Optimization Meta heuristic that represents the new direction in the field of Swarm Intelligence is introduced in this paper. The main goal of this document is to explore the possible applications of collective bee intelligence in solving combinatorial problems characterize by indecision. The growth of the new heuristic algorithm for the Ride-matching problem using the proposed approach serves as a clarifying example and shows the individuality of the proposed concepts.

Table 1.1 Word done using previous techniques

Author	Description	Technique
Lokesh Malviya, Akhilesh A. Waoo M.Tech Scholar , Sanjay Sharma, PhD. Professor, MANIT BIST Bhopal India	They proposed the DSR routing with multipath routing with the concept of load balancing	Multipath routing Technique
Venkatesh, A Indra, R Murali Professor, Dept. of Mathematics, Dr. Ambedkar Institute of Technology	They proposed network architecture, applications based support, strategies based on routing, forwarding strategies, mobility models and quality of service metrics	Non delay tolerant network technique, Contention based forwarding technique, object pursuing based on efficient routing
Antonio Vincenzo Taddeo, Alberto Ferrante ALaRI, Faculty of Informatics, University of Lugano, Lugano, Switzerland	They propose a protocol to negotiate security settings for the communications. This protocol aims at minimizing the power consumption and at providing the highest possible security level associated with the communications	Peer to peer communication technique using linear programming method
Jie Luo Xinxing Gu Tong Zhao Wei Yan School of Electronics Engineering and Computer Science, PKU, Beijing, China	The concept of using buses as the mobile infrastructure to improve the network connectivity is proposed and the routing is performed using that method	Priority algorithm using shortest path

REFERENCES

1. Li, Fan, and Yu Wang. "Routing in vehicular ad hoc networks: A survey."Vehicular Technology Magazine, IEEE 2.2 (2007): 12-22.
2. Logapriya, Mrs R., and Mrs R. Kavitha. "OVERVIEW OF ROUTING PROTOCOLS FOR VEHICULAR AD-HOC NETWORKS." (2014).
3. Malviya, Lokesh, Akhilesh A. Waoo, and Sanjay Sharma. "New Load Balanced Multi-Path Dynamic

Source Routing Protocol for Mobile Ad-HOC Network."International Journal of Computer Applications (0975–8887) Volume (2013).

4. Goyal, Priyanka, Sahil Batra, and Ajit Singh. "A literature review of security attack in mobile ad-hoc networks." International Journal of Computer Applications 9.12 (2010): 11-15.
5. Raghavendran, C. H. V., G. Naga Satish, and P. Suresh Varma. "Security challenges and attacks in mobile ad hoc networks." International Journal of Information Engineering Electronic Business 5.3 (2013): 49-58.
6. Bibhu, Vimal, et al. "Performance Analysis of black hole attack in VANET."International Journal of Computer Network and Information Security (IJCNIS)4.11 (2012): 47.
7. Ahmed, Eman Farag, Reham Abdellatif Abouhogail, and Ahmed Yahya. "Performance Evaluation of Black hole Attack on VANET's Routing Protocols."International Journal of Software Engineering & Its Applications 8.9 (2014).
8. Marler, R. Timothy, and Jasbir S. Arora. "Survey of multi-objective optimization methods for engineering." Structural and multidisciplinary optimization 26.6 (2004): 369-395.
9. Thomas, Riya Mary. "Survey of Bacterial Foraging Optimization Algorithm."
10. Mitchell, Melanie. An introduction to genetic algorithms. MIT press, 1998.
11. Verma, Karan, Halabi Hasbullah, and Ashok Kumar. "Prevention of DoS attacks in VANET." Wireless personal communications 73.1 (2013): 95-126.
12. Liu, Bisheng, Jerry T. Chiang, and Yih-Chun Hu. "Limits on revocation in VANETs." 8th international conference on applied cryptography and network security. 2010.
13. Yoshikawa, Masaya, and Kazuo Otani. "Ant Colony Optimization Routing Algorithm with Tabu Search." proceedings of the International Multiconference of Engineers and Computer Scientists. Vol. 3. 2010.
14. Teodorović, Dušan, and Mauro Dell'Orco. "Bee colony optimization–a cooperative learning approach to complex transportation problems." Advanced OR and AI Methods in Transportation: Proceedings of 16th Mini–EURO Conference and 10th Meeting of EWGT (13-16 September 2005).–Poznan: Publishing House of the Polish Operational and System Research. 2005.