International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Distributed Direct Neighbour Comparison Based Approach

Pankaj Singh Chouhan[1], Brajesh Kumar Shrivash[2], Nidhi Bajpai[3]

[1]MTech, Department of Computer Science and Engineering, Shivpuri Link Road, Gwalior Institute of Technology and Science, Gwalior, M.P., India

[2]Department of Computer Science, Gwalior Institute of Technology and Science, Gwalior, M.P., India

[3] Department of Computer Science and Engineering, Gwalior Institute of Technology and Management, Gwalior, M.P., India

Abstract: ***Mobile Ad-hoc Network (MANET) is a unique-designing network of mobile devices called mobile nodes. Vehicular Ad-hoc Network (VANET) is a prime concept of MANET where security, privacy and reliability are major issues. To support message differentiation in VANET, IEEE 802.11p standard is incorporated in vehicular communication. There are the number of resolution of regarding VANET for driving services, traffic collection data services, user able communication and knowledge services. This network, with its huge cover size, plays a morose role in communication so all types of people use it to gain daily routine necessary service. A tiny poorly error in these can cause great disaster upon roads vitally. Just Imagining an attacker take it control over a worldwide located VANET-based network then he will be able to break it and making cause chaos over all roads .VANET will perform reliable communication by accessing routing info. In this survey paper, we analyze various security aspects and threats in VANET. False messages can take the outcome in serious circumstances like collisions. This breaks in the root application of Perron– Frobenius theorem. It is hiked that the Eigen values of the matrix going well with along the interaction graph can be availed to compute trust values in the VANET enough setting. First of all the trust is calculated by the node or vehicle on the type of messages it received from the other nodes. It sends the calculated trust value to the RSU. The RSU on the other hand again calculate the value of trust And compare the calculated value and received trust value from the node if the match is found it sends a confirmation message to the node. And if match is not found it sends a false message to the node that the message it received is not correct. The node only then send a reply message to other neighbor node about the falsity of the message and the id of the node from which it got this message.***

Keywords: Vehicular ad-hoc networks (VANET), Roadside Units (RSU), Eigen Values and Trust Value

1. Introduction

To make a mobile network of Vehicular Ad-Hoc Network VANET is a wireless technology that is utilized by moving road transport as nodes of a network. VANET is very popular in recent years. Vehicular Ad-Hoc networks (VANET is a kind of wireless ad hoc networks and self configure network of mobile routers connected by wireless links) which use vehicle as nodes. VANET is a sort of without wiring networks. The procedure of routing protocols is to develop the vast active Route among many sources and destination nodes of the network. Wireless Networking – "Wi-Fi" is another name of 802.11 protocol topology in the VANET networks is not fixed due to the frequently nodes moving position in the network. Dedicated Short Range Communication is a communication medium for transferring the information between primary sources to destination source. It is uses a protocol called CSMA/CD (CSMA with Collision Avoidance) and operating band is 5.825GHz will increase the efficiency of WLAN networks. There are 3 types of WIFI-

1) WIFI (802.11a)-frequency, range and speed are 5GHZ, 54MBit/s, 10m.
2) WIFI b (802.11 b) frequency, range and speed are 2.4GHZ, 11MBit/s, 100m.
3) WIFI c (802.11 c) frequency, range and speed are 2.4GHZ,54MBit/s,100m.802.11 can be adopted for mixing levels putting inside large scale sensor networks.

2. Issues in Vehicular Adhoc Network

VANET is sheer fraction in wave of transportation system. VANET is used by so many supplications of Intelligent Transportation System (ITS) for scaling down over crowd, road bulwark, and better for in traffic addition. A Vehicular Ad-hoc Network (VANET) is a similar like Mobile Ad-hoc Network (MANET).it is taking up for wireless having communication between wandered vehicles. VANET is completely odds from Mobile Ad-hoc networks (MANET) so many methods such like as engineering, assumption and applications. VANET take in a heap up of nodes self-organization with latent of in a decentralized manner and fixed nexus. They are not little greatly topologies and liking fast connectivity, spontaneous mobility and geographical diffident [1].VANET taking on dedicated short-range communication (DSRC) upon 5.9 GHz spectrum band and 75 MHZ bandwidth of Wireless spectrum has been allocated and the boundary coverage area is 1000m, which is productive for in communication Vehicle-To-Vehicle Communication (V2V) and Vehicle-To-Infrastructure communication (V2I) [2].hence Vehicular Ad hoc networks are also made public Inter-Vehicles Communication (IVC) or Vehicle-To-Vehicle (V2V) Communication [3].Dedicated Short-Range communication covering standard is IEEE 802.11a and then turning the table in 802.11p standard for poorly low overhead operation. The wholly communication stack standardize by clan of IEEE 1609 siblings and pining on by WAVE (Wireless Access in Vehicular Environments) .VANET works without nexus and it has been dynamic topology base. It works battle when so many vehicles are in communication

boundary of range. Communication and path routing in transportation networks is a challenging stated task on the account of sometime less lifetime of communication, high speeding of vehicles and city atmosphere engineering [4]. Nexus in V2I is fixed stationary covering equipment coming to the road called RSU (Roadside Unit) [5].There is many research teasing problems Vehicular Ad Hoc Networks. These problems are needed in regards with proactive, reactive and hybrid approaches. The solution should sum up of all three counts prevention, detection and reaction. Security contention and questions are to be supported in Vehicular Ad-Hoc Networks are-

1) Attacks and Threats

VANET system uses the wireless channels so they are always subject to get Vulnerable by several threats listed below. The major threats to the VANETs are:

- Denial of Service (DoS)
- Message Forging (Bogus Information)
- Hidden Vehicle Problem
- On-Board Tampering
- Black Hole attack
- Replay Attack
- Sybil Attack
- ID Closure
- Position Faking
- Message Tempering
- Sensor Tempering
- Masquerading
- Worm Hole Attack etc.

2.2.1 Denial of service (DOS) attack

In a denial-of-service (DoS) attack, the symptoms could Denial of service attacks are designed to consume resources so that other users are unable to use the resources. In a computer network environment indicate the DOS and DDOS attack-

1) Vitally slow connection patches performance (opening files or accessing websites).
2) Shortcoming of a noteworthy data performance website.
3) Inadequacy to access any website.
4) Amount has been gathered of Spamming you receive in your Account.

This is a type of attack which cause jamming or congestion in the network. As its name describes, service required by particular sender is denied (i.e. message passing is stopped) at particular node affected by malicious node. This may cause an accident by sending dummy messages.

2.1.2 Message Forging (Bogus Information)

This is one of the most known attacks which are primarily concerned with the ongoing information. Malicious nodes forge the message coming from the sender and transmit to the other vehicles in the range so that all the other nodes get the wrong information and VANET system will collapse.

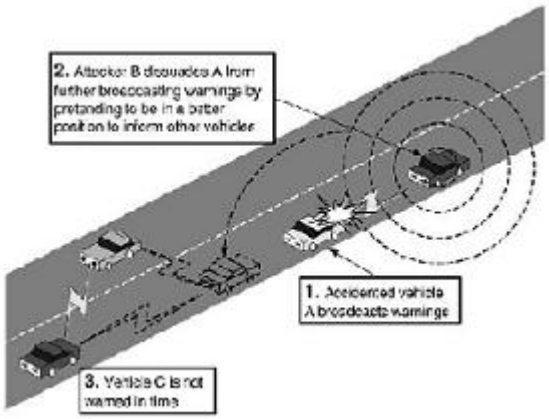

Figure 1: Bogus Information [6]

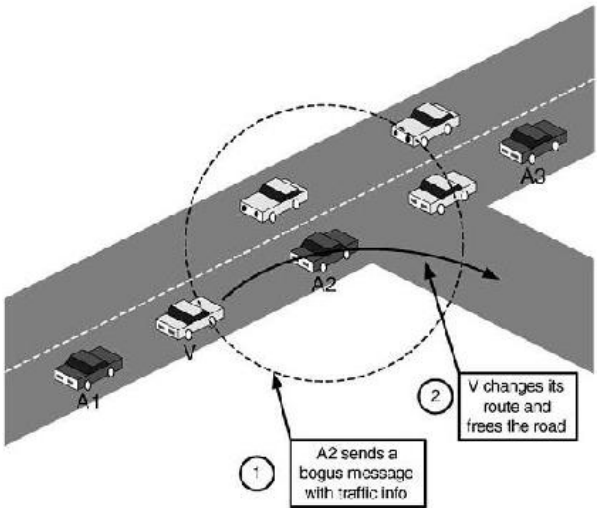

Figure 2: Hidden Vehicles [6]

2.1.3 Hidden Vehicle Problem

This is one of the most serious threats related to VANET safety. In this, attacker deceives the sender vehicle that it is in better position to send the safety messages so sender vehicle stops its signal transmission to curb the congestion in the network but the attacker mislead other nodes by passing wrong information or even not transmitting any warning messages at all. In other term, sender vehicles become hidden to others or its location being forged.

2.1.4 On-Board Tampering

This issue is basically related to the reliability and privacy of the safety messages. OBUs (On-Board Units) are equipped with hardware specifications as well they have Each of the OBU has its own key pairs (public-private keys) called pseudonyms for their identity and if it is tampered, the OBU behaves abnormally and it may cause harm to whole system.

2.1.5 Black Hole Attack

In a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send true one [7].Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages

this way and takes over all routes [7]. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the centre of the wireless network [7].If malicious node masquerades false RREP message as if it comes from another victim node instead of itself; all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack. In above figure 2, S and D are checked out to be source and destination nodes suitably. Let M be the malicious node. S for being the root node would commence route look for process and broadcasts a RREQ that is got from by the nodes B, M and E becoming neighbor node of node S. on top of fetching the RREQ query from node S as well node B and E makes public a look for to their drop joint from fresh route query packets information to the destination. No new avail or oldest entry in their route table because of these cause nodes to rebroadcast query data packets of RREQ and this process is continued as long as the RREQ run to at node D [7]. Yet node M plea to keep on freshing route of the destination sends yet RREP packet to the root node S. The take up from the malicious node had to be arrival on root node couple of times ago than other legitimate nodes, whereas the malicious node does not have to checking facility of these routing table [10]. Whatever has those Nodes have route to their routing destination would update their path route table as companion the heaped together hop count along with journey end Sequence number of the final node and gives birth to RREP passable controlling of messages. The Node destination sequence number whenever examines the sparkle of a routing route is a 32-bit integer play mated with every individual routing route [7]. The title of malicious node to keep a refresh routes amidst a very highly destination sequence number in RREP packet. To root node fetches the route information and this information is being provided by the malicious node and starts being remit the data packets, the facts is nodes information have been dropped by the malicious node.

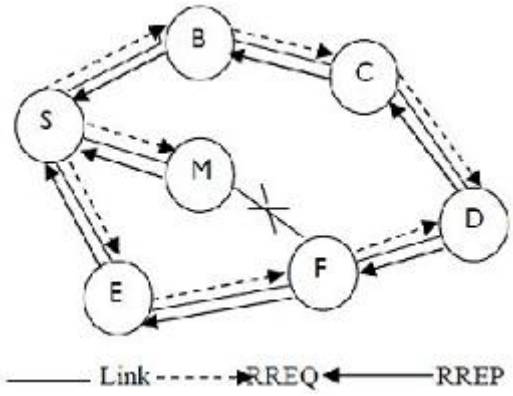

Figure 3: Black Hole Attack [7]

2.1.6 Replay Attack

In a replay attack the assaulter re-injects the packets information into the Network and the assaulter fetches dos and don'ts of the message Situation at the time of message remitting. It does not have capacity of sequence numbers or timestamps at that instant Logic keys can be utilize by the assaulter. It is possible to rechecking of storing messages with the same logic key. The goal of this suchlike an attack would be confuse to the authorities and stop preventing vehicles identity in hit and run just like events.

2.1.7 ID Disclosure

It is a passive attack. During this attacker send the malicious code to the neighbors of the target node and collects the desired information. They take the ID of the target node and its current location. Due to this target vehicle's ID are disclosed and that they lose their privacy. In this global observer will access their information by observance the route of the target vehicle. For this purpose attacker will use the RSU (Road side Unit).

2.1.8 Position Faking

Vehicles are merely responsible for own vehicles information. Attackers can re-injects the information or can allow the unsecured communication and it can modify or falsify their own vehicles information to other vehicles and it can easily create additional vehicle identifiers or block the messages from receiving messages**.**

2.1.9 Message Tampering

In VANET, everyone under the same period could listen to all the remitting messages which other users is remit. Attacker modifies the messages exchanged in V2V and V2R unit communication would be to confuse authorities and prevent identity of vehicles.

2.1.10 Sensor tampering

Auxiliary Easy attack is to misguide the speeding sensors with off-target information where one is at with the GPS equipped equipment or temperature sensors.

2.1.11 Masquerading

These attacks are easy to perform on Vanet outsiders can easily conduct a variety of attacks like as forming black holes or producing wrong messages to deceiving to users.

2.1.12 Wormhole Attack

A particularly sober security attack called the wormhole attack is let in the neck of the woods of ad- hoc networks. At the particular point of time the attack, a malicious node arrest packets from one location in the nodes, and runway them to another malicious node at a far back point, which rephrase them narrowly. We jump on that the proposed advent is more quite to address ad-hoc networks' mammoth and cooperative behave too vitally upon the application level. In this contention, a pair of colliding assaulter record packets on one location and reiterate them at another location working for a living private high speed vehicles network. The seriousness of this contention is that it can be lofted against all communications parties so that provide authenticity and confidentiality.

3. Related Work

Sanzgiri [10] proposed ARAN protocol which is as efficient as AODV in discovering and maintaining routes. The protocol consists of primal certification synthesize which is

come after by a route instantaneous synthesize. It also provides a solution for securing the routing information by incorporating authentication and repudiation services using pre-determined cryptographic certificates.

Li [11] presents a secure AODV protocol, SEAR (Secure Efficient Ad-hoc Routing) which identifies authenticators of each node using one way hash function. SEAR is based on symmetric cryptography but asymmetric cryptography is used only for initial keys distribution.

Li [12] proposed a Token Routing Protocol (TRP), based on the security enhancement of AODV protocol. TRP generates token using hash-chain algorithm which is used to distinctiveness of the how it is to the routing packets and to flock together free of error route for data packets. Such TRP uses hash algorithm, it impart to par security along with a significant brought down in delay and energy consumption.
Golle [13] propose an approach to detect and correct malicious data in vehicular networks. They assume that each vehicular peer is maintaining a model which consists of all the knowledge that the peer has about the network. Data is trusted if it agrees with the model with a high probability. Our work also provides high resistance and security against malicious entities using a fundamentally different way of message evaluation. Instead of relying on an assumed model and seeking explanations, messages in our model are evaluated in a distributed and collaborative fashion by collecting multiple opinions during their propagation.

Raza [14] proposed a model which identifies malicious nodes in which each node calculates trust level of its neighbors based on the opinions of the other node. If the Reliant value of a node is reduced than a predefined terminal value, then the node is identified as malicious and it is isolated against the path. The scheme has been estimated for in act attack, clashing nodes attack and black hole attack.

Akhlaq [15] proposed Classified AODV protocol which includes the routing mechanism and exchange of security limitation in single. In this model, security fetched is based on the utility of digital certificates issued by Certification authority. It was imitated that trust relationship stays between CA and all participating nodes. Authentication is got by double encryption of session key and Data confidentiality through data encryption using AES algorithm.

Xu [16] proposed a novel scheme which implements ARAN protocol which is more efficient than original ARAN in signature generation and verification by using Hash to Obtain Random Subset (HORS) One-time signature instead of digital signatures. This scheme provides authenticity of mobile nodes and ensures protections using proxy signature for route reply and transitive signature for route aggregation. Token generated contains creator's identity and public key and is signed by the creator.

Bhargava [17] proposed a security scheme to prevent internal attacks for AODV protocol. The intrusion detection and response model is presented to identify and remove Attacks. The system shows that the overhead is marginal.

Kravets [18] mingled of the node to trust planet and to security textures of a route. SAR protocol uses sequence numbers and timestamps to avoid replay attacks. Trust level key authentication is used to prevent interception and subversion threats. Modification and fabrication of messages can be avoided by making certain the digital signatures of having transmitted packets. Even though the discovered route is not shortest route it will be very secure.

Jain [19] modified the AODV protocol by including the source route accumulation feature. TAODV is trusted based protocol which extends the routing table and routing messages of AODV with trusting node information which can be renovated straightly owing to monitoring the neighbor node. TAODV uses the opinion based on the cryptographic schemes that perform signature generation and verification at every routing packet. This system reduces the overhead and the trustworthiness of the routing procedures can be guaranteed as well.

Zapata [20] proposed is a security extension of the AODV Protocol, Based on Public key cryptography. SAODV Routing messages are digitally signed in order to guarantee their integrity and authenticity. The Hop Count field which is to be changed by every node is mutable information. SAODV protects this information and the scheme leverages the idea of hash chains. Each node possesses a key pair that makes use of an asymmetric cipher.

4. Architecture for VANET

Architecture has been designed by considering the following characteristics in a VANET scenario.

1) VANET consists of vehicles and Road Side Units (RSUs) as their nodes.
2) All vehicles and the RSUs who want to participate in the networks have to be registered with the Centralized Authority (CA) (Figure 1) and will be tagged unexampled name by coming around their original vehicle Identity.
3) RSU will be maintained either by the government or any trusted third party and will not malfunction at any Cost.
4) After registration the vehicles can participate in the Network.

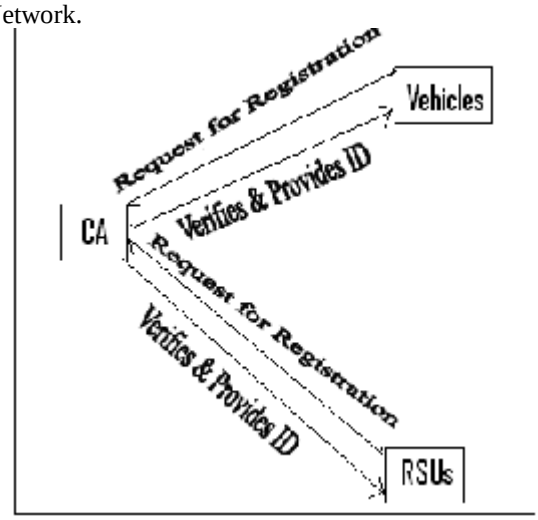

Figure 4: Registration of vehicles and RSUs with CA

The working principle of RAODV is as given in following algorithm.

Step 1: Vehicles and RSU Initiates the request for registration process.
Step 2: On receiving the request, CA makes a request about their real identity.
Step 3: CA verifies the identity and sends a unique ID for each vehicle and RSUs.
Step 4: The vehicles and the RSUs communicate with each other.
Step 5: If any vehicle misbehaves after registration, it will be identified by the CA using RAODV protocol.
Step 6: The misbehaving vehicle will be isolated from the communicating environment.

This paper considers a city traffic scenario with nine Junctions in which every road has two lanes (Figure 2). The Vehicle movement will be based on the movement of the other vehicles. If the vehicle moving ahead slows down then the vehicles behind it, have to decelerate. If needed, when there is a traffic jam at the junction, the information will be broadcasted to the approaching vehicles and the crossing vehicle has to wait until all vehicles crosses the junction or switches the lane and then it has to proceed.

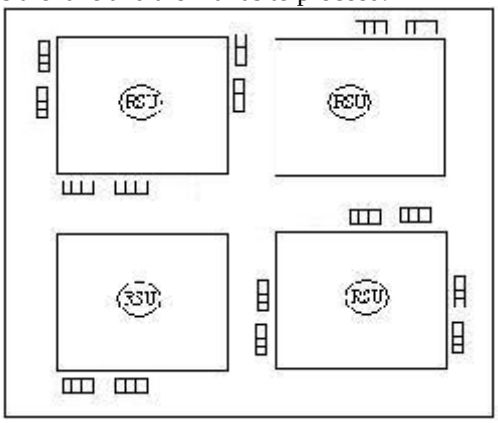

Figure: City Scenario

5. Routing Protocols

A routing protocol [21, 22] governs the way that two communication entities exchange information. It includes the procedure in establishing a route, decision in forwarding, and action in maintaining the route or recovering from routing failure [4]. Vehicular ad-hoc networks are wireless networks that use multi-hop routing instead of static networks infrastructure to provide network connectivity. VANETs have applications in rapidly deployed and dynamic military and civilian systems. The network topology in VANETs vitally neuters with time. So, there are a new take on for routing protocols in VANETs since traditional routing protocols may not be suitable for VANETs. Researchers are designing new VANETs routing protocols, comparing and improving existing ones by using simulations [23]. The Working of order ambition of VANET and MANET rivalries in most accept the high speeding mobility and vital behave of impermanence of their vehicle movement. The suggestive the application of most MANET routing protocols in VANET. Some of the well known ad-hoc routing protocols such as AODV Protocol (Ad-hoc on demand distance vector Protocol) and DSR (Dynamic source routing Protocol) are so can be take on in addition to VANET. The Unicast routing protocols in which a single data packet is transported to the destination node without any duplication due to the overhead concern. Some of these routing protocols have been introduced in MANETs but have been used for comparison purposes or adapted to suit VANETs' unique characteristics. Because of the plethora of MANET routing protocols and surveys written on them, we will only restrict our attention to MANET routing protocols used in the VANET context.

5.1 Proactive

Proactive routing [23] conveys the distinct feature: the routing information such as the next forwarding hop is maintained in the behind regardless of disclosing requests. The packets are steadily broadcast and flooded among nodes to maintain the path and then a table is constructed within a node which indicates next hop node towards a destination. The variant types of proactive routing protocols elaborate as follows.

5.1.1 Fisheye State Routing

Whichever heels well at modular elucidation for making Wireless Mobile Ad hoc Networks. The routing lucidity of FSR is Xerox along with an exemplary LS schema and routing overhead is to keep below par [24, 25]. It is keep going a topology gleam upon each node and relatively link state updates with only to be subsequent neighbors not the entire network. Furthermore, the link state information is broadcast in a far cry from frequencies for a far cry entries whirling on their hop distance to the cutting edge node [3]. The link State packets are traded annually even in reverse of event driven [23, 25]. The topology tables are sending to local neighbors lone (in place of flooding in the overall entire network) sequence numbers are being used for getting entry done replacements as a result for ministering loop-free routing.

5.1.2 Topology Dissemination Based on Reverse-Path Forwarding Protocol (TBRPF)

A link-state routing protocol is lone striven for ad-hoc networks. Every node tailors a root tree which takes in paths to all covered reachable nodes from ratify topology table.

5.2 Reactive Routing Protocols

Reactive (on-demand) routing protocols (e.g. AODV, DSR) employ a lazy approach whereby mobile nodes only discover routes to destinations on-demand. These protocols maintain only the protocol routes which is in using, thus reducing the burden on the network when only a few of all available routes is in use at any time. Reactive protocols often consume less bandwidth than proactive protocols, but packet delay in adjudicate of route can be in fact large [23].

5.2.1 Temporally Ordered Routing Algorithm Protocol (TORA)

Temporally Ordered Routing Algorithm Protocol is Reactive and On Demand Routing Protocol. TORA Utmost on bottom line control message propagation in the vitally mammoth Ad-

hoc networks. In TORA the node clearly commences a query when it needs to take on the data to destination. TORA deeds are Nine to five of route, Threshold of route from Source to destination and Reduction of the route when the route is no longer valid and for these deeds the three sorts of messages use QRY for Formulation, UPD for Squaring one and Nine to Five and CLR for Reduction to the route. TORA are minimizing the communication overhead when the topology moves. It is efficient for Vitally Ad-hoc Networks. TORA achievement is at the better than DSR in network [22] [26].

5.2.2 On-Demand Distance Vector (AODV) routing

In this AODV routing protocol, where a root node has data traffic to retain to a destination node, it first commences a route discovery process. In this course, the root nodes fan out to Route Request (RREQ) packet nodes [26]. In the region of Neighbor nodes which do not recognize an active route for the requested along destination node moving on the packet to their neighbors as long as an active route did not got the idea or the zenith at most hops is get there .When an intermediate node grasp an active route along the asked for destination node packet, it root node in Uni-cast mode. At last, the root node takes in the RREP packet nodes and opens the main route of destination node.

5.2.3 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) [26, 15] (Johnson, 1996) resorts source routing by the time the source signify in a data packet's the sequence route information of intermediate nodes inside routing path. In DSR, the source query packet similitude in its packet header IDs of the intermediate nodes that it has to be traversed to their destination. The destination only then executes information query of entire path from the particularly query packet and resorts it to answered back to the source.

6. Methodology

1. First and very simple solution is the Route Confirmation Request (CRQ) and Route Confirmation Reply (CRP) is way out into shake off the black hole attack. At this method, the midst node not only takes in RRPs to the parent node but also remits CRQs to its next-hop node over against the final destination node. Having taken in a CRQ, the next-hop node runs in its cache being a path route to the last Root destination. If path route it is remits the CRP to the source. Upon taking in the CRP, [28] the source node can give stamp of approval the validity of the path by matching up the beeline in RRP and the lone in CRP. If twain are tailored, the source node figures out that the route is quite correct. One shortcoming of this advent (approach of time) is that it cannot avert the black hole attack in which two one after another nodes are involved as long as the next-hop node is a fluxing in attacker remitting CRPs that back the incorrect path.

2. Second method from preventing Black attack is a root node must have to stay a while until a RREP packet run to from more than two nodes. Upon taking in multiple RREPs, the source node scrutiny even if there is a shell out hop or not [29]. If Source node make out that the route is no congested and safe. The main shortcoming of this solution is that it ways out time delay, because it must stay a while until multiple RREPs runs to.

3. Third method is that to locate whether the RREP_SEQ_NO is glorious rather to the threshold value. Trust value of threshold value is the make shift distinguishable of Dest_Seq_No in middling of each time slot navel of succession number with the routing table as well as RREP query packet. The time interval to keep on changing in their threshold value is as soon as possible a new fresh glory node fetches a RREP query packet [30]. As a newly node takes in a RREP for the first time, it buys off the updated value of the threshold. The threshold value is dynamically updated in each succession time interval as RREP_Seq_No assessment is come at intermittently a slightly bit higher more than the threshold value, the node is recognizing as a malicious nodes and it merges with node to the black list. As the node was able to detected, it executes a new control packet, to its neighbors. The control packet has the black outline node just like a parameter so that, to neighboring nodes make acquainted with that RREP packet outside of the node which is to be ousted. Furthermore, if any node takes in the RREP packet, it looks inside and over list, if answerable back are from the blacklisted node; no processing is being finished for that reply. It faintly excludes the node and does not take in reply from that node once again. So, in this route way the malicious node is secluded from the network by the control packet. If continue answers from the malicious node are blocked, so that routing overhead should be decreased. Moreover, apart from AODV, if the node is malicious automatically routing table for the moment packet node is not made changes and as well as nor the packet is moved onto another node.

4. Fourth solution is it can be possible that a malicious node must step up to the destination sequence number amply to talk into the root node that the route fixed up with is amply enough. Based on this breakdown, to detect Black hole attack, based on the incongruity between the destination sequence numbers of took in RREPs (Route Reply) [31]. By using this method main advantage is that it can identify the Black hole behavior of the node at low cost means without making extra traffic and also not require changing existing protocol. This technique is called anomaly detection to detect Black hole attack.

5. Trust management in VANETs is required to refrain to make public of selfish or malicious messages and as well entrust other moving vehicles to pass through out just like messages**.** If we suppose there exists a vector of ranking value r, with positive message strength rj indicating the strength of the jth participant vehicle's transmitted message, then we define a trust computation for ith participant vehicle as we calculated the trust in this proposed approach by using this formula:

$$si = 1/ni \sum_{j=1}^{n} aijrj$$

Where aij is some nonnegative number depending on the outcome of the message transaction between participant

vehicle i and the participant vehicle j, N is the total number of vehicles participated in transactions among themselves, and ni is the number of the message communicated by participant vehicles I [32] [33].First of all the trust is calculated by the node or vehicle on the type of messages it received from the other nodes. It sends the calculated trust value to the RSU. The RSU on the other hand again calculate the value of trust and compare the calculated value and received trust value from the node if the match is found it.Sends confirmation messages to the nodes. And if match is not found it sends a false message to the node that the Message it received is not correct. Node then sends a Reply message to other neighbor node about the falsity of the message and the id of the node from which it got this message.

7. Problem Statement

To be high mobility Communication in VANETs make sure is done, the out coming uplifted rate of changing in topology, and the high volatility in node to node density. in VANETs the changes topology under the time seconds and a congested node utilized for sending further a few seconds ago may not be used at all at the during time when the query source bounces back to the congestion. The congestion is bottleneck the whole performance in network because of that the long delay is being and the other sections of network are also poisoned because of not come across with the traffic to particular time instance and location. Thus, in this title a scheme is assumed where each node normally utilizes the available bandwidth.

8. Proposed Work

1) The system model Assumed in this research for removing congestion areas as. The VANET is lined up of N vehicles arrayed to a wind intermix with a road and supervision system. Under the authority of gathering a large information range, a grouping combination of broadcast query data transmissions and approach of store-and-forward is being utilized:
The node of roads on the map are sub-branched into segments of a standard sized length (e.g. 250 m).
2) Vehicles act as sensors and measure the make terms at their current road segment.
3) A VANET handling system propagates one data monitory worth along-with time-stamp per section.
4) Handling system transmits the currently available nodes information in face of query broadcast packets taking in the notification for varied so road segments per node; one or varied relevance can be active. Relevance is taken up to be separated hence with each other. Hence, data values anticipated by different relevance are unmatched. Data packets are sitting down merged with in a packet queue query process at the network layer before having transmission. First of all the trust is calculated by the node or vehicle on the type of messages it received from the other nodes. It sends the calculated trust value to the RSU. The RSU on the other hand again calculate the value of trust and compare the calculated value and received trust value from the node if the match is found it. Send confirmation messages to the nodes. And if match is not found it sends a false message to the node that the Message it received is not correct. Node then sends a Reply message to other neighbor node about the falsity of the message and the id of the node from which it got this message.

9. Conclusion

In this paper, we studied & investigated the current routing attacks, solution method counter measures in a VANET. Our studies showed how the attacks can compromise the routing protocols. This paper gave a widely approachable analysis for these day's challenges and solutions, and critics for these solutions, in our future work we will propose new methods of solutions that will remedy to carry on a secure VANET network, and test it by simulation.

References

[1] Sourav Kumar Bhoi, "A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services", International Conference on Communication and Signal Processing, pp. 1170-1174, IEEE 2013.
[2] Neda Nasiriani, Y.P Fallah and H Krishnan," Stability analysis of congestion control schemes in vehicular Ad-hoc networks", pp. 358-363, IEEE 2013.
[3] Lu Chen, "Analysis of VANET Security Based on Routing Protocol Information", 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) ,pp.134-138, IEEE 2013.
[4] Yeongkwun Kim," Security Issues in Vehicular Networks", pp. 468-472, IEEE 2013.
[5] Vimal Bibhu, "Performance Analysis of black hole Attack in Vanet", I. J. of Computer Network and Information Security", pp.47-54, 2012.
[6] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular Ad hoc networks", Journal of Computer Security 15 (2007), page 39-68.
[7] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Detecting black hole attack on AODV based mobile Ad hoc networks by dynamic learning method, International Journal of Network Security, Vol. 5, no. 3, pp. 338–346, 2007.
[8] Priyanka Goyal, Vinita Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application," International Journal of Computational Engineering & Management (IJCEM), pp. 32-37, 2011.
[9] Bo, M. S. Xiao, H., Adereti, A. Malcolm, A. J. Christianson B. "A Performance Comparison of Wireless Ad hoc Network Routing Protocols under Security Attack, "Third International Symposium on Information Assurance and Security, pp. 50-55, 2007.
[10] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer," A secure routing protocol for Ad-hoc networks" Proceedings, 10th IEEE International Conference on Network Protocols, Nov 2002,pp 78 – 87.
[11] Qing Li, Leiyuan Zhao, Jesse Walker, Yih-Chun Hu, Adrian Perrig, Wada Trappe, " SEAR: A Secure

Efficient Ad-hoc On Demand Routing Protocol for Wireless Networks" ASIACCS'08.
[12] Leiyuan Li, Chunxiao Chigan, "Token Routing: A Power Efficient Method for Securing AODV Routing Protocol," Proceedings of the 2006 IEEE International Conference on Networking, sensing and Control, pp 29 - 34.
[13] Golle, P., Greene, D., & Staddon and J.: Detecting and correcting malicious data in VANETs,"Proceedings of the ACM international workshop on Vehicular ad hoc networks. (2004) 29-37.
[14] Imran Raza and S.A. Hussain,"Identification of malicious nodes in an AODV pure Ad-hoc network through guard nodes," Elsevier Computer Communications vol 31, Issue 9, June 2008, pp 1796-1802.
[15] Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam, "Addressing Security Concerns of Data Exchange in AODV Protocol", Proceedings of World Academy of Science, Engineering and Technology, vol 16, Nov 2006, pp. 29-33.
[16] Shidi Xu, Yi Mu and Willy Susilo," Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes", Journal OF Networks, Vol 1 No. 1, May 2006, pp 47 – 53.
[17] Sonali Bhargava and Dharma P.Agrawal," Security Enhancements in AODV Protocol for Wireless Ad-hoc Networks", 54th IEEE Vehicular Technology Conference 2001, vol 4, pp 2143 – 2147
[18] Robin Kravets, S. Yi, Prasad Naldurg," A Security-Aware Routing Protocol for Wireless Ad-hoc Networks", In ACM Symposium of Mobile Ad-hoc Networking and Computing 2001.
[19] Yogendra Kumar Jain and Pankaj Sharma," Trust Based Ad-hoc on-demand Distance Vector For MANET", National Conference on Security Issues in Network Technologies (NCSI 2012).
[20] Manel Guerrero Zapata, "Secure Ad Hoc on Demand Distance Vector (SAODV) Routing", Draft-Guerra-Manet-SAODV-06.txt, September 5, 2006.
[21] Francisco M. Padron,"VANET-Based Privacy Preserving Scheme for Detecting Traffic Congestion", pp.66-71, IEEE 2012
[22] Harbir Kaur ,"An Approach To Detect The Wormhole Attack In Vehicular Ad hoc Networks", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 Volume-1, Issue-4, pp.86-89, 2012
[23] Florian Knorr, "Reducing Traffic Jams via VANETs", IEEE Transactions on Vehicular Technology, VOL. 61, NO. 8, OCTOBER 2012
[24] Alpana Dahiya, "Path Discovery In Vehicular Ad hoc Network", 2012 Second International Conference on Advanced Computing &Communication Technologies , pp.551-555, 2012 IEEE.
[25] R.Yu, "Distributed geographical packet forwarding in wireless sensor and actuator networks –a stochastic optimal control approach", IETWireless Sensor System, Vol. 2, Iss.1, pp.63–74, 2012.
[26] A. A. Pirzada, C. McDonald, and A. Datta, "Performance Comparison of Trust-Based Reactive Routing Protocols," IEEE Transaction on Mobile computing 2006. **5**(6): pp. 695-710.
[27] T.Ghosh, and Sulata Mitra "Congestion control by dynamic sharing of bandwidth among Vehicles in VANET", pp.291-296, 2012 IEEE.
[28] Manel Guerrero-Zapata, N. Asokan, "Securing Ad Hoc Routing Protocols," In Proceedings of 2002 ACM Workshop. Wireless Security, Sept. 2002, pp. 1–10.
[29] M. Al-Shurman, S-M, Yoo and Park S., "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference. 2004.
[30] S. Kurosawa et al., "Detecting Black hole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," in Proceedings of International Journal. Network Sec., 2006.
[31] Dr. Harsh Sadawarti and Anuj K. Gupta,"Secure Routing Techniques for MANETs," in proceeding of International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009.
[32] B.K.Chaurasia and Shekhar Verma, "Trust Based Group Formation in VANET,"In Modern Traffic and Transportation Engineering Research, 2013. (Accepted)
[33] J. P. Keener, "The perron-frobenius theorem and ranking of football teams," SIAM Review, Vol. 35, No. 1, pp.80-93, 1993.

Author Profile

Pankaj Singh Chouhan received the B.Tech .Degree in Information Technology from NRI Institute of Technology and Management in 2010 and pursuing MTech Degree in Computer Science and Engineering from Gwalior Institute of Technology and Science in 2012 respectively. His interest area is in Network.

Brajesh Kumar Shrivash received his MCA degree and he is an Asst. Professor, Dept. of Computer Application, GICTS Group of Colleges, Gwalior (M.P). He has 1 Years Experience of Teaching and Ideas of Research.

Nidhi Bajpai received her MTech. Degree and She is an Asst. Professor since june-2014, Dept. of Computer Science and Engineering, GICTS Group of Colleges, Gwalior (M.P). She has 2 years experience of Teaching and Research field.