Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

LI-AODV: LIFETIME IMPROVING AODV ROUTING FOR DETECTING AND REMOVING BLACK-HOLE ATTACK FROM VANET

ZAID A. ABDULKADER[1,2,3], AZIZOL ABDULLAH[2,4], MOHD TAUFIK ABDULLAH[2,5], and ZURIATI AHMAD ZUKARNAIN[2,6]

[1]Al Iraqia University, Baghdad, Iraq

[2]Faculty of Computer Sciences and Information Technology Universiti Putra Malaysia 43400 Serdang, Selangor, Malaysia

E-mail: [3]zaid9979@yahoo.com, [4]Corresponding Author: azizol@upm.edu.my, [5]taufik@upm.edu.my, [6]zuriati@upm.edu.my

ABSTRACT

Vehicular Ad-hoc Network (VANET) is an emerging technology and is an application of Mobile Ad-hoc Network (MANET). So it has same characteristics like wireless medium, dynamic topology, collision interference. Objective of VANET is to create and provide communications among group of vehicles without any central base station. An attack like Black hole in VANET is a main issue that degrades performance of whole network. Many existing algorithms tried to solve this issue but not completely. In order to solve above problems in VANET from black hole attack, we propose a new routing protocol named "*Lifetime Improving Ad-hoc On-demand Distance Vector (LI-AODV)*". To reduce overload in routing process we introduce a scheduling algorithm named "*Hybrid Round Robin with Highest Response Ratio Next (HRRHRRN)*". To prevent the network from Black hole attack we propose a new security algorithm called HMAC-SHA3-384 which is a combination of SHA3-384 and HMAC. This LI-AODV achieves better performance in lifetime of the network, reduces black hole attack, End-to-End delay, throughput, packet loss, Packet delivery ratio. Our experimental procedure provides efficient identification and removal of black hole attack in urban VANET.

Keywords: *VANET, Black hole attack, AODV routing protocol, Ad-hoc network, HMAC, SHA3-384.*

1. INTRODUCTION

VANET (Vehicular Ad-hoc Networks) continues to provide new applications by facing large number of challenges. This network is responsible for communication between vehicles which moves. VANET is different from MANET that vehicles (nodes) do not move randomly; rather it follows some strict rules like fixed paths (Urban roads and highways). There are various applications in VANET such as Road Traffic Safety, Traffic Engineering or Efficiency, Comfort and Quality of Road Travel, Dynamic Topology, Frequent Disconnections, Mobility Modeling, Predictable Mobility Patterns, Use of Other Technology, No Power Constraint and Stringent Delay Constraints. VANET are responsible for communication between moving vehicles in a certain environment. Here communication is done on two types they are 1) Vehicle to Vehicle Communication 2) Vehicle to Infrastructure (Road Side Unit) Communication. The main challenges of VANET are 1) Quality of Service (QoS): QoS guarantees for users with reduced delay, transmission without packet loss, less retransmission. 2) Efficient Routing Algorithm Design: It refers a routing algorithm with less delay, maximum system capacity and less computational complexity. 3) Scalability and Robustness: VANET is scalable with several network scales and robust to topological changes when required. 4) Co-operative Communication: here the information exchange is done among themselves 5) Network Security: A security mechanism is designed which information exchange is done with concerned node without any loss [1]. Figure 1 describes the Architecture of VANET.

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

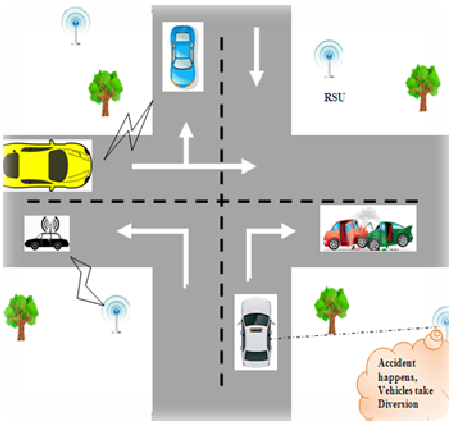

Figure 1 VANET Architecture

Routing plays major role in the networking for transferring the packets from source to destination. Traditional routing mechanism is not applicable for the Ad-hoc networks, since their topology is time varying. Routing is divided into three types they are: Pro-active Routing, Reactive Routing and Hybrid Routing. Here Pro-active Routing is a table driven mechanism where every node maintains a routing table ex: Link State Routing (LSPR), Reactive is an on-demand process, and they maintain routes when they needed ex: AODV (Ad-hoc On-demand Distance Vector), Hybrid Routing is a combined work of both Proactive routing and Reactive routing protocol, here each node proactively maintains the topological information within its routing zone only ex: ZRP (Zone Routing Protocol). AODV is a reactive Routing which determines a route to destination when source needs to send any message. This routing algorithm is loop-free and avoids the counting to infinity problem. The drawback of AODV routing protocol is lower performance in terms of scalability and higher latency [2].

In VANET, Dedicated Short Range Communication (DSRC) is a frequency band which is used as DSRC (Communication medium). This delivers safety and non-safety messages for the entire network. Attackers create more problems in network by getting full access of communication medium (DSRC). Commonly attackers cover main area of the network that depends on the nature of attacks. Black hole attack is one of the attacks which are more vulnerable to the Vehicular network. In this type of attack, an attacker node transmits the packet through itself. This node attracts the source by sending reply packets to source node, when source node transmits packet through attacker node, finally the packets are dropped [3] and [4].

In paper [5], author proposed a modified AODV protocol named ISDNAODV that identifies and eliminates black hole attack in the MANET network. Black hole attacks are of two types they are 1) Single black hole attack which is applied via one of the existence nodes in the network 2) Total Black hole attack is in which two or more attacker nodes cooperates together for an attack. In this protocol they introduced some rules for AODV protocol that identifies the black hole attack based on monitoring packet transferring for every node. There is a drawback in this protocol, while monitoring the packet transmission we need to monitor the lifetime of every node otherwise packet loss will occur. Many existing researchers produced an application of various solutions that results in highest delay.

In Paper [6], black hole attacks are eliminated by the AODV protocol with new rules and to safe guard the original messages in MANET. In this system, new rules are generated on the AODV protocol. Here initial request is flooded to all other neighboring nodes and receives reply from every nodes. While receiving the reply packets, source node waits and makes decision about the replies of every nodes and decision is taken using newly generated rules. After that a safe route is analyzed and chosen for packet transmission. This system results in eliminating of black hole attacks and results in higher delay.

On detect and remove black hole attack, Researchers focused in MANET, and for protecting VANET, many security algorithms are proposed based on Cryptography. For transferring the messages with higher security files are encrypted with the cryptographic algorithms. Nowadays Hashing functions are utilized for compressing the message and they are forwarded. Hash algorithms like MD (Message Digest), SHA (Secure Hash Algorithm) are used for secure packet transmission in the network.

In our proposed routing mechanism we introduce a new algorithm named "LI-AODV: Lifetime Improved AODV" Routing which detects and removes the black hole attack in VANET and also it improves the network's lifetime. Initially we identify the energy of every node. A RREQ message from the source node is flooded to all neighbor nodes and we receive RREP from the neighbor nodes. Here we use path rater which allows choosing the best path from source to destination. After choosing best path, source node use six rules that analyze behavior of nodes based

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

on RREQ and RREP message transmission between nodes. If best path contains malicious node, then alternate best path is chosen for packet transmission in the network and a warning signal is transmitted over a network for removing a specified attacker node. To prevent our network we introduce a novel hashing algorithm called HMAC-SHA3-384. Our experiment results improved lifetime of network.

The main contribution of our proposed system is as follows:

1) Introduced a LI-AODV routing Algorithm for detecting and eliminating the black hole attacks in Vehicular ad hoc Network with high ratio of detection rate-true positive and generates a low ratio of false positive rate.
2) Introduced a load balancing algorithm called Hybrid Round Robin with Highest Response Ratio Next (HRRHRRN) that decrease the average waiting time to increase the network speed.
3) Designed a security algorithm named as "HMAC-SHA3-384" for preventing the network from vulnerable attacks.

Section 2 describes the related works done in existing system. In Section 3 we see the problems that are created in AODV routing mechanism. In Section 4 we define and discuss about the proposed routing algorithm and security algorithm. In Section 5 we present the performance evaluation and experimental results of our proposed algorithm. Finally in Section 6 we conclude the paper.

2. LITERATURE SURVEY

Researchers such as Kunal V. Patil and M. R. Dhage discussed about VANET and they proposed a new routing algorithm for VANET [7]. In VANET, performance of routing protocols depends on different scenarios like city and highway. A new automatic selection of optimal configuration offers best performance. In this process, a necessity first algorithm is introduced instead of greedy search algorithm. Based on proposed protocol, network traffic load of administrative packet is reduced. The main idea of this routing protocol involves two steps 1) Suitable Configuration extraction and 2) Deployment of it. This will result in more efficient and accuracy in developing communication cost for improving throughput and efficiency.

In paper [8], author Mukul Sharma presented an advanced AODV protocol in MANET. Existing AODV Routing algorithm introduces higher communication delay due to single route reply. To avoid this author introduced Advanced AODV (Reverse AODV (ADV-AODV)) protocol which helps to find multiple route replies. It reduces path fail correction messages in the network. Initially a RREQ is transmitted to find a destination node, after finding destination node, immediately destination node floods Reverse Request (R-RREQ) to find the source node.

In Paper [9], authors like Ketan S. Chavda, Ashish V.Nimaval, proposed a modification in existing AODV routing protocol. This finds optimal path between sender node and receiving node. This algorithm does not modify any working procedure and it does not affect working of either intermediate or destination node. It has pre-process call named Process-RREP which continues to accept all RREP packets. After receiving RREP packets form neighboring nodes it calls a function named Compare_RREP which actually compares every RREP packets based on their sequence numbers. A higher sequence number of a destination node is identified based on same RREP packets. Then this specific node is suspected to be malicious node and alert message for node identification is generated to their neighboring nodes which results in elimination of black hole attack.

In paper [10], an improved AODV protocol is proposed that reduce the unbalanced node usage which results in higher energy consumption and delay. This system introduces a stability factor which conserves and stabilizes energy among nodes followed by a delay reduction mechanism which reduces average end-to-end delay in the network. This stability factor is used for calculating the energy of each node. This considered that low energy level leads to number of link breaks. This process allows 3 modifications in that work, 1) Stability Factor 2) Time to Live (TTL) for RREP 3) modified Expanding Ring Search (ERS) for route discovery operation.

In paper [11], Researchers such as Fei Wang, Yongjun Xu, Hanwen Zhang, Yujun Zhang and Liehuang Zhu proposed a new Two-Factor LIghtweight Privacy preserving (2FLIP) which enhances security in VANET for communication. In order to achieve goals a two-factor authentication is introduced based on biological password and decentralized certificate authority (CA). This Factor Authentication in VANET is mainly done by Message Authentication Code (MAC) and hashing operations which improves privacy and security in the network. Here every vehicle is equipped with a tamper-proof device (TPD) which would be used with biometric

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

technology. This tamper-proof device is embedded with a OBU (On-Board Unit) in order to store keys and to verify the messages. In paper [12], Researchers discussed a scenario based performance analysis in VANET based on AODV and GPSR routing protocols. These scenarios are done under several traffic conditions with performance metrics such as Packet Delivery Ratio (PDR) and average End-to-End delay (E2E delay). For experimental verification they used Urban Scenarios and Highway Scenarios.

Researchers such as Peppino Fazio, Floriano De Rango, Cesare Sottile, Pietro Manzoni, Carlos Calafate suggested a new protocol for reducing the reduction of interference level during mobile transmission in VANET environment. This considers availability of different channels in the spectrum. Here an interference aware routing scheme is proposed for multi radio vehicular networks that maximize average SIR level connection between source and destination. This idea is integrated with reactive routing protocol such as AODV protocol which allows designing a new protocol named Dynamic Frequency Interference Aware AODV (DFIA-AODV) [13]. Here a recurrent evaluation of SIR level from source towards destination is proposed which gives opportunities for choosing next-hop in routing operations depending on best SIR values. This mechanism is based on signaling scheme of AODV which takes advantages of dynamic allocation of DSRC spectrum.

In paper [14], a secure mechanism is introduced an algorithmic approach that focus on analyzing and improving security of AODV in MANET. Aim of this approach is to detect and remove black hole attack in the network and they introduce an additional route to the intermediate node which replies RREQ message that verifies the route existing between intermediate node and destination node. If the reply to source is yes, source node establishes a route to destination and it allows packets in that route to reach destination. If the reply is no, source node discard route to the intermediate node and it generates an alarm message to the whole network for drop packets to malicious node. But this approach gives best results when working with single black hole attack whereas it does not applicable for cooperative black hole attack. Here they use Data Routing Information (DRI) table that will be used in cache and current routing tables which works with modified AODV routing protocols.

Authors like P.A. Kamble and Dr. M.M. Kshirsagar presented a cross layer technique which finds channel security at link layer for AODV protocol to improve the communication between vehicles for safety applications [15]. This improved AODV process reduces End-to-End Delay in the network based on broadcasting the data packet when there is a local repair. For improving security in AODV, a new SAODV mechanism is introduced which includes digital signature and hashing functions they use digital signatures for authenticating non mutable fields then for authenticating hop count fields hashing chains are used.

In paper [16], authors discussed about the Secure Hash Algorithm (SHA 3). This algorithm provides a good security for data using authentication format by generating hash code. Three transforms such as rho, pi and chi are merged into single transform for logical optimization. It has a fast running speed and it is widely used in digital signatures and 3DES key generation systems. SHA have different variants like sha224, sha256, sha512 and sha1024.

Researchers like Hengheng Xie, Azzedine Boukerche, Antonio A.F. Loureiro proposed a multi-channel error recovery for video streaming application in VANET. In a VANET, error recovery is a critical issue for high quality video streaming and real time videos [17]. So an error recovery process proposed in Multi-channel such as reliable channel and unreliable channel. To reduce the delay in the network we use Priority queue, Quick Start and Scalable Reliable channel (SRC).

3. PROBLEM DEFINITION

VANET is a subgroup of MANET, which allows communication between vehicles on the road side for improving traffic and safety applications. VANET is slightly different from MANET because in MANET nodes can move dynamically whereas in VANET nodes movement is strictly warned. This network is not supported against attacks; one main attack is Black hole attack. Many existing algorithm [5] tries to identify the black hole attack, after identification it choose alternate path for packet transmission in the network. But this approach has a drawback that it does not notify energy of the node. If node's energy decreases during packet transmission then it results in packet loss.

During routing process in VANET, every node behavior is analyzed and based on result of analysis the source node send packets to intermediate node. For analyzing the behavior of nodes in the network, many rules in [6] are used for

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

notifying the behavior of intermediate nodes. For every transaction we need to analyze the behavior, after analyzing nodes we need to identify the safe route for packet transmission which results in higher delay. Many existing cryptographic hash functions [16] are used for providing secure message transaction between the vehicles. To solve this problem proposed a routing algorithm that includes lifetime of a network and reduces delay in the network.

4. PROPOSED WORK

4.1. Overview:

VANET is a kind of Ad-hoc networks that provides communication between Vehicle to Vehicle and Vehicle to RSU (Road Side Unit). In our proposed system, we introduce a routing algorithm named Lifetime Improving Ad-hoc on-demand Distance Vector routing (LI-AODV) that indentifies and removes black hole attack in the network. Initially, sender node floods RREQ to its neighboring nodes and it receives the RREP from all neighbors. We use path rater for choosing the best path for packet transmission to destination node.

After choosing best path, source node notifies the malicious behavior of nodes based on nodes behavior. If best path has malicious nodes then alternate path is chosen for packet transmission. This algorithm results in better performance in terms of lifetime, end-to-end delay, throughput, packet delivery ratio, attack detection. We introduced a security algorithm named HMAC-SHA3-384 for preventing the network from black hole attack. Figure 2 specifies the proposed architecture of VANET.

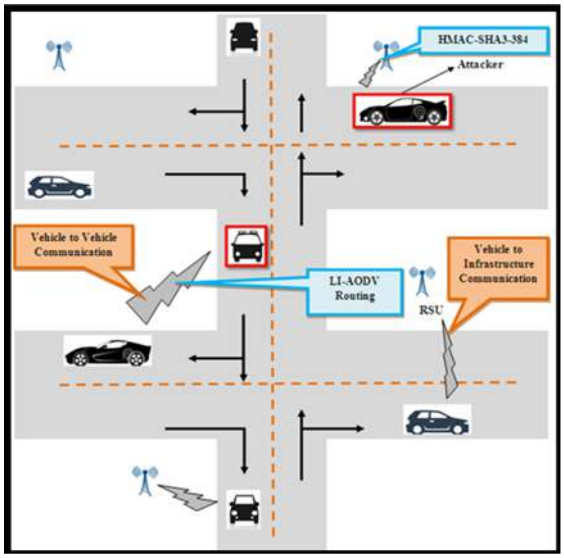

Figure 2 Overview of Proposed System

4.2. Routing Algorithm:

Routing is an important process in networking which selects best paths for packet transmission from source node to destination node. In our proposed system, our routing algorithm is similar to AODV protocol which has some additional rules and constraints. In order to detect black hole attack every node must be active to transfer the packet to reach other node, so that we identify the energy of the node based on Stability Factor [10]. Stability factor is defined as ratio of node's remaining energy to its initial full energy. This factor is used to track remaining energy of node in the network.

$$\text{Stability Factor (SF)} = \frac{\text{Remaining energy of node}}{\text{Initial Full energy of node}}$$

By using stability factor, we notify the energy of every node which must have ability to transmit the messages. This results in improvement on lifetime of the network. Then sender node transmits RREQ packet to the neighboring nodes and it receives reply packet (RREP) from neighboring nodes. Here we use path rater for choosing the best path from source node to destination in the network. Our best path is chosen with additional constraint called SF. This stability factor informs the energy of nodes that has capacity to transmit messages to other nodes. Our specific best path does not contain any malicious nodes (Black hole attackers), where packets must be transformed safely to destination, so that we propose some rules that specify the behavior of nodes and source node identifies the intruders. Here the behavior is denoted by the packet transmission of RREQ and RREP packets.

The following rules are used for identifying the attacker node in the network,

1) When a node delivers packets to destination then it is an honest node.
2) When a node receives many data and it sends other data, then it has a possibility of misbehavior node.
3) When a node contains less number of RREP and with higher sequence number must be a misbehavior node.
4) When a node sends RREP with higher sequence number to source node have the possibility of misbehavior node.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5) Followed by Rule 2, specific node sends RREP packet to source node, then it is surely a misbehavior node.
6) Followed by Rule 2, specific node does not send any other packets to others, and then it is assumed to be a selfish node.

Based on the above rules, we check the malicious attackers in our best path. If any malicious node exists in the best path, we choose alternate best path using path rater. We generate alarm signal in the network for eliminating malicious node. Figure 3 describes proposed LI-AODV Routing and Figure 4 describes proposed routing algorithm.

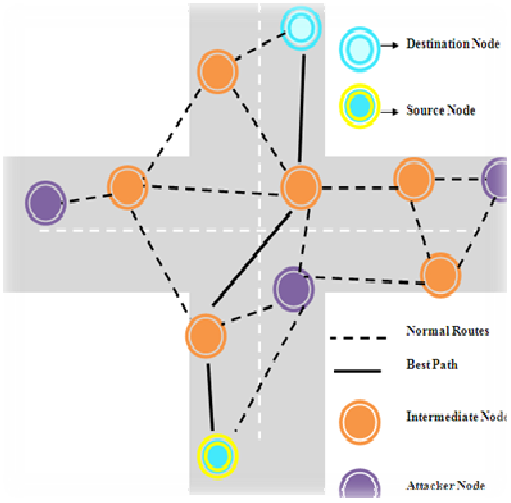

Figure 3 Proposed LI-AODV Routing

==========

Pseudo Code: LI-AODV Routing Algorithm

==========

Input: RREQ from S

Output: Identifying and Eliminating Black hole attack

Begin
Step 1: S → RREQ to I_N
Step 2: S ← RREP from I_N
Step 3: Calculate SF
Step 4: Choose B_{path}
Step 5: Check B_{path} using R
Step 6: if (B_{path} is error)
  Generate A
  Choose Alter B_{path}
  Goto 5
 Else
  Transmit M, S → D
Step 7: End If
End

==========

Figure 4 Proposed LI-AODV Routing

The above Pseudo code describes our routing algorithm, here (S is a sender node, D is a Destination node, A is Alarm signal, I_N represents intermediate nodes, SF is the Stability factor, B_{path} denotes the best path and R is the proposed rules for identifying black hole attack). Initially sender nodes transmit RREQ to Intermediate nodes and receive RREP from Intermediate nodes. We calculate stability factor for all nodes and choose best path from source to destination. Using our proposed rules we identify the attackers in best path followed by generating alarm signal for eliminating malicious node in the network. Finally we choose alternate best path for transmitting packets after the verifying it.

4.3. Load Balancing:

Load balancing is defined as the capability to balance traffic across two WAN links without using complex routing protocols. This results in serving the user's request faster and all works are completed with same amount of time. In our proposed system, we introduce a new load balancing algorithm named Hybrid Round Robin with Highest Response Ratio Next (HRRHRRN). In this paper, we calculate Highest Response Ratio and Hybrid priority for every packet.
Response Ratio (RR) is calculated by,

$$RR = \frac{Waiting\ Time + Service\ Time}{Service\ Time} \quad (1)$$

Then Hybrid Priority (H_P) is calculated by,

$$H_P = 0.5 * E_P + 0.5 * RR \quad (2)$$

E_P is the External Priority which denotes the burst time of every packet and RR is obtained from equation (1).

Initially packets are allowed in the ready queue according to arrival time. The remaining burst time is calculated for identifying Dynamic Time Quantum. Here the process with higher H_P is selected and allowed to process queue and it is allowed to run in CPU with Dynamic Time Quantum. Then remaining burst time is calculated for other process and goes on, it ends when the ready queue gets empty. Figure 5 represents the flowchart of our proposed scheduling algorithm. Figure 5 shows pseudo code for our proposed algorithm.

The algorithm 5 describes about the proposed, initially user requests are allowed to fill the ready queue. A_i is the arrival time for packets,

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

B_i is the burst time for packets, U_i is the packets to be scheduled, PQ is the process queue, and RQ is the ready queue. If ready queue (RQ) is filled, Dynamic Time Quantum (DTQ) and Response Ration (RR) and Hybrid Priority ($H_{P(i)}$) are calculated for each and every process. Then the packet is selected according to the hybrid priority which is allowed in the process queue (PQ). Here TQ is the time quantum, UWT is the updating waiting time, RB is the remaining burst time and B is the burst time. The user requests are processed in the server according to the Dynamic Time Quantum. If DTQ expires, when the process is not completed then remaining burst time is calculated and their weighting time is updated otherwise the next packet in the ready queue is allowed to process in the server. The packets are processed in the server until the ready queue gets null.

==========

Pseudo code: Hybrid Round Robin with Highest Response Ratio Next (HRRHRRN)

==========

Inputs:

RQ, PQ, U_i → $\{U_1, U_2, U_3 \ldots U_n\}$,
A_i → $\{A_1, A_2, A_3 \ldots A_n\}$,
B_i → $\{B_1, B_2, B_3 \ldots B_n\}$

Initialization:

RQ=0, TQ=0, Awt=0

1. Begin
2. For i=1 to n
3. RBi =0, RRi=0, UWTi=0
4. RBi =Bi
5. Enter Ui into RQ
6. while (RQ !=Null)
7. DTQ= $\frac{(\sum_1^n RBi)}{n}$
8. $RR_i = \frac{UWTi+RBi}{RBi}$
9. HP(i) = 0.5 * EP + 0.5 * RRi
10. For i=1 to n
11. Sort Ui with HP(i)
12. Select Ui with higher HP(i)
13. Ui □ PQ
14. End
15. If (RBi <= DTQ)
16. Process Ui
17. Remove Ui from RQ
18. Else
19. RBi = Bi - TQ
20. Update RBi
21. End if
22. Update RQ
23. For i=1 to n
24. Update UWTi
25. Goto 4
26. End
27. while End
28. End

==========

Figure 5 Hybrid Round Robin with Highest Response Ratio Next (HRRHRRN)

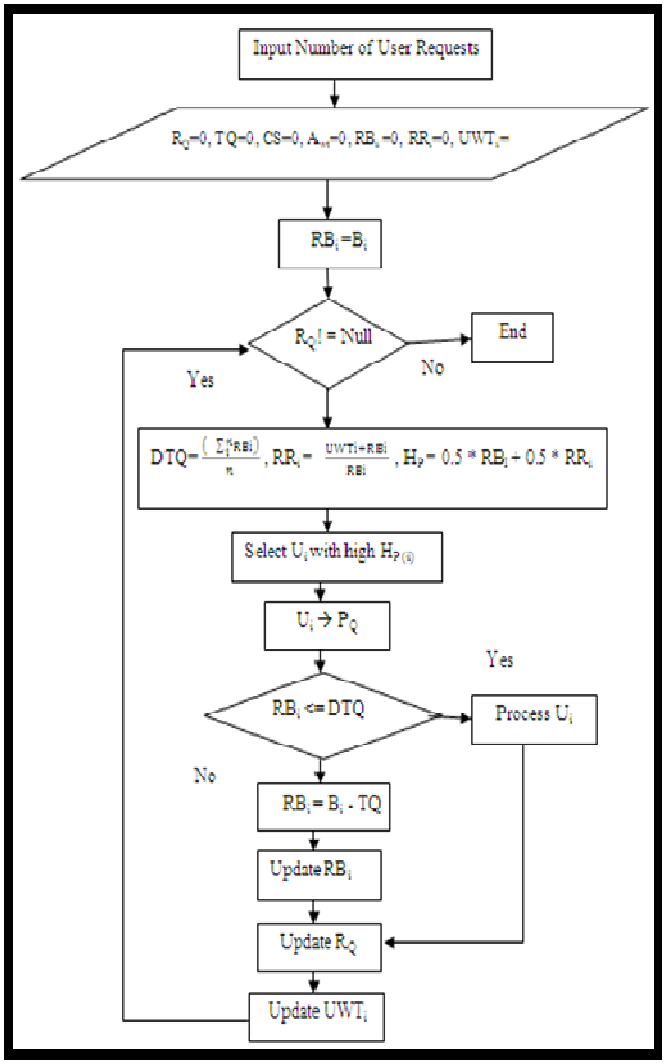

Figure 6 Flowchart for Hybrid Round Robin with Highest Response Ratio Next (HRRHRRN)

4.4. Security:

Network security is defined as a protection mechanism that protects file accessing, securing directories in a computer against hacking, misuse and unauthorized access in our system. In VANET, Black hole attack is a more vulnerable attack which degrades the performance of network. To improve the performance of VANET, we propose a new

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

secure algorithm named as "HMAC-SHA3-384". Our algorithm is a combination of SHA3-384 and a keyed-hash message authentication code (HMAC).

SHA-3 uses a sponge function (Keccak Family) [18] where a data is absorbed and their result is squeezed out. In the absorbing phase, the message blocks are XORed into subset of the state and they all are transformed whereas in squeeze phase output blocks are read from same subset that are alternated with state transformation. In this process, the size of the part read and written is denoted as read (r) and the part which is untouched by i/p or o/p is denoted as capacity (c). This (c) determines the security of SHA3-384. The SHA-3 hash function are defined from Keccak function [18] such as,

Keccak[c] (M, n) = Sponge [Keccak-p [1600, 24], pas10*1, 1600-c] (M, n).

Hash Function as,

SHA3-384(M) = Keccak [768] (M || 01, 384)

Here M is the message, n is the Output length and Capacity (c) is the double of digest length (768) i.e. c = 2n. The two bits [01] which are appended to message used for distinguish the messages for SHA-3 hash functions from messages. Finally it generates a secret key "K". After this we perform HMAC operation which is described as,

$$HMAC(M) = h((K \oplus opad) \| h((K \oplus ipad) \| M))$$

Finally Message Authentication Code (MAC) is generated for the corresponding message. Figure 8 describes flowchart of HMAC-SHA3-384 and Figure 7 represents the pseudo code for HMAC-SHA3-384.

==========

Pseudo code: HMAC-SHA3-384 Algorithm

==========

Input:

Message M, bits b= 768, C_1 = 00110110,
C_2 = 01011100

Step 1: Message M
Step 2: Compute K using SHA3-384
Step 3: Compute Hash (K)
Step 4: if length (K) < b
Pad 0 to K
K → K^+
Step 5: [$K^+ \oplus$ ipad with [C_1] by b/8 times] →S
Step 6: (Append M and S) → Z
Step 7: Hash (Z) → Z_1
Step 8: [$K^+ \oplus$ opad with [C_2] by b/8 times] →S_0
Step 9: Attach (Z_1 & S_0) → Z_2
Step 10: Hash (Z_2) → HMAC

==========

Figure 7 HMAC-SHA3-384 Algorithm

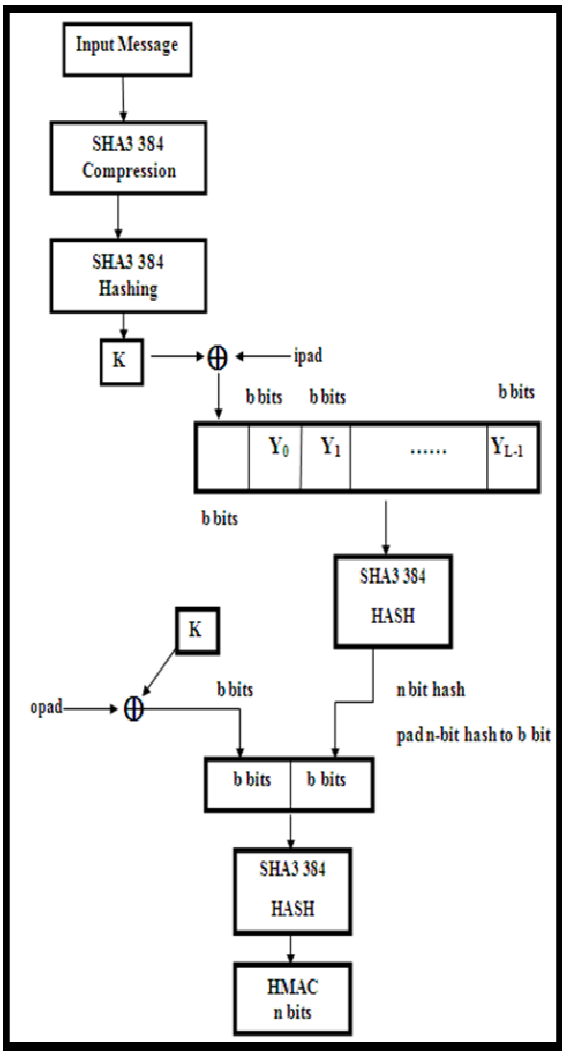

Figure 8 HMAC-SHA3-384 Algorithm

5. PERFORMANCE EVALUATION

In this section, we compare our proposed system with existing systems. In our proposed system we slightly modified the AODV protocol for reducing malicious behavior in the network. Here we consider parameters such as End-to-End Delay, Packet delivery ratio, Average Waiting time, Throughput, Loss of packet, Energy Consumption, Overhead. Here the existing systems such as AODV Protocol [5], ISDNAODV protocol [5] and Improved AODV Protocol [10] are used for removing Black hole attack in MANET, here Round Robin with Highest Response Ratio Next (RRHRRN) [19] is scheduling algorithm. We extend all these algorithms and mechanism in our proposed system that identifies Black hole attack in VANET. Existing systems working procedure are as follows:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- AODV Protocol:

  Ad-hoc on-demand Distance Vector protocol is an on-demand dynamic routing protocol; a source node has no valid route or direct route to destination node so, it initiates a route discovery process by broadcasting a RREQ to its neighbors for sending packets to destination. An intermediate node receives the RREQ packet that has a specific route to destination or it is just the destination then it returns RREP packet to the source node. This routing protocol minimizes the usage of routing table.
- ISDNAODV Protocol:

  This Protocol is an improvement of AODV Protocol which identifies the malicious node or destructive nodes in the network. This introduces the new rules for identifying the destructive nodes during routing process based on behavior of nodes. This improves better performance in terms of percentage for identifying black hole attack in the network.
- Improved AODV Protocol:

  This protocol is similar to the normal AODV protocol which has additional constraints on route discovery process. In general AODV process remaining energy of every node is not considered. During the routing process nodes energy gets decreases that results in packet loss. They use stability factor and Time to live (TTL) constraint for reducing the packet loss and improve the lifetime of network.
- Round Robin with Highest Response Ratio Next (RRHRRN):

  This algorithm uses dynamic time quantum (DTQ) by using the mean of burst time of process and it fills Ready Queue based on arrival time of requests. Here the Response Ratio (equation 1) is calculated for every request in the queue. Then request with higher response ratio is selected that is allowed to run in CPU. After finishing waiting time for every request is updated in the ready queue.

5.1. Simulation Results:

We implement our experiment on OMNeT++ simulation framework. This simulation tool helps us to perform proposed system with new algorithms. OMNeT++ simulation was conducted with some considering parameters which are shown in table 1.

Table 1: Simulation Parameters

Parameters	Values/Ranges
Number of nodes	50
Speed	15 m/s, 20 m/s, 25 m/s
RSU	4
Area	2000*2000
Transmitted Power	2mW
Beacon Interval	1 second
Lane	Two Lane
Sensitivity	-85 dBm

To conduct our experiments 50 nodes are used. Here all nodes are mobile in nature and it moves in a speed of 20 m/s, 25 m/s and 30 m/s. In our simulation, we include a pre-simulation step with SUMO setup. This SUMO setup includes extracting road map, creating road network and converting into routes and traffic flow. This SUMO setup can also create obstacles in road map. Here we use C++ coding for the components. We consider our simulation area is about 2000 X 2000 then we use 4 RSU (Road Side Units) and 5 attackers (Black hole Attack) in the VANET.

5.2. Performance Metrics:

In our proposed system we consider some of the parameters that prove our results efficiently on OMNeT++ Simulation that between existing system and proposed system. Here are some of the metrics are

- End-to-End Delay
- Average Waiting Time
- Packet delivery ratio
- Throughput
- Packet loss
- Overhead
- Energy

These parameters are explained in sub section and plotted with its graphical representation in section 5.3.

5.2.1. End-to-end delay:

End-to-End Delay plays a major role in routing process that specifies average time taken for a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

packet for transmission across a network from source to destination. The delay occurs during the route discovery process and it is measured in second.

The End-to-End Delay is calculated by,

$$\text{End-to-End Delay} = \frac{\Sigma(Arrive\ time - Send\ time)}{\Sigma(Number\ of\ Connections)}$$

5.2.2. Average waiting time:

Waiting time is defined as that amount of time a request is sitting ideal before it is processed. Average waiting time is simply averages the wait times (measured in seconds) of all requests.

5.2.3. Packet delivery ratio:

Packet Delivery Ratio (PDR) is defined as the ratio of number of delivered packets from source node to destination node. This describes the level of delivered data to destination.

$$\text{Packet Delivery Ratio} = \frac{\Sigma(Number\ of\ packet\ receive)}{\Sigma(Number\ of\ packet\ send)}$$

5.2.4. Throughput:

Throughput is defined as the rate at which processing of something. Throughput in network is a measure of how many number of units of information is processed by a system at a given time i.e. bits per second (bps). It is degraded by various factors such as behavior of end-user, physical medium and available processing of power.

5.2.5. Packet loss:

Packet Loss is defined as the discarding of packets in a network whenever a network devices like router gets overloaded, the incoming packets after overloading cannot be accepted at a given moment. It is calculated by difference between the total numbers of packet send and number of packet received.

Packet loss = Number of packet send - Number of packet received.

5.2.6. Overhead:

Overhead in the network is defined as that delivering a high fraction of messages to their destination.

5.2.7. Energy:

In our proposed system, we use stability factor that finds the remaining energy of node. Here if the energy of node goes down then the link of nodes connection breaks which results in packet loss and if the energy consumption (measured in joules) is low then our network improves the lifetime.

5.3. Comparative Analysis:

We conduct some experiments of our proposed system and compare to its existing system when concentrating variance of each parameter.

5.3.1. Average waiting time:

Our proposed scheduling algorithm named HRRHRRN is compared with previous RRHRRN scheduling algorithm [19] that gives best results in our experimental procedure. Figure 9 describes the graphical representation in terms of order of burst time in x-axis and average waiting time in y-axis. Order of burst time is described as decreasing, Increasing and random.

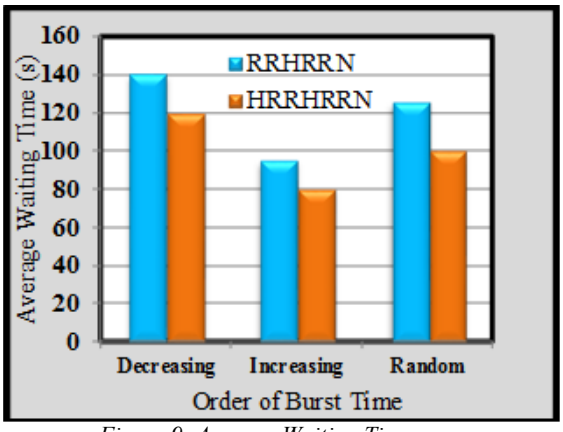

Figure 9 Average Waiting Time

5.3.2. Energy consumption:

Our proposed routing algorithm consumes less energy. Here initially we select route with higher energy for packet transmission. Figure 10 describes the comparison of proposed routing process with existing AODV routing. In graphical representation x-axis describes the speed of nodes and y-axis describes the energy consumed in joules.

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

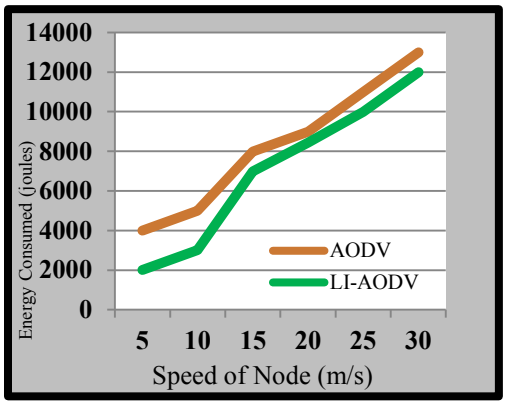

Figure 10 Energy Consumption

5.3.3. End-to-end delay:

Figure 11 displays the graphical representation of End-to-End delay performance in our proposed routing algorithm. In the graph x-axis represents the speed of nodes in terms of m/s and y-axis represents the end-to-end delay in seconds. Our proposed routing algorithm is compared with normal AODV routing, previous AODV routing that gives better performance.

Figure 11 Performance of End-to-End Delay

5.3.4. Throughput:

Figure 12 describes the graphical representation of Throughput performance in our proposed system. In the graph x-axis represents the speed of nodes in terms of m/s and y-axis represents the number of bits in MBPS. Our proposed routing algorithm is compared with normal AODV routing, previous AODV routing that achieves best results in network.

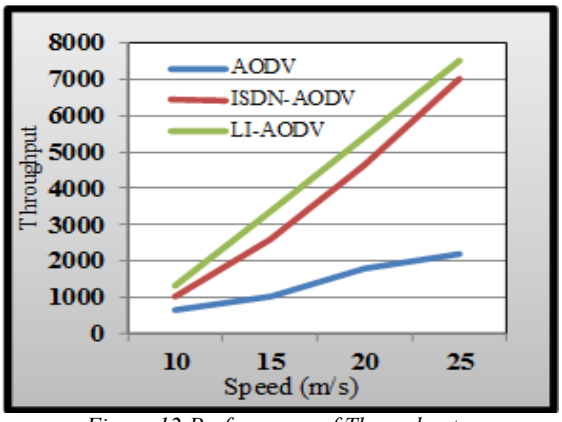

Figure 12 Performance of Throughput

5.3.5. Packet delivery ratio:

Figure 13 displays the graphical representation of Packet Delivery Ratio (PDR) performance in our proposed routing algorithm. In the graph x-axis represents the speed of nodes in terms of m/s and y-axis represents the percentage of PDR. To achieve best performance in PDR, our proposed routing algorithm is compared with normal AODV routing, previous AODV routing.

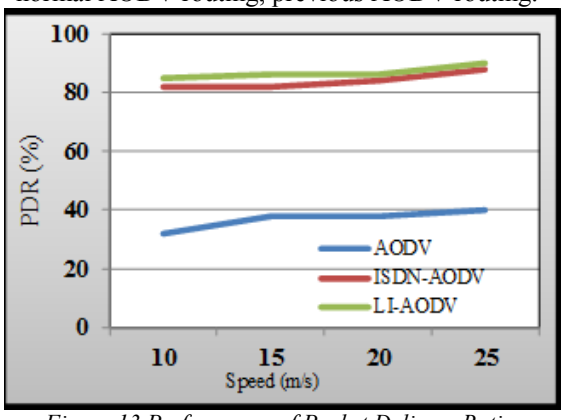

Figure 13 Performance of Packet Delivery Ratio

5.3.6. Packet loss:

Figure 14 displays the graphical representation of Packet Loss performance in our proposed routing algorithm. In the graph x-axis represents the speed of nodes in terms of m/s and y-axis represents the percentage in Packet loss. To know the performance of routing in terms of Packet loss, our proposed routing algorithm is compared with normal AODV routing, previous AODV routing that provides best results.

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

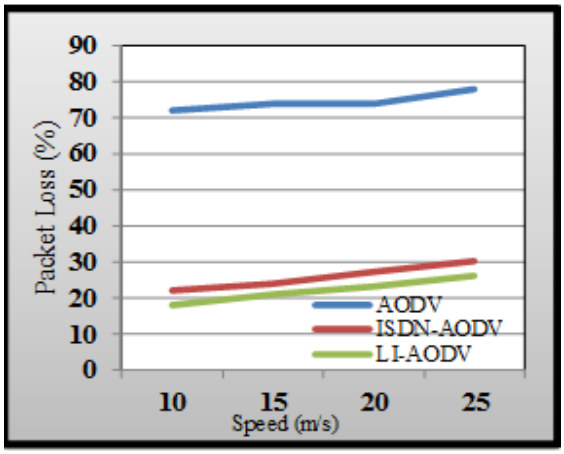

Figure 14: *Performance of Packet loss*

5.3.7. Detection rate:

Figure 15 displays the graphical representation of detection rate of malicious nodes in the network. Detection rate is defined as the percentage of malicious node detected and its classification. Here the detection rate is calculated as,

$$\text{Detection Rate} = \frac{\textit{Number of Malicious Nodes Detected Correctly}}{\textit{Total Number of Malicious Nodes}}$$

To know the performance of in terms of detection rate of Black hole attackers, our proposed routing algorithm is compared with normal AODV routing, previous AODV routing that provides best results.

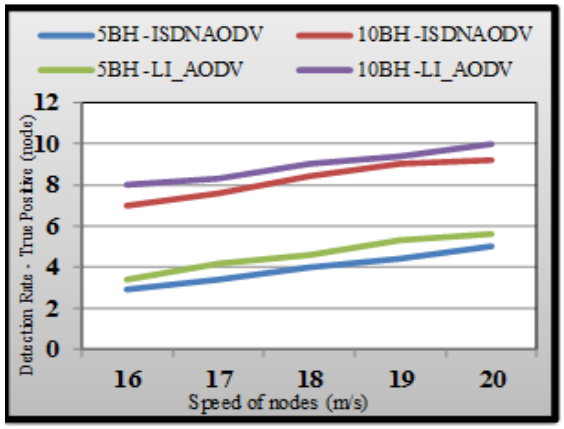

Figure 15 Performance of Detection rate

5.3.8. Misdetection rate:

Figure 16 displays the graphical representation of Misdetection rate of honest nodes in the network. Misdetection rate is defined as the percentage of honest nodes incorrectly denoted and classified as malicious node. Here Specificity is denoted as number of honest nodes which are correctly identified. Here the misdetection rate is calculated as,

$$\text{Specificity} = \frac{\textit{Number of Honest Nodes identified Correctly}}{\textit{Total Number of Honest Nodes}}$$

Misdetection rate = 1 - Specificity

To know the performance of in terms of misdetection rate, our proposed routing algorithm is compared with normal AODV routing, previous AODV routing that provides best results.

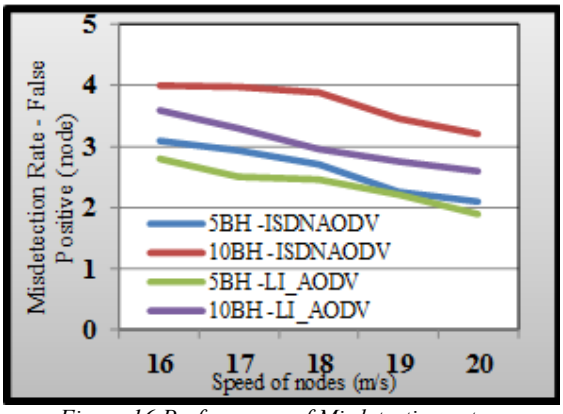

Figure 16 Performance of Misdetection rate

5.4. Performance comparison

In this subsection, we compare the performance of LI-AODV with ISDNAODV [5] in terms of detection rate-true positive, misdetection rate-false positive rates.

According to Figure 15 and Figure 16, we show that LI-AODV exhibits a high detection rate-true positive (over 98%) and generates a low false positive rate (lower 1,7 %) even when the speed of vehicles increase. In addition, LI-AODV outperforms ISDNAODV in terms of packet delivery ratio (over 92 %). Furthermore, comparing with AODV and ISDNAODV, our LI-AODV decrease the end-to-end delay and the packet loss ratio.

6. CONCLUSION

VANET is an infrastructureless network which is also a MANET with only difference is that movement of nodes in VANET is strictly warned. Black hole attack is a most vulnerable attack which degrades the VANET network. In order to eliminate attackers in the network, we propose a novel routing algorithm named *LI-AODV (Lifetime Improving Ad-hoc On-demand Distance Vector Routing),* the proposed work increased the detection rate of black hole attack and decrease the false

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

positive rate in urban VANET comparing with the previous works. To reduce the overload in the routing process we introduce a novel scheduling algorithm named *Hybrid Round Robin with Highest Response Ratio Next (HRRHRRN)*. Our proposed routing algorithm results in best performance in terms of End-to-End delay, throughput, packet loss, energy, overhead, packet delivery ratio and average waiting time. To protect our proposed system efficiently we introduce a secure algorithm called *HMAC-SHA3-384*. This algorithm provides good security in the network.

In future work, improving our LI-AODV to detect and remove black hole attach in highway VANET, second we prevent our network by improving our LI-AODV routing process for identifying other vulnerable attacks such as Wormhole attack, Sybil attack.

REFERENCES:

[1]. Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications 2013, 3(3): 29-38, DOI: 10.5923/j.jwnc.20130303.02.

[2]. Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastavam, " An Overview of AODV Routing Protocol", International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-728-732 ISSN: 2249-6645 www.ijmer.com.

[3]. Megha Nema, Prof. Shalini Stalin, Prof. Vijay Lokhande, "Analysis of Attacks and Challenges in VANET", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014) 831

[4]. AJAY RAWAT, SANTOSH SHARMA, RAMA SUSHIL, "VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS", Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-301-304 Available online at http://www.bioinfo.in/contents.php?id=55.

[5]. Sina Shahabi, Mahdieh Ghazvini, Mehdi Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack", Springer Science+Business Media New York 2015

[6]. Mehdi Medadian, M.H. Yektaie, A.M Rahmani, "Combat with Black Hole Attack in AODV routing protocol in MANET", 978-1-4244-4570-7/09/$25.00 ©2009 IEEE.

[7]. Kunal V. Patil1, M. R. Dhage, "The Enhanced Optimized Routing Protocol for Vehicular Ad hoc Network", international Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013, Copyright to IJARCCE www.ijarcce.com, 2013.

[8]. Mukul Sharma, "An Advanced Implementation in AODV Routing Protocol in Mobile Ad Hoc Networks (MANET)".

[9]. Ketan S. Chavda, Ashish V.Nimaval, "REMOVAL OF BLACK HOLE ATTACK IN AODV ROUTING PROTOCOL OF MANET", 4th ICCCNT – 2013, July 4 -6, 2013, Tiruchengode, India.

[10]. Mrs. Sangeeta Kurundkar , Apoorva Maidamwar, "AN IMPROVED AODV ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORKS", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013 , Copyright to IJAREEIE www.ijareeie.com 3003

[11]. Fei Wang, Yongjun Xu, Hanwen Zhang, Yujun Zhang and Liehuang Zhu, "2FLIP: A Two-Factor Lightweight Privacy Preserving Authentication Scheme for VANET", DOI 10.1109/TVT.2015.2402166, IEEE Transactions on Vehicular Technology.

[12]. Raj Bala, C. Rama Krishna, "Scenario Based Performance Analysis of AODV and GPSR Routing Protocols in a VANET", 2015 IEEE International Conference on Computational Intelligence & Communication Technology.

[13]. Peppino Fazio, Floriano De Rango, Cesare Sottile, Pietro Manzoni, Carlos Calafate, "A Distance Vector Routing Protocol for VANET Environment with Dynamic Frequency Assignment", 978-1-61284-254-7/11/$26.00 ©2011 IEEE.

[14]. Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, " Security Measures for Black Hole Attack in MANET: An Approach".

[15]. Miss. P.A. Kamble Dr. M.M. Kshirsagar, "IMPROVEMENT OVER AODV ROUTING PROTOCOL IN VANET", Volume 4, Issue 4, July-August (2013), pp. 315-320

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[16]. Avinash Kumar, C.H Pushpalatha, "Design of SHA-3 Algorithm using Compression Box (3200 bit) for Digital Signature Applications", International Journal of Emerging Engineering Research and Technology Volume 3, Issue 12, December 2015, PP 146-153 ISSN 2349-4395 (Print) & ISSN 2349-4409

[17]. Hengheng Xie, Azzedine Boukerche, Antonio A.F. Loureiro, "MERVS: A Novel Multi-channel Error Recovery Video Streaming Protocol for Vehicle Ad-hoc Networks", DOI 10.1109/TVT.2015.2397862, IEEE Transactions on Vehicular Technology

[18]. "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", FIPS 202.

[19]. H.S. Behera, Brajendra Kumar Swain, Anmol Kumar Parida, Gangadhar Sahu, "A New Proposed Round Robin with Highest Response Ratio Next (RRHRRN) Scheduling Algorithm for Soft Real Time Systems", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-3, February 2012.