Proficient System Design Using Artificial Bee Colony Algorithm with B-AODV Protocol in VANET

Renuka[1], Er. Chandni Guleria[2]
[1]M.Tech , [2]Assistant Professor
Department of Electronics and Communication Enginering, Sri Sai University Palampur

Abstract **-** Vehicular specially appointed system (VANET) can essentially enhance the activity well-being and effectiveness. The fundamental thought is to enable vehicles to send activity data to roadside units (RSUs) or different vehicles. The RSUs are settled at the street sides which are utilized to interface the vehicles to each other. Every vehicle is introduced with an OBU, which is utilized to play out all calculation and correspondence errands. We implement the B-AODV routing protocol to detect the clone attack and replace the duplicate nodes in the vehicular network. We enhance the performance parameters with artificial bee colony approach. We demonstrate the proficiency benefits of the proposed conspire through execution assessments regarding calculation postponement and transmission overhead. In addition, the broad reenactment is led to confirm the effectiveness and pertinence of the proposed plot in this present reality street condition and vehicular activity.

Keywords **-** Vehicle ad-hoc network, AODV routing protocol, broadcast message and artificial bee colony.

I. INTRODUCTION

In current years, Vehicular Ad-hoc Networks have attracted a lot of kindness from the research community. The main reason of research in VANET is to improve vehicle safety by Vehicle to Vehicle and Vehicle to RSU communication. For example, in the case of an accident, a VANET should be able to warn all imminent vehicles. Nodes share information using the wireless channel in VANET [1]. VANETs can be exploited for a broad range of safety and non-safety applications, allow for value additional services such as vehicle safety, automatic toll payment, traffic [1,2] management, improved navigation, location based services such as conclusion the closest fuel station, eatery or travel lodge and infotainment applications such as long as access to the Internet. For instance, in the case of a coincidence, a VANET should be able to warn all approaching vehicles [3]. Nodes share information using the wireless channel in VANET. Malicious nodes take benefit of wireless communication environment for realizing the spoofing attacks. In such a condition, an attacker fakes its identity to deception as another node. Sybil attack is a spoofing attack in which an attacker can produce multiple identities either by forging, stealing or by using any other resources. Attackers use some or all of these identities [4] to fabricate information about traffic and/or event. An attacker can create an impression of traffic congestion to mislead neighboring nodes. It can also insert false information in the network by using the identities of non-existing nodes.

II. Overview of VANET

Vehicular networks permit [5] cars to communicate with each other and with a distinct infrastructure on the road. Infrastructures can be purely ad hoc between cars or facilitated by making use of an infrastructure. The organization typically consists of a set of so called roadside units that are connected to each other or even to the Internet [6]. VANET uses three systems: (1) Intelligent transportation systems (2) Vehicle-to-roadside communication and (3) Routing-based communication

Fig.1: Intelligent transportation systems

Intelligent transportation systems: The inter-vehicle communication conformation Figure no: 1 uses multi-hop multicast or programme to transmit traffic correlated information over multiple hops to a group of receivers. In intellectual transportation systems, vehicles need only be concerned with activity on the road forward and not behind. Vehicle-to-roadside communication: The vehicle-to-roadside communication formation Figure no: 2 characterizes a single hop transmission where the roadside unit sends a broadcast message to all prepared vehicles in the vicinity. Vehicle-to-roadside communication formation provides a high bandwidth link between automobiles and roadside units. [7].

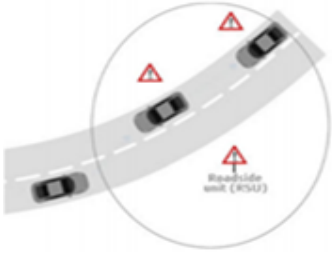

Fig.2: Vehicle-to-roadside

Routing-based communication: The routing based communication arrangement Figure no: 3 is a multi-hop unicast where a message is broadcasted in a multi Routing based announcement hop fashion until the vehicle carrying the anticipated data is reached. When the request is received by a vehicle preserving the desired piece of information, the application at that vehicle instantly sends a unicast message containing the information to the vehicle it established the request from, which is then exciting with the task of forwarding it towards the query source.

A numerous of applications are intended for these systems, some of which are already probable in some recently designed vehicles Figure no: 4

- Vehicle collision cautioning
- Safety distance warning
- Motorist assistance [8]
- Co-operative driving
- Co-operative cruise control
- Distribution of road information
- Internet access
- Map location
- Driverless vehicles [9]

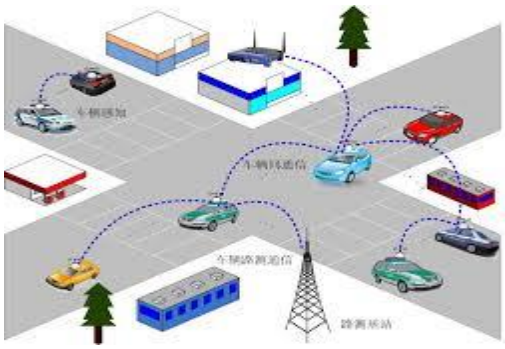

Fig.4: Various VANET applications [10]

III. RELATED WORK

Christophe J et.al (2005) describes a new model for highway traffic and events that can be used to automatically produce movement files readable by the NS-2.28 simulator. Through reproductions of such vehicular networks using flooding and IEEE 802.11 for safety-related applications [11]. **Mandeep Kaur et al,; (2016)** presented RTMU is using various mathematical computations for traffic pattern investigation to detect the aberration in data traffic between the cluster nodes. All of the nodes in the scenario are GPS location aware nodes and sharing their location actively with RTMU. Also all of the VANET nodes connect with each other through RTMU [12]. **Nikita Lyamin et al., (2014)** applied the new method for real-time detection of Denial-of-Service (DoS) attacks in IEEE 802.11p vehicular ad-hoc networks (VANETs) is planned. The study is focused on the "jamming" of periodic position messages (beacons) exchanged by vehicles in a platoon. Prospects of attack detection and false alarm are projected for two different attacker models [13].

Table no. 1 Differentiate the various techniques and Performance parameters.

Year	Attack /Technique/Model Used	Performance Parameters
2002	Modeling Highway traffic [14]	Packet, Lower Density and Higher Density
2016	AODV or TORA[15]	-
2012	Dynamic Source Routing[16]	E2E,PDR,Goodput and Throughput
2013	DDoS Intruder[17]	Detection Rate and Acceptance rate of Packets

Vinh Hoa LA et al,; (2014) present in this paper a survey of VANETs attacks and solutions in sensibly considering other similar works as well as informing new attacks and categorizing them into different classes [18].

IV. PROPOSED WORK

This section presents the used tool for the simulation of results. Also a brief for the method to generate GUI is elaborated. The proposed concept of Vehicular ad hoc network is also discussed in this section

Step I: Initialize the vehicular ad-hoc network, to create the network focus in data transmission. Vehicular nodes are plotting in a particular network to transfer the data one node to another node. The search source node and destination node for vehicular ad-hoc network.

Step II: To generate the coverage set for calculate the distance in particular range.

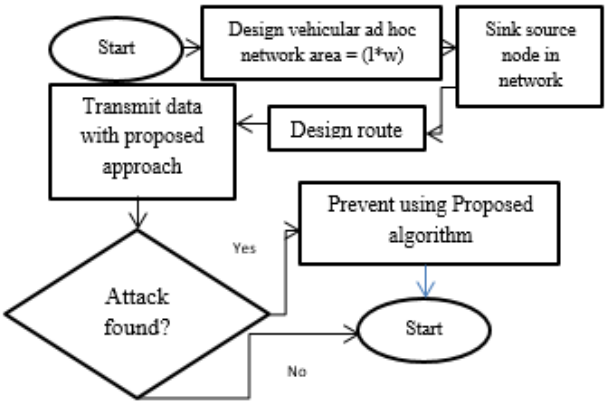

Fig.5: Proposed Architecture

Step III:. In clone attack, a challenger might detention a sensor node and reproduction the secret information to another node known as duplicated node. Then this duplicated sensor node can be connected to detention the information on the network. The challenger can also inject

false information, or influence the information passing through cloning nodes.

Step IV: We implement the Shortest on demand distance vector routing protocol. It generates the route discovery and route maintenance in the Vehicular ad hoc network. It calculates the shortest distance in the route. In the routing protocol used to detect the attacker node in the vehicle network. Information Transfer one node to another node attacker will come and loss the information in particular node. After, we detect the attacker node then calculate the performance parameters like throughput, energy consumption and packet delivery rate etc.

Step V: Implement the proposed algorithm used for mitigating the effect of the vehicle nodes in the network. We optimize the attacker effect with the help of Artificial Bee Colony Optimization with f value.

Step VI: To evaluate the performance parameters like throughput, delay and packet delivery rate and etc.

V. RESULTS AND DISCUSSION

In this section, we implemented the vehicular ad hoc network using B-AODV and ABC algorithm. We design the code based on GUI (graphical user interface). In this section we are describing the result of the vehicular ad-hoc network with road side unit, balanced on demand distance vector routing protocol and artificial bee colony optimization techniques. We explained the interface and consequences of the network.

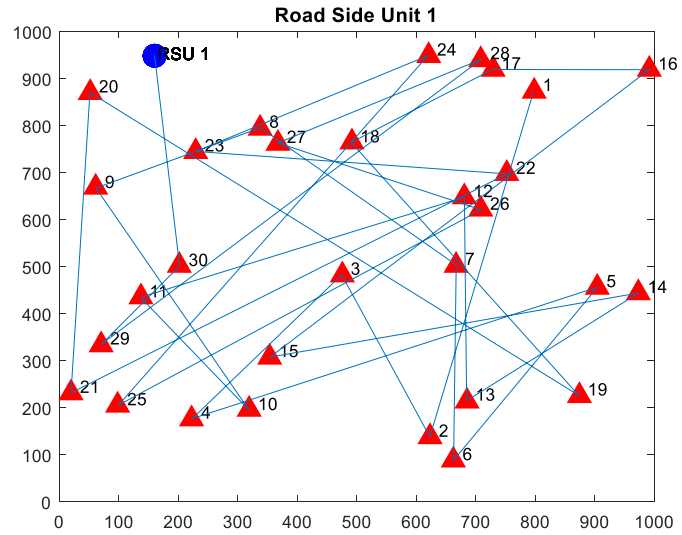

Fig.6: Road Side Unit 1 in VANET

Figure shows that, the road side unit 1 in the vehicular ad hoc network. A line format shows that the communication between one vehicular to another vehicular through the receiver points.

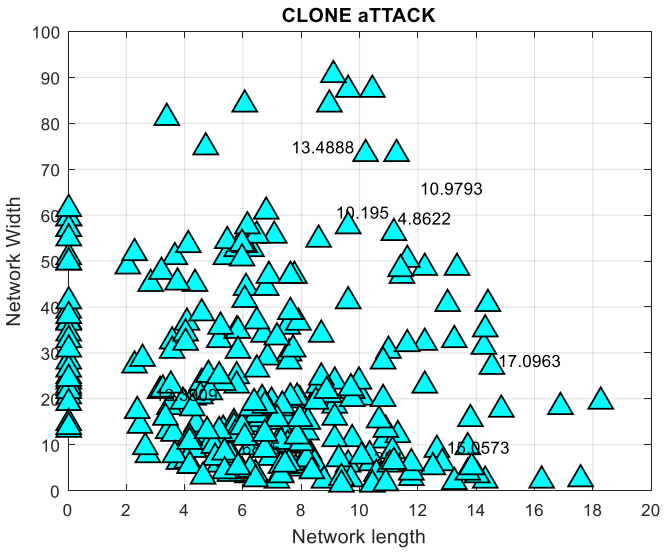

Fig.7: Clone Attack

Above figure shows that, the clone attack in the vehicular ad hoc network. Clone attack defines the multiple copies in the attacker nodes.

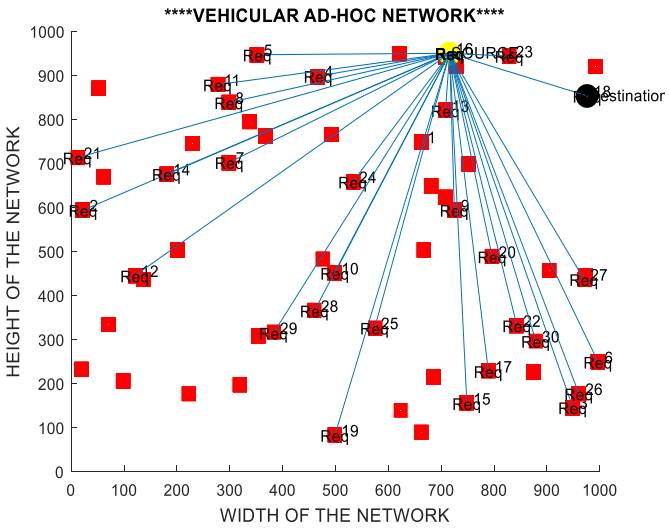

Fig.8 B-AODV Protocol

The above figure shows that the B-AODV (Balanced ad hoc on demand distance vector) routing protocol is a reactive routing protocol which establish a route when a node requires sending data packets. It has the ability of unicast & multicast defeating. It uses a terminus sequence number which makes it dissimilar from other on demand routing protocols.

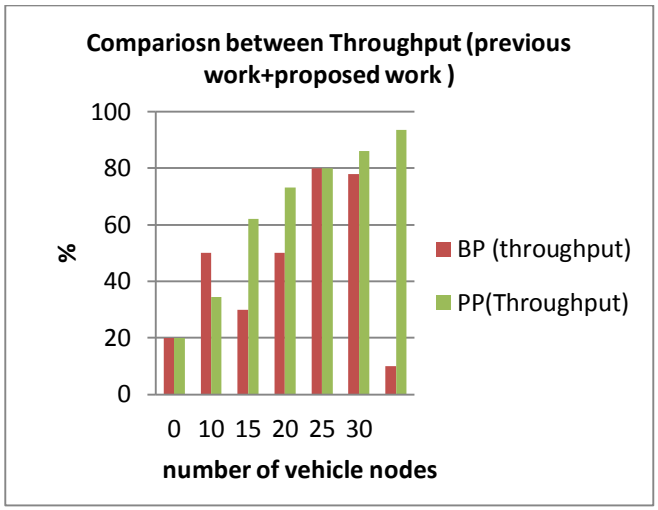

Fig.9 Comparison between Throughput using Base work and proposed work

The above figure defines the throughput value with base paper and proposed paper parameters. Throughput means to achieve the maximum accurate network to secure data transmission, but improve the performance with optimization algorithm.

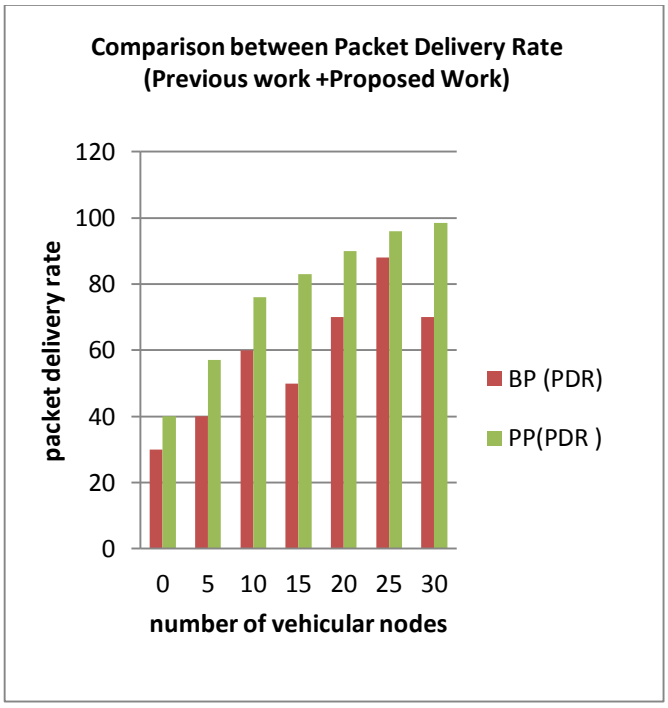

Fig.10: Comparison between Packet Delivery Rate using Base work and proposed work

The above figure defines the packet delivery rate value with base paper and proposed paper parameters. Packet delivery rate means to achieve the maximum packet sent the destination of the network to secure data transmission, but improve the performance with optimization algorithm.

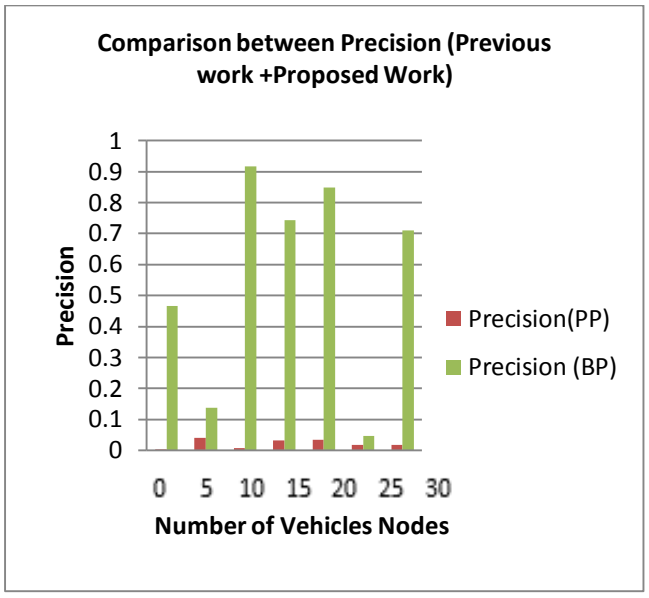

Fig.11: Comparison between Precision using Base work and proposed work

The above figure shows that the comparison between precision using base work and proposed work. We improve the performance with the true positive value in the proposed work.

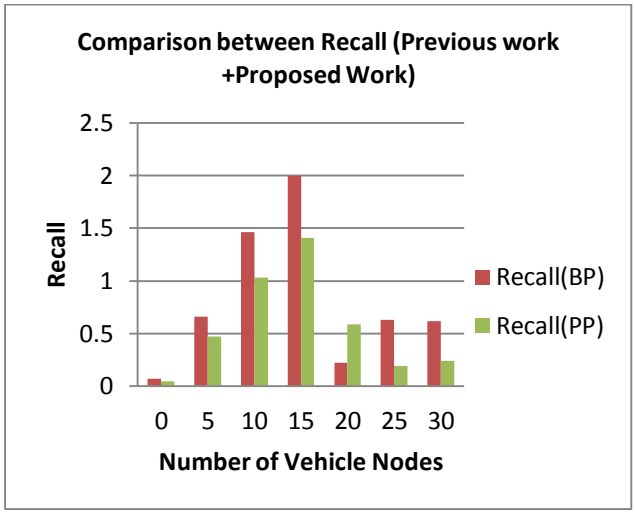

Fig.12: Comparison between Recall using Base work and proposed work

The above figure shows that the comparison between recall using base work and proposed work. We improve the performance with the true negative value in the proposed work.

VI. CONCLUSION

In this section defines, plainly identify trials in this environment, review current trust replicas planned for different conditions, and opinion out their problems when

existence taken to the VANET area. Then we suggest a list of significant belongings that should be archived by trust organisation for VANET, situation an exact area for investigators in this area. Our investigation thus attends as single phase faster near the project and expansion of actual trust organization for the positioning of security, life serious and road complaint associated systems by managements and commercial organizations to increase road protection and diminish the amount of car chances and traffic congestion. In this thesis, we have studied an attack on the VANET network known as clone Attack which makes false identities from a single entity. Multiple copies are generated through this attack. It causes traffic congestion, jamming etc. We have formulated our problem and have found a solution to resolve this attack . We implement the routing protocol is a reactive routing protocol which establish a route when a node requires sending data packets. It has the ability of unicast & multicast defeating. It uses a terminus sequence number which makes it dissimilar from other on demand routing protocols. We have generated an algorithm called Artificial Bee Colony Algorithm which has been applied. The minimal model of forage selection of actual honey bees, the colony of artificial bees in ABC contains three groups of bees: employed bees associated with specific food sources onlooker bees viewing the dance of employed bees within the hive to choose a food source, and scout bees searching for food sources randomly. Both onlookers & scouts are also known as unemployed bees. After that proposed technique which has been improved my results like throughput, packet delivery rate etc.

VII. REFERENCES

[1]. Jiang, Hao, Hao Guo, and Lijia Chen. "Reliable and efficient alarm message routing in VANET." *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008.

[2]. Panayappan, Ramu, et al. "VANET-based approach for parking space availability." *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*. ACM, 2007.

[3]. Knorr, Florian, et al. "Reducing traffic jams via VANETs." *Vehicular Technology, IEEE Transactions on* 61.8 (2012): 3490-3498.

[4]. Grover, Jyoti, Manoj Singh Gaur, and Vijay Laxmi. "A novel defense mechanism against sybil attacks in VANET." Proceedings of the 3rd international conference on Security of information and networks. ACM, 2010.

[5]. Golle, Philippe, Dan Greene, and Jessica Staddon. "Detecting and correcting malicious data in VANETs." *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004.

[6]. Balmahoon, R., and R. Peplow. "Vehicular Ad-Hoc Networks: An Introduction to Privacy." Southern African Telecommunication Networks and Applications Conference (SATNAC) will be held from. Vol. 2.

[7]. Taleb, Tarik, et al. "A stable routing protocol to support ITS services in VANET networks." Vehicular Technology, IEEE Transactions on 56.6 (2007): 3337-3347.

[8]. Martinez, Francisco J., et al. "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)." *Wireless Communications and Mobile Computing* 11.7 (2011): 813-828.

[9]. Merlin, Christophe J., and Wendi B. Heinzelman. "A study of safety applications in vehicular networks." Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on. IEEE, 2005.

[10]. Singh, Ajit, et al. "A relative study of MANET and VANET: its applications, broadcasting approaches and challenging issues." *Advances in Networks and Communications*. Springer Berlin Heidelberg, 2011. 627-632.

[11]. Merlin, Christophe J., and Wendi Beth Heinzelman. "A study of safety applications in vehicular networks." In IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005., pp. 8-pp. IEEE, 2005.

[12]. Kaur, Mandeep, and Manish Mahajan. "Protection Against DDOS Using Secure Code Propagation In The VANETs." (2016).

[13]. Verma, Karan, Halabi Hasbullah, and Ashok Kumar. "Prevention of DoS attacks in VANET." Wireless personal communications 73, no. 1 (2013): 95-126.

[14]. H. Füßler, M. Mauve, H. Hartenstein, and D. Vollmer, "A Comparison of Routing Strategies in Vehicular Ad-Hoc Networks", Reihe Informatik, March 2002.

[15]. Kaur, Mandeep, and Manish Mahajan. "Protection Against DDOS Using Secure Code Propagation In The VANETs." (2016).

[16]. Rawat, Ajay, Santosh Sharma, and Rama Sushil. "VANET: Security attacks and its possible solutions." Journal of Information and Operations Management 3, no. 1 (2012): 301.

[17]. Jadhao, A.P. and Chaudhari, D.N., "A Novel Approach For Security Aware Topological Based Routing Protocol In Vehicular Adhoc Network", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013.

[18]. Lyamin, Nikita, Alexey V. Vinel, Magnus Jonsson, and Jonathan Loo. "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11 p Vehicular Networks." IEEE Communications letters 18, no. 1 (2014): 110-113.