The Security Impact on Vehicular Ad-hoc Network

Jeyasuriya GanesanKanchana (40202287), Pranay Gulipilli (40185364), Vamsi Mohan Pavuluri (40165590), Ramya Gurumurthy (40218557), Sai Chandra Sekhar ReddyDwarampudi (40189233), Sudeep Kumar Chamarthi (40184676)

***Abstract* — Vehicular Ad-Hoc Networks (VANET) have acquired a ton of fascination and significance. It improves street security and offers many efficient administrations. VANET (Vehicular Ad-hoc Network) is one of the emerging technologies with a vast number of advantages. As an advanced technology with plays, a crucial role in autonomous driving cars the security of the technology is a very big concern. Several attacks can be performed on the VANET, which makes the system unreliable. A vehicular ad hoc network (VANET) allows vehicles to communicate with one another and with roadside equipment (RSUs). VANETs provide Road safety, traffic congestion, navigation, and other roadside services. VANETs are vulnerable to different types of attacks as the mode of communication between the V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) is wireless. Different approaches are being introduced to mitigate Bogus Attack, Sybil Attack, Timing Attack, Black Hole Attack, GPS Spoofing Attack, and Worm Hole Attack.**

***Index Terms*— Vehicular Ad-Hoc networks (VANET), Black Hole Attack, Route Request (RREQ), Route Reply (RREP), Software Defined Network (SDN), Roadside Unit (RSU).**

I. Introduction

A vehicular ad-hoc network is a type of network in which nodes (vehicles) can communicate with each other and with the infrastructure on the road. SDN (Software Defined Network) is a new growing topic in computer networks that aims to make it easier and more efficient to manage and operate network systems. The primary goal of SDN is to decouple network hardware (such as switches and routers) from control decisions. Its advantage is that it dramatically reduces the complexity of network management. The decoupling of the data and control planes in SDN allows for better network management and control. NDN (Named Data Networking) is a future Internet technology that aims to eliminate IPv4 addressing issues. Communication between nodes in the NDN is based on content names instead of IP addresses Due to various circumstances such as speed and traffic congestion, the process of exchanging wireless messages between vehicles and Roadside Unit (RSU) for security applications experiences fluctuation in processing latency. As wireless network resources undergo fluctuation in processing delay due to RSU, this results in a serious side-channel assault in VANETs [2].

VANET is a self-sorting out network that permits vehicles to speak with one another. Each taking the part vehicle in the organization goes about as a remote switch or hub, permitting vehicles to associate and convey. AODV is significantly utilized in directing conventions for VANET. VANET correspondence has been classified into two kinds.

Vehicle to Vehicle (V2V) Communication - This type of communication occurs from vehicle to vehicle without the sponsorship of any networked framework. This kind of communication is apt for short-distance communication. It is dependable and extremely speedy. Vehicles comprise OBU (On-Board Unit), which process information gathered from different sensors and is liable for speaking with different vehicles and foundation [3].

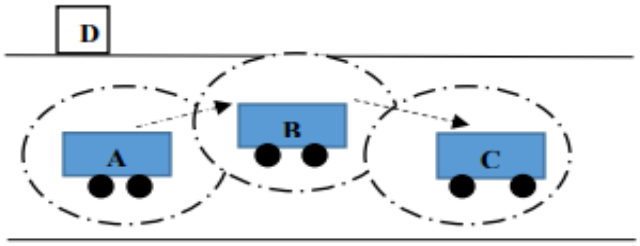

Fig1. Vehicle to Vehicle (V2V) Communication [3].

Figure 1 represents the communication between vehicles A, B, C, and the network infrastructure D. Vehicles A, B, and C are in short distance communication range where multi-hopping is used to make Vehicle A communicate with Vehicle C.

Vehicle to network framework Communication - Infrastructure goes about as a static hub. They are additionally named Roadside Units. Correspondence happens among vehicle and street-side units, it is proper for long-reach interchanges [3].

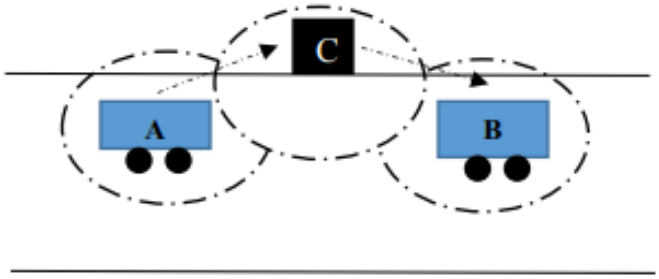

Fig2. Vehicle to network framework Communication [3].

Figure 2 represents the communication between vehicles A and B and the network infrastructure C. As observed vehicles A and B are not in the range for short-distance communication so they make the communication feasible through the Roadside Unit (RSU).

In Section II we discussed different attacks on VANET security and the prevention mechanisms for dealing with such attacks. We discussed different techniques involved with different attacks in

Section III and we concluded by analyzing the best approaches for mitigating the mentioned attacks in Section II.

II. ATTACKS ON VANET SECURITY

Vehicular Ad-Hoc Networks (VANET) are vulnerable to Black Hole attacks considering the transmission idea of the remote medium and an absence of security standards. Following are the possible attacks on the VANET.

A. Black Hole Attack

There are several attacks associated with malicious nodes one of the serious threats associated with the malicious nodes is a black hole attack. The attack is performed in such a way that the malicious node rapidly answers with RREP (Route Reply) when it gets RREQ (Route Request) data packet the from source node or its adjoining nodes even though it doesn't have a course to the objective. Prior to sending RREP (Route Response) data packet, it doesn't check its routing table, and by and large, it is the first node to answer the RREQ. On getting RREP source hub sends an information data packet to the malicious hub, it drops all the parcels got. In this way, black hole impacts organizational correspondence by dropping every one of the data packets [3].

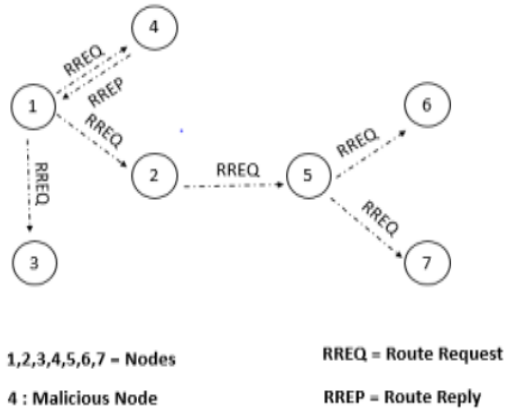

Fig3. Black Hole Attack [3]

Figure 3 represents a scenario where Node 1 is the source node and node 6 is the destination node and Node 1 must communicate with Node 6. The source node checks its own routing table for an immediate way to the destination node. There is no immediate way accessible subsequently RREQ data packets are communicated by Node-1 to its adjoining hubs 2, 3, and 4 for course revelation. Upon receiving the RREQ from Node-1, Nodes 2 and 3 check their steering table to track down the course to the objective. Meanwhile, Node-4 sends RREP to the source expressing that it is the closest neighbor hub to the Destination. Hub 1 advances the information parcel to Node-4 in the wake of getting RREP yet Node - 4 drops every one of the data packets got by it [3].

Related Work: -

One of the recommended a strategy by Sun B is to detach the black hole in view of the neighborhood approach. At the point when the source node finishes the course disclosure, it needs to know the neighbor node set of its objective node. Consequently, it sends an extraordinary information packet to the objective node in the way that it got RREP and it sends that control parcel in a substitute way. Assume if there should arise an occurrence of black hole presence, the Source node gets two different neighbor node sets. By this, we can close there exist a malicious node that is performing black hole assault. The node that answered with RREP will be disposed of. Another technique was proposed by Ashok to recognize malicious nodes with the assistance of versatile specialists. Source node creates a portable specialist in the organization. The versatile specialist will visit the adjoining node in the ongoing course and ought to assess the hear rate. Creators approximated edge esteem. If the hear rate is bigger than the limit esteem, the node could be disposed of which created an RREP data packet [3].

Proposed Work: -

In this approach, street-side units assume a significant part. RSU's in VANET is competent to speak with one another. Street side unit dispenses IP address for every portable hub that enters the organization, and it refreshes the apportioned IP address in its lord directing table and offers subtleties to other street-side units. Each hub in the organization shares its routing table with the closest street side unit.

It consists of two stages to detect the black hole attack they are: -

1. Stage 1: - Prelim Stage
2. Stage 2: - Secure Stage

Stage 1 - Prelim Stage

Source hub communicates RREQ data packets in the network and illuminates the closest street side that it started course disclosure and starts a clock. The source node hangs tight for a specific time span to get all conceivable RREP course reactions from the hubs in the organization. For the most part, the malignant hub would be the first hub to answer with the RREP bundle. In that specific time stretch, all the RREP way reactions are put away in a way reaction table by source hub in climbing request with deference to jump included in that specific course. source hub shares a way reaction table to the side of the road unit. Street side unit checks whether there is a legitimate course between the node that sent RREP and the objective node from the ace steering table. If an immediate way is accessible street side unit illuminate's source node to start correspondence. Assuming no legitimate course is found, the Roadside unit marks it as pernicious with a 70% likelihood [3].

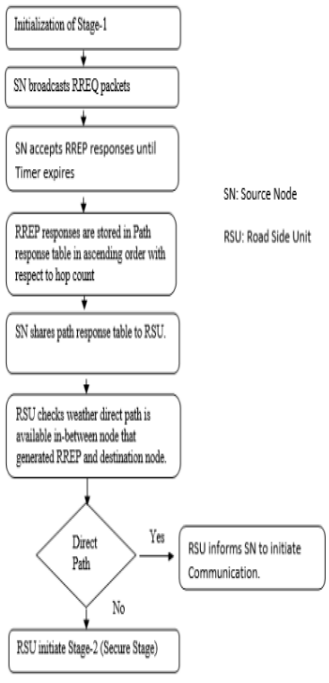

Fig4. Flowchart for Stage 1 [3].

Stage 2- Secure Stage

In this stage Roadside Units chooses an unused IP address, it eliminates. The objective node IP Address from the RREQ packet and replaces with an unused IP address. RSU communicates RREQ bundle in the network for course revelation. Assuming the very hub that was recognized in the prelim stage answers to the RSU expressing that it has a substantial course to the objective, that specific hub could be disposed of. Street side unit quickly answers to source hub also, broadcasts to the whole organization about its presence and separates it [3].

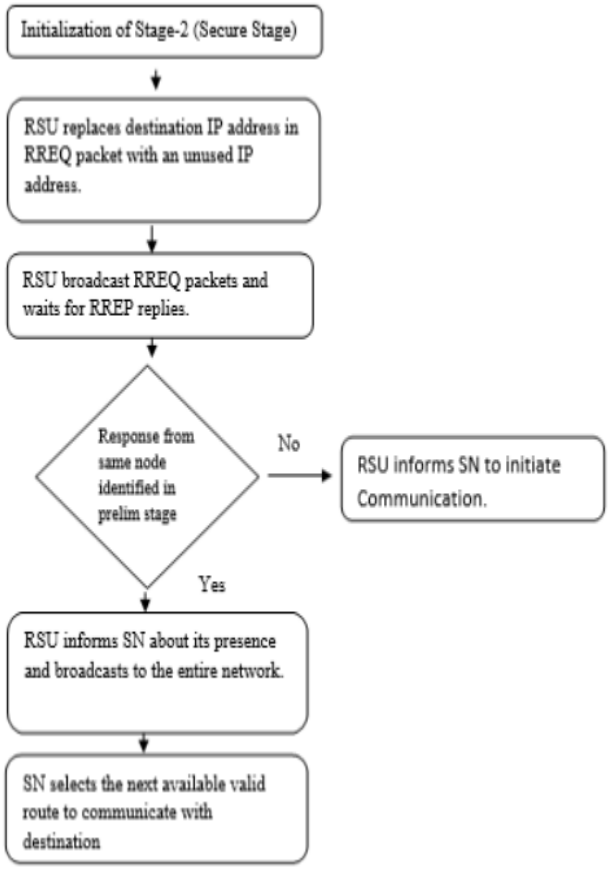

Fig5. Flowchart for Stage 2 [3].

Black Hole Attack:

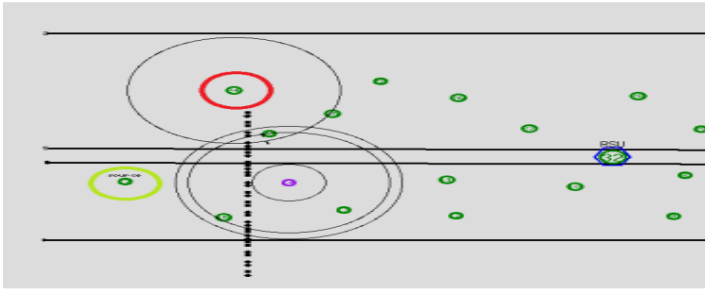

Fig 6. Black Hole Attack [3].

Figure 6 represents the occurrence of a black hole in the organization. The source node is set apart in the green circle, it communicates RREQ data packets for course revelation. Malicious node unicasts RREP answer to the source node. Source node after getting RREP advances the information bundle to the malicious node. It drops every one of the bundles without sending them to the objective hub. The malicious hub is set apart with a red circle. AODV convention couldn't identify the presence of a black hole [3].

Disposal of Black Hole by the suggested approach

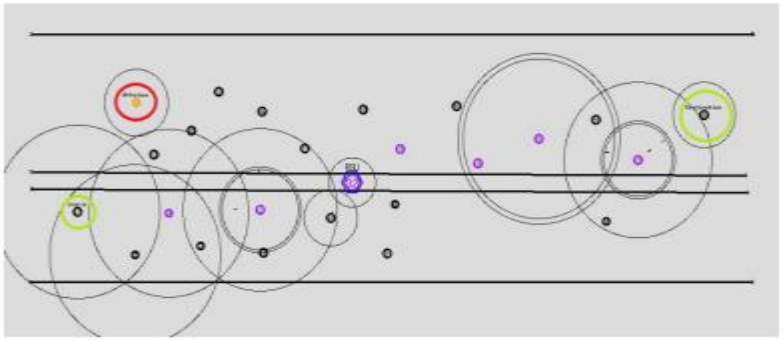

Fig7. Disposal of black Hole [3].

Figure 7 represents the malicious node is being segregated by the suggested approach. The source node chooses the next accessible way to speak with the objective. Source and Destination nodes are set apart with a green circle, and the malicious node is checked with a red circle. Nodes that have a substantial way are set apart in the violet variety.

Results

Packet Delivery Ratio is characterized as a proportion of parcels obtained by the sink hub to the information parcels started by the source hub.

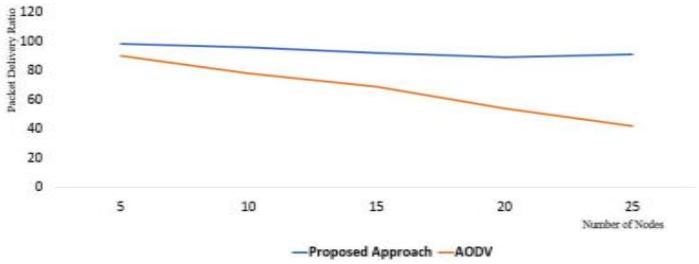

Fig8. Packet Delivery Ratio [3].

In Figure 8 PDR is plotted for the AODV convention and suggested technique by considering 25 hubs. It very well may be seen in the suggested strategy that PDR is fair when contrasted with the AODV convention since black holes could be distinguished and confined right away [3].

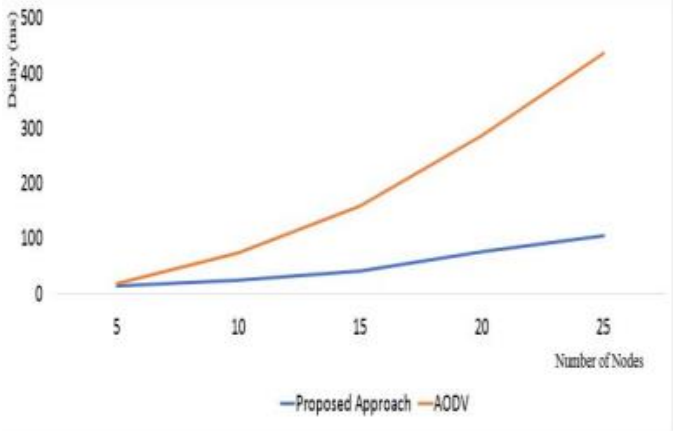

Fig9.End-to-End Delay [3].

Figure 9 represents the observed end-to-end delay associated with the data packets to reach the objective from the source node by using the proposed approach defer time is negligible when contrasted with the AODV convention.

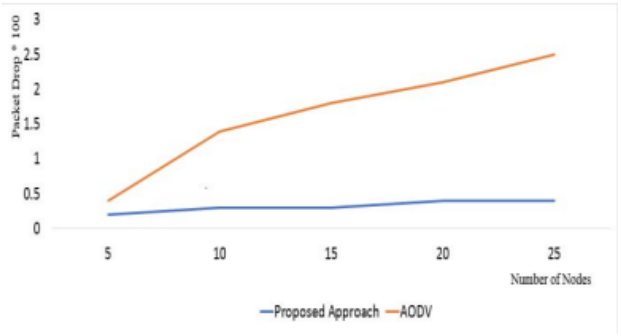

Fig10. Packet Drop [3].

Figure 10 represents the packet drop plotting for the AODV convention and suggested approach by considering 45 nodes. It very well may be seen in the suggested strategy that data packet drop is less when contrasted with AODV convention due to disposal black hole.

B. *Sybil Attack*

Sybil attack is performed on the authentication of the VANET and should be performed by an active attacker. It has medium impact on the network [4]. In this attack, the attacker creates multiple identities of the node which can send false data to the other nodes in the network. The data in this attack is sent with prefabricated identity. This attack is primarily performed by the attacker OBU on the genuine OBU for getting different benefits. This attack is mostly implemented by the attacker to have clear roads in which he will travel. The attacker will create numerous instances of him and send them to the legitimate user, creating an illusion that there is high amount of the traffic in a certain path in which he wants to travel. This will make the legitimate users to choose a different path and the path which in illusion of instances is created will be empty and the attacker can travel freely [4]. This attack can also be used thief's to create illusion to the police by creating multiple instances of the car and deviating the police in a wrong direction chasing a wrong car [4]. The following figure demonstrates the Sybil attack in which the attacker car C will create numerous identities of the car C in the route he/she wants to travel. This message of fake high traffic density is sent to the other legitimate car user like car B and car D. On getting this message car B and D choose a different path making the fake high density traffic path clear for the car C.

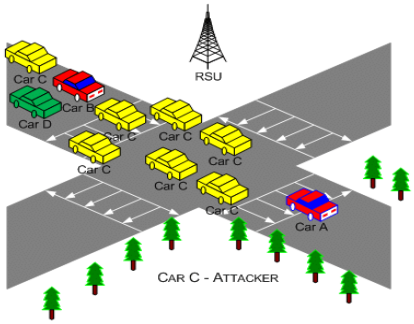

Fig11. Sybil attack on VANET [4]

Attack process Mechanism

There are various communication steps between the authentic VANET user and the attacker. For most of the attacks performed on the VANET the following steps are common [5]. The detailed steps are as follows.

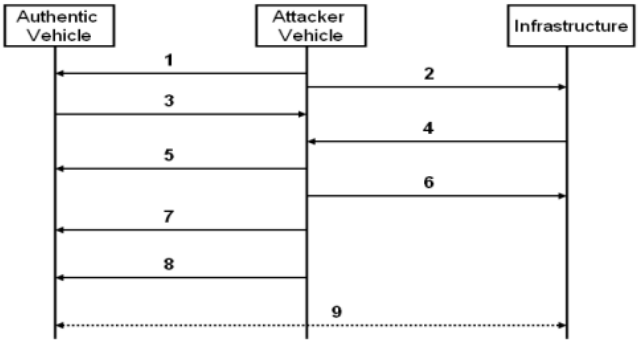

Fig12. Attacks process mechanism [4]

Steps performed by the attacker:

1. The attacker launches the first-class attack (Sybil attack) [5] to other genuine vehicle in the VANET network.
2. The same attack is sent to the main infrastructure of the VANET.
3. The attacker vehicle receives the Safety messages from the other vehicles.
4. Infrastructure sends safety message to the attacker.
5. The attacker changes the content of the message and send it to the other vehicles.
6. Attacker vehicle sends wrong message to the infrastructure.
7. Attacker sends timing attacks to other vehicles.
8. Attacker vehicle launches social attack to the nearby vehicles.
9. The communication between the vehicles and the infrastructure is continuously monitored by the attacker vehicle.

Defense against Sybil attack:

There are various methods which can provide defense against the Sybil attack. The following are some of them

1. Recourse Testing: Recourse testing can act as a defense mechanism against Sybil attack. This defense mechanism assumes that some resource will be in limited proportion to an entity. In this computational puzzle are used to test the computational resources of the node [6]. Sometimes the attacker might have high resources for computation than honest mode in such cases radio resource testing is used.
2. Usage of Public Key Cryptography: In this a PKI is used for VANET called CPKI. The authors described a complete defense solution for the secure communications and solved the problem of key distribution and a mechanism for key cancellation when misused. Each vehicle is provided with a public key to get authenticated. The toughest part in this defense methodology is the integration between VANET and PKI. This solution must undergo vigorous testing in the real world.
3. A pre-defined propagation model: In some cases, the VANET model is confined to a pre-programmed and defined propagation model. In this the strength of the

signal power with respect to the position is used to detect any form of inconsistencies. Here node itself act as a crucial point in collection the data from the other nodes [6]. It analyses the strength of the signal received from the node with respect to the new position. A node is identified as an attacker if there is deviation in the value from the expected one.

4. Secure Positioning: It is another defense mechanism to prevent Sybil attack. It is based on the reliability of the locations claimed by the vehicles [6]. Here the signal and location of the transmitting peer node are verified by collaborating the trusted peers to identify and authenticate. Direction and signal strength are mainly used as parameter for this method. Verifiable multiliterate approach along with distance bounding protocol and base stations is used to send the accurate position. All the pairwise secret keys can be established by the nodes directly.
5. Distinguishability: In this the VANET data is evaluated. Multiple data are correlated and given a score, based on the score the higher score entities are accepted. This is approach assumes that all the entities are equipped with special devices through which they can communicate with the main physical source.

C. *Timing Attack*

There are two types of applications in VANETs: (i) safety critical applications and (ii) informational applications. Applications that require data in real-time are known as safety-critical applications. They carry important information that must be delivered to cars as soon as possible. These programs offer information regarding the current state of the highway, such as accident reports, VIP protocol movement, and traffic congestion. To achieve data integrity and security, it is critical to send and receive data in the VANET. One or more attacker vehicles are used in a timing attack, which is a relatively novel attack in VANETs. These attacker vehicles do not send safety-critical data to other vehicles promptly, but they do impose some extra packet delays in terms of timeslots.

Other vehicles close to the attacker vehicle, on the other hand, received these data packets after they were required. The timing attack scenario is visually depicted in Figure 13. TAP [2] technique is responsible for detecting attacker vehicles and then mitigating them by utilizing controller functions in a network.

Timing attack prevention Scheme

In TAP, we first detect a vehicle and then determine whether the vehicle in question is an attacker or not.

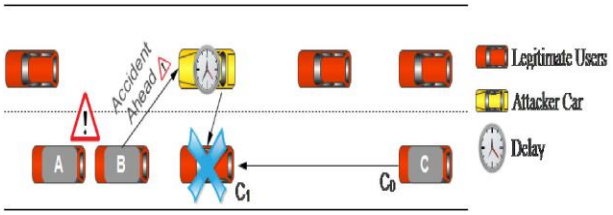

Fig13. Timing Attack Scenario [2]

When an attacker vehicle is discovered, the SDN [7] controller uses the controller defaulter list to ameliorate the situation. This method prevented the network from forwarding any delayed emergency packets. This operation is always carried out on the next hop node from the attacker's vehicle.

Algorithm 1: Send/Receive Emergency Packet

```
1:  OnSendEmergencyPacket[vID, getCoor, PAT, PPAT, PGT]
2:  vID ←getNodeID()
3:  xCoordinates ←getX()
4:  yCoordinates ←getY()
5:  setCoor(xCoordinates, yCoordinates)
6:  PAT ← getPacketArrivalTime()
7:  PPAT ← getPerviousPacketArrivalTime()
8:  PGT ← getPacketGenerationTime()

9:  OnReceivedEmergencyPacket [vID, getCoor, PAT, PPAT, PGT]
10: If (vID != Controller_Defaulter_List) then
11:     D ←calculateDistance(receiver(getCoor), sender(getCoor))
12:     ∂ ← D/S
13:     v ←PAT-∂
14:     if (v != PPAT) then
15:         Forward vID to Controller
16:     else
17:         Forward Emgergency Packet to Face
18:     end if
```

TAP [2] technique is responsible for detecting attacker vehicles and then mitigating them by utilizing controller functions in a network. For safety-critical applications, Algorithm 1 shows how to transmit and receive emergency packets. The first coordinates and vehicle ID of the relevant vehicle are placed in the packet fields, i.e., x coordinates, y coordinates, and vID fields, respectively, to transmit emergency packets to other vehicles (Lines 1-5). Following that, the vehicle receives the packet arrival time (PAT) as well as the preceding packet arrival time (PPAT). PPAT values will be 0 if the relevant vehicle is a consumer and is sending the packet for the first time in the network (Lines 6-7). The latest packet generation time (PGT) is now calculated using the vehicle's clock. The suggested scheme's main contribution (TAP) is to keep the attacker out of the network. A new vehicle, on the other hand, checks the Controller-Defaulter-List first when it receives an emergency packet. Control messages will be used to populate this list. The previous sender's vehicle id is included in the packet received by a vehicle.

This vehicle id is now compared to the Controller- Defaulter-List, which was previously cached (Line 10). If the results were the same, the vehicle would immediately drop the most recent packet and take no further action (Lines 19-20). It reveals that this previously received packet came from a vehicle that the controller had already identified as an attacker. If no matches are found, it signifies that the previously received packet came from a vehicle that isn't an attacker or hasn't been detected as one. In this example, the detection process begins after the attacker list is matched. A vehicle's x, y, and sender's x, y coordinates are used to compute distance throughout the detecting procedure (Line 11). Following the distance calculation, the vehicle determines the time it takes for a packet to arrive from a source to a destination using a signal propagation speed of 3.0*108 m/s. is a time period obtained by dividing distance (D) by signal speed (S) (Line 12). After that, this time period value is subtracted from the packet arrival time (PAT) to obtain the prior vehicle arrival time, which is used to determine

whether the previous car caused any packet delays (Line 13-14). If the value of the prior vehicle's arrival time does not match the value of (PPAT) in the packet, the previous vehicle is an attacker who has introduced a delay to the packet. When it gets to automobiles after they require it, this package is now useless. As a result, the previous vehicle's id is forwarded to the controller, who saves the attacker's id in its defaulter list (Line 15), and if no delay is applied, the vehicle simply forwards the emergency packet to other vehicles, indicating that the previous car isn't an attacker.

D. Wormhole Attack

Wormhole attack is a destructive and popular attack in VANET as well as in further ad-hoc networks and it is a kind of network layer attack. Wormhole attack involves two or more malicious nodes, and data packets from one end of the malicious node are tunneled to the other malicious node at the other point, and these data packets are broadcasted. The tunnel which is formed between two tricky attackers is considered a wormhole. The malicious nodes in the wireless network listen to the packet which are not intended for them and make them pass through the tunnel to another end. Wormhole attack is a type of Denial-of-service attack (DOS), and it disrupts the network routing. Wormhole attack can simply obstruct the path of multicast and broadcast routing. [8]

Models in Wormhole Attack

This type of attack is classified into three models.

1. *Open Wormhole:*

In this type of attack, the source sends the data packets to wormhole which tunnels them to other wormhole and then pass on to the destination. The remaining nodes in network cannot be used for data transfer and can be ignored.

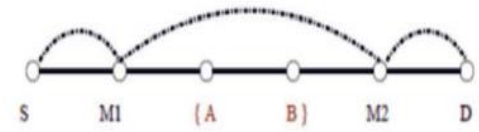

Fig 14. Wormhole for packet encapsulation *[9]*

2. *Half-open Wormhole*

In this type of attack the data packets are sent to a wormhole from the source and it will directly transfer them to destination. [9]

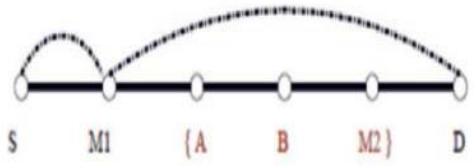

Fig 15. Half-open wormhole attack *[10]*

3. *Close Wormhole*

In this type of attack the data packets will transfer directly from source to destination in a single hop. [10]

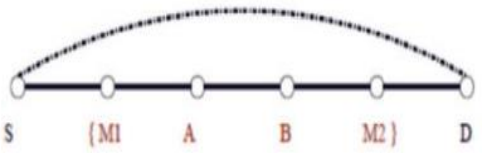

Fig 16. Closed wormhole attack *[10]*

Wormhole Attacking Modes

1. Wormhole using packet encapsulation
2. Wormhole using out-of-band Channel

Wormhole using packet encapsulation

Wormhole attacks are particularly damaging to many ad-hoc and sensor network protocols, such as the DSR and AODV protocols. First, we show how to launch a generic wormhole attack against such routing protocols, using DSR as an instance. If a node, say S, needs to find a route to a destination, say D, S floods the network with route request packets. Any node that receives the request packet processing it, adding its identity to the source route, and rebroadcasting it. To reduce network flooding, each node broadcasts just the first route request it gets and declines any subsequent copies of the same request. D generates a route reply for each route request it receives and sends it back to S. The source S then chooses the best path from the route replies, which could be the path with the fewest hops, or the path associated with the first arrived reply. This protocol, however, will fail in a malicious environment. When a malicious node in one part of the network receives a route request packet, it tunnels it to a second conspiring party in a remote location near the destination. The route request is then rebroadcast by the second party. The neighbors of the second colluding party receive the route request and drop any subsequent legitimate requests arriving on legitimate multi-hop paths. As a result, the routes between the sender and recipient pass through the two colluding nodes, which are said to have formed a wormhole between them. This prevents nodes from discovering valid pathways that are more than two hops away. One manner for two colluding malicious nodes to get involved in a route is to simply give the false impression that the route through them is the shortest, even if they are many hops away.

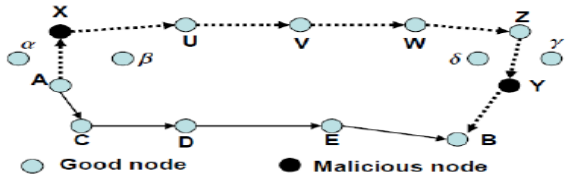

Fig 17. Wormhole for Packet Encapsulation [10]

Consider Figure 17 in which hubs A and B attempt to find the shortest way between them, in the presence of the two malicious hubs X and Y. Hub A transmissions a route request (REQ), X gets the REQ and epitomizes it in a parcel bound to Y through the way that exists among X and Y (U-V-W-Z). node Y demarshalls the packet, and rebroadcasts it once more, which arrives at B. Note that because of the packet encapsulation, the hop count does An Approach To Detect The Wormhole Attack In Vehicular Ad hoc Networks n Worldwide Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) not increment during the crossing through U-V-W-Z. Simultaneously, the REQ goes from A to B through CD- E. Hub B currently has two routes, the first is four hops long (A-C-D-E-B), and the second is obviously three jumps long (A-X-Y-B). Hub

B will pick the second route since it has all the earmarks of being the briefest while in all actuality it is seven jumps in length. So, X and Y prevail with regards to including themselves in the course among A and B. Any steering convention that utilizes the measurement of most brief way to pick the best course is helpless against this method of wormhole attack. This method of the wormhole attack is not difficult to send off since the two finishes of the wormhole needn't bother with to have any cryptographic data. [10]

Wormhole using out-of-band Channel

This method of the wormhole attack is sent off by having an out-of-band high-transfer speed channel between the malicious nodes. This channel can be accomplished, for instance, by utilizing a long-range directional remote interface or a direct wired connect. This method of assault is harder to send off than the past one since it needs specific equipment capacity. Think about the situation portrayed in Figure 18. Node A is sending a route request to hub B, hubs X and Y are vindictive having an out of- band channel between them. Node X tunnels the course solicitation or route request to Y, which is a genuine neighbor of B. Hub Y communicates the packet to its neighbors, including B. Hub B gets two course demands — A-X-Y-B and AC- D-E-F-B. [10]

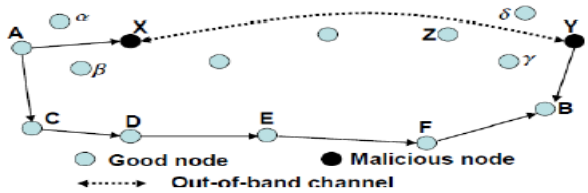

Fig 18. Wormhole using out of band channel [10]

Solution to Wormhole Attack

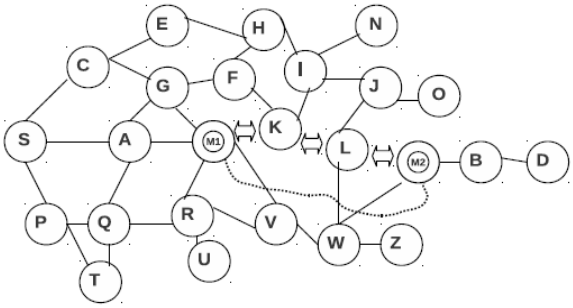

Fig 19. Wormhole Attack [10]

To avoid wormhole attack, the hubs taking part in the VANET correspondence must be enlisted in the organization. Every hub or node is furnished with the exceptional id which would help in keeping up with the record of every single hub or node involved in the network. The confirmed users or nodes decline the probability of the out-of-band channel wormhole attack as attackers wouldn't have the option to upset the course.

Each packet or message sent between two hubs ought to be safeguarded utilizing hashing calculations which would keep up with the integrity of the packet at each hub. If the attacker changes the contents of the message and attempts to disturb the correspondence, then that change results in a difference in hash esteem which would alert the organization against the attacker. The attacker frames the wormhole during the course revelation stage. To keep away from the development of wormhole Harbir et al., [10] proposes a strategy where after the reply from the objective the source has a total rundown of the moderate hubs shaping the route. As we probably are aware the total organization comprises of just validated clients, so it is challenging for the external attacker to disturb the course however there is plausible that the attacker compromises the genuine clients and afterward structure their own in the middle of between two authentic nodes stowing away their organization from the other hubs. [10]

E. Bogus Attack

Bogus information attack is one of the most dangerous attacks that involves transmitting false information to nodes for personal gain. The attacker can be an outsider or an insider in this attack. The attacker broadcasts misleading information in the vehicular network in order to influence the decisions of other vehicles in the network. The attacker node simply creates a false node in its immediate vicinity and informs the network that there is traffic in that area. As a result, other vehicles will take a detour rather than the quickest route.

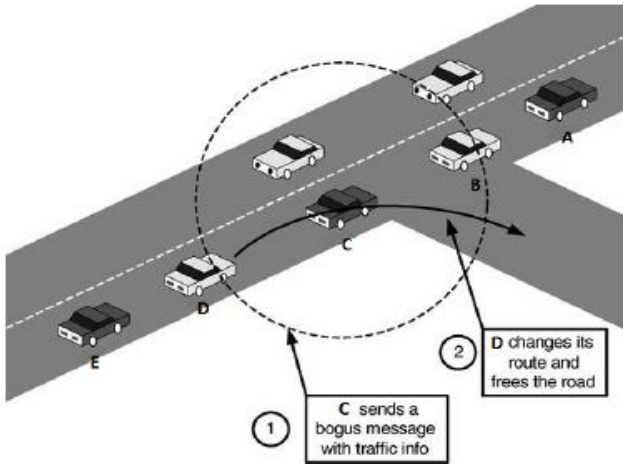

Fig 20. Bogus Attack [11]

As you can see in the Fig20., node C transmits a fake information about the traffic and as a result, node D changes its path. This attack can be used by an individual for his personal gain or an intruder can pass the false information to other nodes in the network causing accidents.

It is important to detect the attack and counteract. Authentication is a basic requirement and crucial step in ensuring security in VANET. To counteract the fraudulent attack, an authentication system is used. When compared to the Message verification methodology, traditional methods such as Cryptographic techniques and Digital Signature (DS) techniques have a large computing overhead. As the vehicles do not cooperate for the authentication of multiple messages in the typical way, each vehicle authenticates multiple safety messages independently. It authenticates several safety messages at the same time using a verification technique that is independent of the number of signatures to be validated. Here, the cars and RSUs work together to validate a number of different signatures of safety messages at the same time. As a result, the time required for message verification is reduced, and authentication speed is increased.

Methodology:

Out of the various attacks that can be performed in the network, Bogus Information attack [1] is one of the most dangerous attacks that sends false information to other vehicles in the network causing traffic and accidents. Below are the various ways to detect the attack.

1. *Sender's Behavior:*

Analyze the senders' behavior, such as the packet and message pattern, and compare them with the normal nodes to identify the attackers [12]. Deviated nodes are deemed as malicious. A reputation-based announcement scheme is used to analyze the node behavior. The receiver decides whether to

accept or reject the packet based on the number score assigned by the scheme. Feedback is given to the node based on the transmission and the server updates the numeric score of the node based on the feedback received. This method requires multi-level communication, hence delay in the detection leads to life-endangering situations.

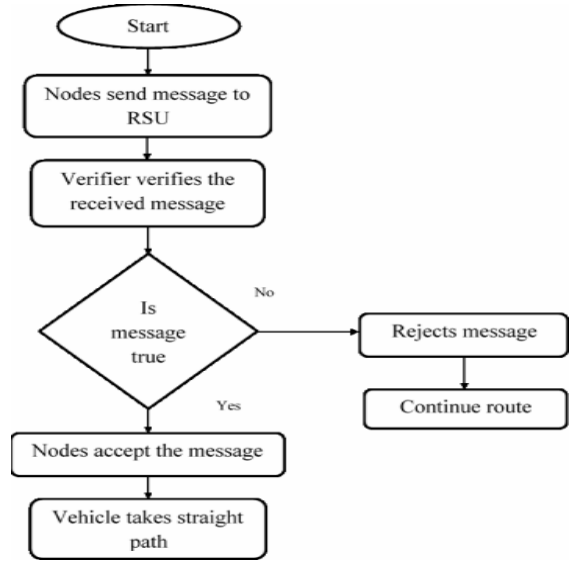

Fig 21. Flowchart of Position Verification Technique [1]

2. *Verification of the Position:*

Greedy routing approaches and geographic routing approaches are the most common types of position-based routing for VANETs. In Greedy routing, nodes transmit the data to the nearest node to the destination as the nodes are aware of their positions and their neighbors' position. All nodes use beacon signals to broadcast their own positions on a regular basis. Every node can then create a neighbor table and use it to make forwarding decisions. In Geographic position-based routing protocols, each mobile node in the topology is equipped with a Global Positioning System (GPS), allowing it to track its own location, as well as the locations of its neighbors. As a result, it makes it easier to find new routes fast. Because of their tolerance to frequent topology changes, routing protocols are more adaptable.

3. *Sensors:*

To identify the fraudulent attack, three types of sensor nodes are deployed [1]. First is the Acceptance Range Threshold (ART) sensor, a self-contained sensor that bases its observations on the node's maximum communication range. Second, Proactive Exchange of Neighbor Tables is a cooperative sensor in which nodes exchange their own tables as well as those of their neighbors and verify that the information received is correct. If the information collected from two neighbor nodes differs, it consults with other neighbors and makes a judgement based on the majority. Last one is the Reactive Position Requests sensor is a cooperative sensor in which the nodes only participate when there is a demand to check the position, such as when a node begins to cheat on the positions. Because all nodes are aware of their own and their neighbors' positions, they begin by selecting some neighbor nodes as acceptors or rejectors. The beacon signals are used to discriminate between close neighbors and distant neighbors. This aids in locating the node that deviates from the place.

The flowchart illustrates the steps involved in detecting the bogus node and how the attack is handled by the neighboring nodes. A car transmits a message to a nearby RSU (Roadside Units), which then relays the message to other vehicles or nodes in the network. By exchanging neighbor node information, the sensors on the OBU verify whether the information acquired is correct. If the information of two nodes differs, it compares it to that of other neighbors in the network and decides based on the majority, indicating the presence of an attacker. When an attacker is detected, RSU distributes information about the attacker across the network. As a result, the attacker's packets are dropped by the other nodes in the network. Now that the nodes in the network have received the right information from their neighbors, the nodes can take action.

F. GPS Spoofing Attack

The Global Positioning Systems (GPS) have become omnipotent in our everyday lives, which is a location of an individual provided by the Global Navigation Satellite Systems (GNSS). The applications range from food delivery applications to Unmanned Aerial Vehicles which makes the GPS prominent aspect with the industries. The spoofing attacks on the GPS signals could lead the vehicle to reach unintended locations as the individual who operates the vehicle may not be aware that the GPS signal has been spoofed. One such GPS spoofing incident occurred in Black Sea for over 20 vessels which caused by the external interference, where the ships receivers were tricked into assuming that their current locations are at the airports and resulted in moving towards wrong directions. But one ship has identified the fault and prompted a message to U.S. Coast Guard Navigation Centre [13].

Shing Ki Wong and Siu Ming Yiu [14] proposed a behavioral detection for the spoofing of the location with the help of gyroscope and accelerometer. The Location Spoofing Attack (LSA) can be classified into two categories namely, Signal Interference and Fake Location Reporting as shown in fig 21. Signal Interference can be considered as the interference of signals occurred between the source and receivers with external entities such as other radio frequency bands. In signal interference, the attacker sends the spoofed signals from the radio transmitter near to the target receiver which clouds the original signals. Fake Location

Reporting is a modification of actual location and reporting wrong location to the desired applications. The proposed detection mechanism is for the latter attack or interface attack which involves Pokémon GO, an application which requires individuals to walk to certain place in order to complete tasks. This application uses mobile GPS to track the user movements. The users modify their current location and falsify the movements, even though they are steady, to the application which results in the completion of tasks, without any physical activity. Usual prevention measures would be disabling allow_mock_location in developer options, checking for any malicious applications during runtime and prohibiting any root privileged devices from playing, etc., But these preventions can be downplayed resulting in the fake location to be notified to the application. The proposed detection mechanism uses gyroscope and accelerometer which records the travelling direction of the user and direction faced by the user's device. If the user is walking and already took two different turns then the angle through which the direction in the device is facing will be different, whereas the angle would be same in case the user is steady. This results in the detection of the location spoofing

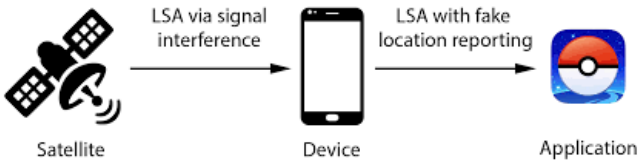

Fig 22. Location Spoofing Attack types [14]

Sagar Dasgupta et al. [15] implemented prediction-based spoofing attack detection mechanism using Long Short-Term Memory (LSTM), a Recurrent Neural Network (RNN) model. Theses GPS signal spoofing attacks can be divided into three types; namely simplistic, intermediate and sophisticated attacks. The simplistic attack lacks synchronization between the spoofed signal and original signal, therefore, easier to detect. The intermediate attack involves both the source signal and spoofed signal in synchronization with the portable-receiver spoofer. Sophisticated attack is hard to detect as the attacker uses multiple phase-locked spoofers to spoof all the transceivers. The detection strategy involves the use of training dataset Comma2k19 which consists of latitude, longitude and speed as GNSS data; speed and steering angle as Control Area Network (CAN) data; accelerations in different directions as Inertia Measurement Unit (IMU) data. The GNSS, CAN and IMU has their respective time, but GNSS time is considered as reference. The prediction-based strategy works in following way; An error threshold is calculated based on the predicted distance travelled between the current location(t) and the immediate future location(t+1) with the GNSS positioning error and the LSTM error. If a vehicle has been deviated from the intended path because of a spoofed signal then according to the threshold calculated, the vehicle can be classified as either under the attack or not.

III. CONCLUSION

The security of vehicular ADHOC networks is discussed in this report. Information sent in the network framework is more urgent. While dealing with different attacks there are malicious nodes and the removal of malicious nodes by different mechanisms makes the network infrastructure reliable. Different real-world scenarios where the GPS of the user is spoofed which leads the user to reach some random location which he is unaware of and he has no clue that his GPS is spoofed where adversary uses fake location reporting to trick the user to go to the wrong destination this kind of attacks can be prevented from using gyroscope and accelerometer which records the directions and prevents the spoofing attacks. We dealt with different attack scenarios based on VANET eventually our readings helped us understand the fact that security is always challenging, and new mechanisms and new real-life scenarios help us better understand the need for security and updating our legacy systems.

Work Distribution among Team Members

Team Members	Work Distribution
Pranay Gulipilli	Analyze the latest research activities related to different attacks on VANET security and discuss the impact of the black hole attack on VANET and are involved in formatting the report based on different attacks.
Vamsi Mohan Pavuluri	Going Through different IEEE research papers based on the GPS spoofing attack and its impact on real-world scenarios.
Sudeep Kumar Chamarthi	Discussed different implementations based on wormhole attacks and their consequences on VANET security.
Sai Chandra Sekhar Reddy Dwarampudi	Review the false data transmission through malicious nodes in the form of the Sybil attack and discussed its mechanisms.
Ramya Gurumurthy	Collectively helped during the merging of different attacks and mainly focused on time delays and timing attacks in VANET.
Jeyasuriya Ganesan Kanchana	Dealt with bogus attack and the functionality of the attack which can lead to misleading nodes to take the wrong routes and its impact on VANET.

REFERENCES

[1] A. A. C. a. N. E. Elizabeth, "Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication," *2018 International Conference on Communication and Signal Processing (ICCSP),* pp. 0388-0392, 2018.

[2] R. A. R. A. Arsalan, "Prevention of Timing Attack in Software Defined Named Data Network with VANETs," *2018 International Conference on Frontiers of Information Technology (FIT),* pp. 247-252, 2018.

[3] P. S. G. a. R. Shanmughasundaram, "Detection and Isolation of Black Hole in VANET," *International Conference on Intelligent Computing,Instrumentation and Control Technologies* , pp. 1534-1539, 2017.

[4] P. A. N. U. a. D. J. Shah, " Attacks on Vanet Security," *International Journal of Computer Engineering & Technology (IJCET).,* vol. 9, no. 1, pp. 8-19, 2018.

[5] I. A. A. I. H. H. &. b. A. M. J.-l. Sumra, "Classes of attacks in VANET," *Saudi International Electronics, Communications and Photonics Conference (SIECPC),* pp. 1-5, 2011.

[6] G. G. a. B. Ducourthial, "On the Sybil attack detection in VANET," *IEEE International Conference on Mobile Adhoc and Sensor Systems,* pp. 1-6, 2007.

[7] F. M. V. R. P. E. V. C. E. R. S. A. a. S. U. D. Kreutz, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE,* vol. 103, pp. 14-76, 2015.

[8] O. A. A. Elahe Fazeldehkordi, "Wormhole Attack," *Wormhole Attack,* 2016.

[9] N. C. Priya Maidamwar, "A SURVEY ON SECURITY ISSUES TO DETECT," *International Journal on AdHoc Networking Systems,* vol. 2, no. ResearchGate, pp. 30-40, 2012.

[10] S. B. A. K. Harbir Kaur, "An Appr An Approach To Detect The W o Detect The Wormhole A ormhole Attack In V ttack In Vehicular Adhoc ehicular Adhoc," *International Journal of Smart Sensor and Adhoc Network,* vol. 2, no. 2, pp. 20-30, 2012.

[11] V. H. LA, "Security Attacks and Solutions in Vehicular Ad Hoc Networks," *International Journal on AdHoc Networking Systems,* vol. 4, pp. 1-20, 2014.

[12] J. Y. W. Z. J. &. Liu and C. Yang, "Detecting false messages in vehicular ad hoc networks based on a traffic flow model," *International Journal of Distributed Sensor Networks,* 2020.

[13] [Online]. Available: https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea .

[14] S. K. W. a. S. M. Yiu, "Location spoofing attack detection with pre-installed sensors in mobile devices," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA),* vol. 16, no. 4, pp. 16-30, December 2020.

[15] M. R. M. I. a. M. C. Sagar Dasgupta, "Prediction-based GNSS spoofing attack detection for autonomous vehicles," *Transportation Research Board 100th Annual Meeting,* 2021.

[16] S. T. Sunilkumar S. Manvi, "A survey on authentication schemes in VANETs for secured communication," vol. 9, pp. 19-30, 2017.

[17] K. S. a. A. Poniszewska-Marańda, "Security methods against Black Hole attacks in Vehicular Ad-Hoc Network," *IEEE 19th International Symposium on Network Computing and Applications (NCA),* pp. 1-4, 2020.

[18] A. A. Mane, "Sybil attack in VANET," *International Journal of Computational Engineering Research (IJCER),* vol. 06, no. 12, pp. 60-65, 2016.