MITIGATING THE EFFECT OF RUSHING ATTACK ON AODV ROUTING PROTOCOL IN MOBILE AD HOC NETWORK

Amit Kumar Bairwa
Manipal University Jaipur
37 PUBLICATIONS **164** CITATIONS

MITIGATING THE EFFECT OF RUSHING ATTACK ON AODV ROUTING PROTOCOL IN MOBILE AD HOC NETWORK

[1]PRATIBHA MISHRA, [2]DR. SACHIN SHARMA, [3]AMIT KUMAR BAIRWA

[1]Research Scholar, [2]Professor, [3]Assistant Professor
[123]Department of Computer Science and Engineering
[123]Rajasthan Institute of Engineering and Technology, Jaipur, India

Abstract: A mobile ad hoc network or MANET is a collection of mobile nodes which establish a network spontaneously and communicate over a wireless channel without any pre-existing infrastructure and no or minimal central administration. Mobile ad hoc network is a wireless network where nodes are moved dynamically in the network. Since Researcher worker has an interest in research of mobile ad hoc network from last several years. In MANET for data transmission, we require of protocol that adopt topology changes. There are three kinds of protocol Reactive, proactive and third is hybrid protocol. AODV is a Reactive protocol or on-demand protocol in which route is discovered on the demand of basis of the source node. Security is the main issue in MANET due to less infrastructure, no central administration, self-configure, and self-arrangement capability. There are various security threats like Black-hole attack, Sybil attack, Gray-hole attack, Worm-hole attack and rushing attack etc. That is used to packet dropping, capturing and degrading network performance. The rushing attack is the most powerful attack. The rushing attack is launched against the on-demand routing protocol. On-demand routing protocol use duplicates suppression mechanism. Rushing attack uses this mechanism and transmits a packet with a high transmission range to the destination node. A Method is proposed to prevent the rushing attack in MANET. The Rushing attack is analyzed with three different scenarios with regard to the performance parameter of Throughput, PDR, Packet Loss, Packet Drop, and End-To-End Delay. In this proposed work, we use a secure technique which secures the network and increase the performance of the network. In this work, we do not use any special hardware. The proposed method is based on the decisional threshold. This technique is optimum to provide a securing network with an increase in the performance of the network.

***Index Terms* – MANET, Routing, Rushing Attack, QoS.**

I. Introduction

A wireless ad-hoc network consists of a collection of mobile nodes in which nodes are communicating with each other without help from a fixed infrastructure. Each node can act as both routers as they forward data packet to other node in the network or host. A wireless ad hoc network is a decentralized type of wireless network they are self-controlled, and self-configured, and infrastructure-less network. The absence of central coordinator and bas station makes operations in MANETs more complex than their counterparts in other types of wireless networks such as cellular networks or wireless local area networks. There are many MANET application is on practice on today’s world. As the result, MANET can be established anywhere the node have connectivity with other nodes can join and leave the network at any point of time [1]. Communication in MANET is done through inter-nodes with each node serves as a router to transmit data. A routing protocol is needed to communicate that serves the route from source to destination. There are many proposed routing protocols; on-demand routing is most preferable among all as its overhead is very low [4]. The high mobility in the MANET network makes it very vulnerable to attack. Attacks can also steal or discard transmitted data source so that data does not received by the destination. Attacks in MANET generally occur in the routing system [6]. Rushing attack is Common in MANET. Some on-demand routing protocol uses duplicate suppression mechanism. Rushing Attack uses this duplicate suppression mechanism via immediately transfer route discovery packet in the order to get access to the transmitting group [7].

1.1. Application of MANET

Mobile ad hoc network has application in many fields which are given below:

- Bluetooth
- Emergency Situation
- Military Environment
- Civilian environments
- Entertainment
- Education
- Industry sector
- Sensor Networking

1.2. Characteristics of MANET

- **Distributed operation:** There is absence of central administrator so the control of the network is distributed among the mobile ad hoc network.
- **Multi-hop routing:** When Source node sends a data packet to the destination node, the packet forwarded through the multiple intermediate nodes.
- **Autonomous terminal:** Each node can act as both routers as they forward data packet to other node in the network or host
- **Dynamic Topology:** In mobile ad hoc network, each node is free to move randomly in any direction at any time. Each node is free to change its link to other nodes frequently.
- **Light-weight terminals:** In mobile ad hoc network, each device is mobile and it has low power storage, small memory, less CPU capability.
- **Scalability:** Scalability is a main issue in mobile ad hoc network because the mobile node has limited power and memory in mobile ad hoc network.

1.3 Challenges in MANET

- **Limited Bandwidth:** Mobile ad hoc network has limited bandwidth in compared to wired network.
- **Security threat:** due to wireless nature of mobile ad hoc network introduce new security challenges.
- **Battery constraints:** battery power is big challenge in mobile ad hoc network because without the battery power MANET is not possible.
- **High Routing:** mobile ad hoc network has dynamic topology so some nodes can change their position in the network and affect the routing table.
- **Topology maintenance:** MANET has dynamic topology. So there is a major challenge to updating information of dynamic link among nodes in mobile ad hoc network.
- **Packet losses due to errors in transmission:** In mobile ad hoc network there is highly a packet loss due to some factor such as hidden terminal that is result of collision.
- **Routing Overhead:** In mobile ad hoc network, nodes are free to change their location at any time therefore it has dynamic topology. So it leads to unnecessary routing overhead.

1.4 Routing Protocol in MANET

In ad hoc network each nodes act as router for forwarding data packet from source to destination node or an end-device. Therefore, in mobile ad hoc network we require of routing protocols for delivered messages reliably and timely manner from source node to destination node. We can establish a correct and efficient route between a pair of nodes using routing protocol [4]. These routing protocols are dividing into three categories: Proactive, Reactive and hybrid routing protocol. DSDV, OLSR and WRP are the proactive routing protocol while AODV, DSR and TORA are reactive protocol and ZRP is the example of hybrid routing protocol. It is combinations of characteristics of proactive and reactive routing protocols.

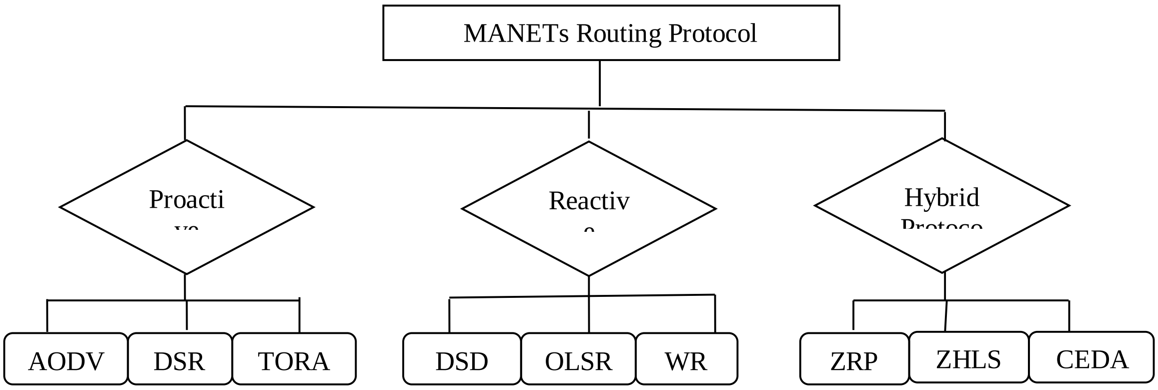

Fig. 1 classification of routing protocol

Table 1 Comparison of routing protocol

Features	Reactive	Proactive	Hybrid
Routing Structure	Mostly Flat	Both Flat & Hierarchical	Hierarchical
Route Acquisition	On demand	Table driven	Combination of both
Routing Overhead	Low	High	Medium
Latency	High due to flooding	Low due to routing tables	Inside zone Low outside similar to reactive protocols
Scalability	Not suitable for large networks	Low	Designed for large networks
Routing information	Available when required	Always available	Combination of both
Periodic Updates	Not needed	Yes whenever the topology of the network changes	Yes
Mobility	Route Maintenance	Periodic updates	Combination of both
Storage Requirement	Low	High	Medium
Bandwidth Requirement	Low	High	Medium
Power Requirement	Low	High	Medium

1.5 AODV Routing Protocol

It is reactive routing protocol in which routes are created when needed so called “on demand”. Dynamic Routing Protocol include source route in packet header which is major drawback of DSR protocol. Larger packet header can degrade the performance of network. DSR can’t use for lager network because if the size of network is larger than the size of header is also become larger and performance of network can be degrade. It is basically an improvement of DSR routing protocol. It is combination of DSR and DSDV routing protocol. AODV routing protocol is improvement of DSR routing protocol. It is combination of DSR and DSDV routing protocol.

Control Packet: In mobile ad hoc network, AODV protocol contains some message which handles the process of Route Discovery and Route Maintenance. AODV contains some Control Packet are Route Request Message, Route Reply Message and Route Error Massage.

1.5.1 ***Route Discovery:*** when a source node S wants to interact with the destination node D and source node S check the routing table if route entry is not exist in the routing table for the destination node D. then Discovery process is begin by Source node S broadcast RREQ packet to its neighbour. Now all nodes of the network checks the Broadcast Id and Source IP Address over accepted RREQ messages. If source address and Broadcast Id of new received RREQ packet is match from already received packet, new RREQ packet is discarded. When a new RREQ packet is broadcast every time, broadcast id is also increased. RREQ message contain last Destination Sequence Number. All intermediate nodes of network hold the route entry in routing table for desired destination node. It matches Destination sequence number in the routing table with that is in the RREQ. If the Destination sequence number in routing table is less than compare to that is in RREQ, it rebroadcast to its neighbour. Otherwise destination node send unicast RREP back to the source.

1.5.2 ***Route Maintenance:*** In the process of Route Maintenance, it use Route Error control packet. The all nodes of network track their own neighbourhood. When route become invalid or route link is broken, generate error message for tell another node which uses this route.

1.6 Threats in MANET

1.6.1 Types of Attacks in MANET:

On the basis of nature, Attacks can be mainly categorized into two types namely: passive & Active Attack.

- Passive attack:
  - ✓ In the passive attack intruder can't modify the content of data packet which is transmitted.
  - ✓ In this attack, an intruder can only read the content of data among the originator and recipient.
- Active attack:
  - ✓ In the active attack intruder can modify the content of data packet which is transmitted.

Active attack can further be forked into external attacks and internal attacks.

- External attack: In this attack, attacker node is not part of the network.
- Internal attack: Malicious nodes which are actually part of the network and which have all Authorization so it is difficult to find it.

Table 2 *Attack according to various layers in MANET*

MANET security Layer	Attacks
Application Layer	Malicious code, Repudiation
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing etc.
Data Link Layer	Traffic analysis and monitoring.
Physical Layer	Traffic Jamming, Eavesdropping

1.3 Rushing Attack

Rushing Attack is a type of denial of service Attack, it is launched opposite to the on-demand routing protocols. Rushing Attack is also called as “sudden forward motion attack”.

Some on-demand routing protocol uses duplicate suppression mechanism. Rushing Attack uses this duplicate suppression mechanism via immediately transfer route discovery packet in the order to get access to the transmitting group.

When a Source node S want to communicate to destination node D. therefore Source node S broadcast RREQ to its neighbour for discover the route from source node S to destination node D in wireless network, if attacker present in the route then he will receive the RREQ packet and transmit to its neighbour via high transmission speed as compared to other node that are present in the wireless network. Packet transmitted via the intruder will first arrive to the destination node due to high transmission speed. Destination node will receive that RREQ and reject other RREQ packet that is arriving after. Recipient discovered that route as long as a legitimate route and use as further communication. Thus intruder has been successfully obtained access in the communication between source node and destination node.

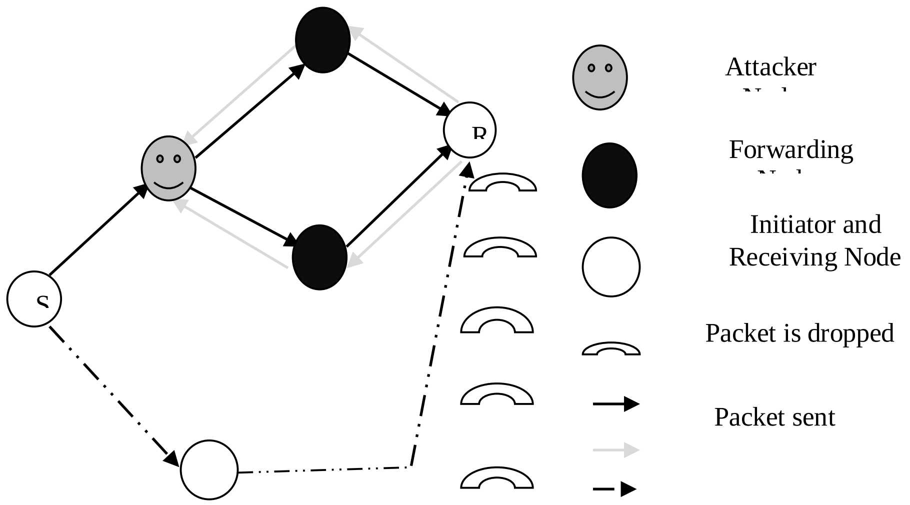

Fig. 2 Rushing Attack

II. Literature Survey

In this chapter, the research work performed by the different researchers, is discussed. A large amount of work is performed to improve the quality of security parameters in MANET Different researchers given the different algorithms, which are discussed below.

Table 3 Literature Survey summary

Sr. No.	Title of paper	Authors	Year	Technique Used
1	Security agents for detecting and avoiding cooperative black hole attacks in MANET	V. G. Mohite and L. Ragha	2015	Cooperative Cluster Agents
2	A New Technique to Prevent MANET against Rushing Attack	Satyam Shrivastava, DharmendraMangal	2014	use path value and Threshold value
3	Performance of AOMDV routing protocol under rushing and flooding attacks in MANET	Sukiswo and M. R. Rifquddin	2015.	AOMDV
4	Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET	H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra	2016	Advanced AODV approach
5	Analysis and prevention of wormhole attack using trust and reputation management scheme in MANET	S. Parbin and L. Mahor	2016	trust and reputation management scheme in MANET
6	A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs	A. Chaudhary, A. Kumar and V. N. Tiwari	2014	Fuzzy Logic

7	Detecting and avoiding of wormhole attack and collaborative black hole attack on MANET using trusted AODV routing algorithm	N. Arya, U. Singh and S. Singh	2015	trusted AODV routing algorithm
8	Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks	A. K. Jain and V. Tokekar	2016	Ignoring first RREP
9	Wormhole Attack Detection and Prevention in MANET Using Bait Scheme	HarjinderKaur, Sukhjit Singh	2017	Bait Scheme
10	Rushing Attack and its Prevention Techniques	Satyam Shrivastava	2013	Secure neighbour detection and secure route discovery procedure

III. Proposed Method

3.1 Threshold Computation

In this paper we propose a new technique to mitigate the effect of rushing attack on AODV routing protocol under in mobile ad hoc network and to improve the performance of the mobile ad hoc network. The threshold value are calculated for discover an optimum path between sender and receiver node. Buffer length, Propagation Delay and round trip time are perceived for producing threshold value.

3.1.1 Round Trip Time

1. Sender node S broadcast RREQ message and record time t_1
2. Source node S received response RREP message and record that time t_{2_i} for each route reply.
3. Now Source node S computed the RTT using above two values as

$$t_{2\_i} + t_1 = t_{3\_i} \qquad (3.1)$$

4. *Computed the threshold RTT in the form of:*

$$\frac{t_{3\_i}}{hop\_count_i} = t_{s\_i} \qquad (3.2)$$

5. Using step 4, calculate t_{s_i} for i number of route

$$\frac{t_{3\_1}}{hop\_count} = t_{s\_1}, \frac{t_{3\_2}}{hop\_count} = t_{s\_2}, \frac{t_{3\_3}}{hop\_count} = t_{s\_3} \qquad (3.3)$$

6. Now calculate avg. threshold RTT as t_{th}

$$t_{th} = \frac{t_{s\_1} + t_{s\_2} + t_{s\_3}}{3} \qquad (3.4)$$

3.1.1 Buffer Length

Node of the network has the Buffer length. Buffer length indicates the load on the node of the network. If the load is less on the node means path is able for communication and this node is secure. The threshold value of the buffer is calculated as:

$$\mathrm{Bt} = \sum_{i=1}^{n} \frac{\text{Length of buffer}}{\mathrm{N}} \qquad (3.5)$$

3.1.2 Propagation Delay:

Propagation Delay = $(t_d - t_s) / 2H$

Where

Propagation Initial Time → t_s

Receiving Reply Time → t_d

H is number of hop count between source node and destination node

Now compute the threshold value of Propagation Delay:

$$Tt = \sum_{i=0}^{n} \frac{\text{Propagation Delay}}{\text{N}} \tag{3.6}$$

N → No. of nodes

Algorithm:

```
Begin
{
S_N = Sender Node
t1 = Record time of RREQ by S_N
t2_i = Record time of Response packet for each route reply
$t_{s\_i}$ = threshold Round Trip Time
$t_{th}$ = avg. Round Trip Time
Bt = threshold value for buffer length
Tt= threshold value of propagation delay
}
S_N broadcast RREQ and note time $t_1$
S_N received response RREP message and note time $t_{2\_i}$
Now node S computed the Round Trip Time using equation 4.1
computed the threshold RTT using equation 4.2
using equation 4.3, calculate $t_{s\_i}$ for i number of route
Now calculate $t_{th}$ from equation 4.4
Using equation 4.5 calculate Bt of the node
Calculate Tt from equation 4.6
if (node (buffer_length) > Bt && node (propagation_delay) > Tt && $t_{s\_1} < t_{th}$) than
    Node as malicious;
    Return;
end if
else if (node (buffer_length) < Bt && node (propagation_delay)>Tt && $t_{s\_1} < t_{th}$) than
    Node as malicious;
    Return;
end if
else if (node (buffer_length) < Bt && node (propagation_delay) < Tt && $t_{s\_1} > t_{th}$) than
    Node is legitimate but on high load;
    Return;
end if
else if (node (buffer_length) > Bt && node (propagation_delay) < Tt && $t_{s\_1} > t_{th}$) than
    Node is legitimate and efficient and select node for routing;
```

```
23: end if
```

3.4 Detection and Prevention Technique of Rushing Attack

In the proposed method, we discover the multiple routes from origin node to target node. In this method, first of all the source node check the routing table if route entry is exist it gives the routing information else Source node broadcast RREQ packet to its neighbour. Whenever target node accept RREQ packet it send response (RREP) to its origin node along the identical path. Starting node broadcast RREQ message and note time $t_{1.}$ Whenever target node accept RREQ message and response RREP message back to Origin node than Origin node record that time $t_{2.}$ If Origin node accepted more than one Response Packet its means that it has multiple paths to target node and record the uniform time t_{2_i} of each RREP packet. Using above two values, we calculate the Round Trip Time t_{3_i} of each path and divide by individual hop_count. Now we will calculate Average Round Trip Time of all paths using the variable $t_{s\_i.}$ The value of Threshold Round Trip Time t_{th} has obtained. Now we compare the value of Threshold Round Trip Time and total round trip time. Than we compute the threshold value of buffer length and Average End-to-End Delay.

Node of the network has Buffer length. Buffer length indicates the load on the node of the network. If the load is less on the node means path is able for communication and this node is secure. End-to-End Delay represent time require to transfer packet from source node to target node. Now compare the threshold value of buffer length, EED and RTT. If buffer length is >Bt, propagation delay >Tt and $T_{s_i}<T_{th}$Than node as malicious and discard this route. If buffer length is <Bt, propagation delay >Tt and $T_{s\_i}<T_{th}$ Than node as malicious and discard this route. If buffer length is >Bt, propagation delay <Tt and $T_{s\_i}>T_{th}$ Than node as Legitimate but on the high load. So route is not efficient. If buffer length is <Bt, propagation delay >Tt and $T_{s\_i}>T_{th}$ Than node is legitimate and not on high load than select route for routing. Thus the invalid route is discarded from the network and improves the network performance and has less overhead and end-to-end delay.

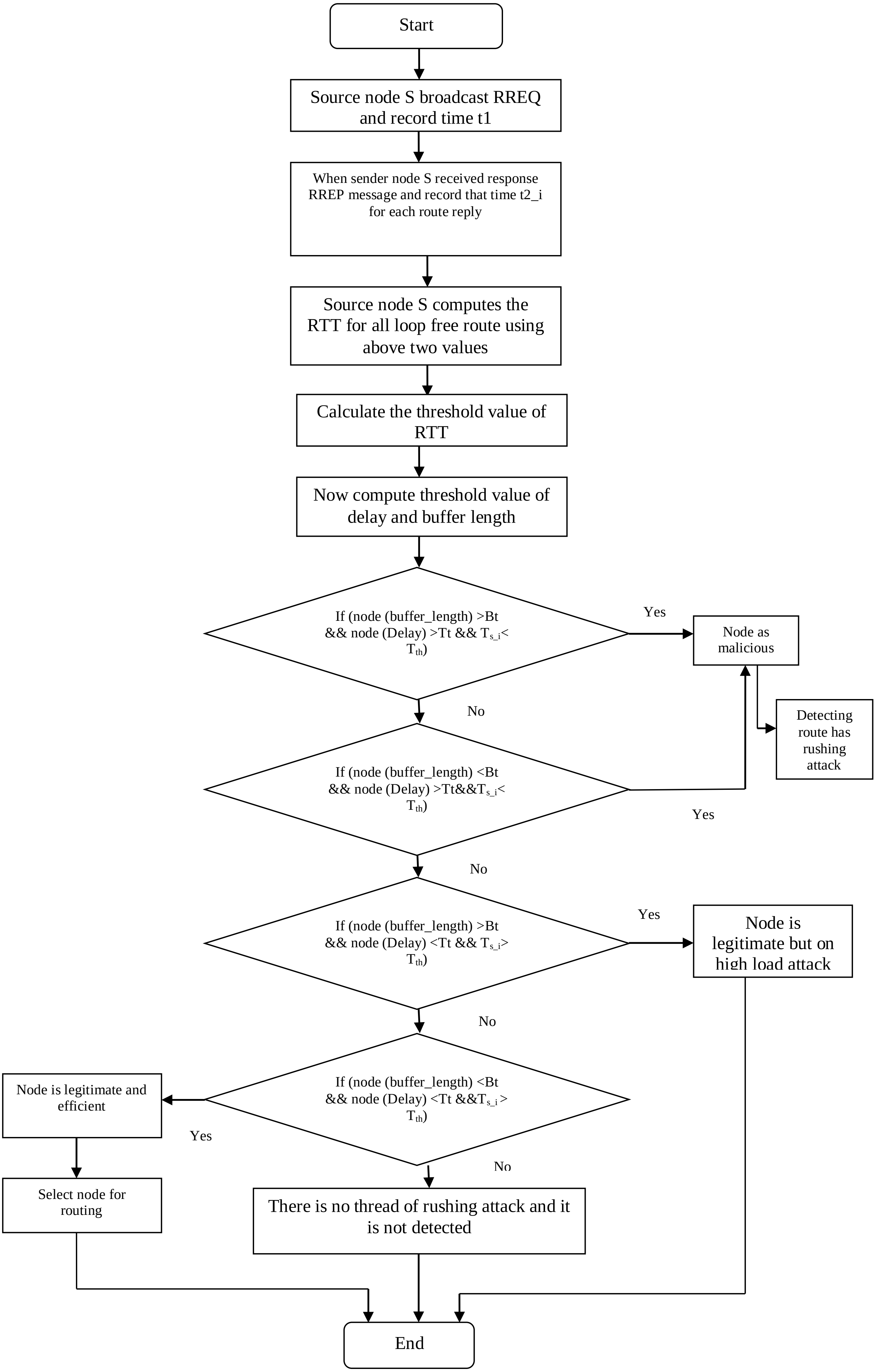
Start
Source node S broadcast RREQ and record time t1
When sender node S received response RREP message and record that time t2_i for each route reply
Source node S computes the RTT for all loop free route using above two values
Calculate the threshold value of RTT
Now compute threshold value of delay and buffer length
If (node (buffer_length) >Bt && node (Delay) >Tt && T_{s_i}< T_{th})
Yes
Node as malicious
Detecting route has rushing attack
No
If (node (buffer_length) <Bt && node (Delay) >Tt&&T_{s_i}< T_{th})
Yes
No
If (node (buffer_length) >Bt && node (Delay) <Tt && T_{s_i}> T_{th})
Yes
Node is legitimate but on high load attack
No
If (node (buffer_length) <Bt && node (Delay) <Tt &&T_{s_i}> T_{th})
Yes
Node is legitimate and efficient
Select node for routing
No
There is no thread of rushing attack and it is not detected
End

Figure 3.1 Flow chart of proposed algorithm

IV. RESULT AND ANALYSIS

Simulations have been carried out in order to evaluate routing protocol. We focused our attention on the evaluation of network performance in terms of Loss Packet, Drop Packet, Packet Delivery Ratio and All Delay, Average End to End Delay and Throughput of a mobile ad hoc network where a number of nodes are varying.

4.1 Simulation setup

TABLE 4.1

SIMULATION PARAMETER

General Parameters	
Number of Nodes	5,10,15,20,25
Topology	Static
Simulation Time	1000 Sec
MAC Layer	802.11
Range	200 meters
Simulation Area	1000 x 1000 meter2
Routing Protocol	AODV
Channel Type	Wireless Channel
DOS Attack	Rushing Attack
Traffic Model Parameter	
Traffic Model	Constant Bit Rate
Packet Size	512 Bytes
Interval	1 Sec

Here topology specify overall square area for network.

1. Traffic model suggest what kind of traffic we are using.
2. Interval specifies time between successive packets.
3. Range specifies wireless network card signal propagation range.

4.2 Simulation Scenarios

Two simulation scenarios are used to simulate the effect of rushing attack and the effectiveness of prevention technique in mobile ad hoc network. The simulation scenarios are:

a. **Implementation of Traditional AODV Routing**

In this simulation scenario, first of all we construct a mobile ad hoc network and configure it with the help of AODV routing protocol. Than an illegal node is set over MANET and gained the performance of AODV protocol with the help of trace file.

b. **Implementation of Proposed Routing Technique**

In this simulation scenario a MANET is constructed and configures it with the help of AODV routing protocol after it an illegal node is constructed over mobile ad hoc network and obtained the performance of AODV protocol.

Finally simulate the effect of prevention technique in the form of PDR, Throughput, End-to-End Delay, Drop packet and Lost Packet etc.

4.3 Performance Parameters

In order to evaluate the performance of our approach, we have used the following Quality of Services Parameters:

4.3.1 All Lost Packet

Lost packet in the network can be defined as the different between sums of the number of data packet transfer by the source nodes and sum of the number of data packet received by destination nodes.

All Lost Packet = (sum of transfer packet - sum of received packet) 4.1

4.3.2 Drop Packet Ratio

Drop Packet Ratio can be defined as the ratio of sum of the number of the data packet lost in the network and the sum of the number of data packet generated by the each source nodes.

Drop Packet Ratio = (sum of lost packet * 100) / sum of transfer packet 4.2

4.3.3 Packet Delivery Ratio (PDR)

It is the ratio of the sum of number of data packets received by the each destination nodes and the sum of number of data packets generated by the each source nodes. Packet Delivery Ratio is denoted by PDR. If packet delivery ratio is high than it shows the protocol performance is also high.

PDR = (sum of number of received packet / sum of number of transfer packet) * 100 4.3

4.3.4 All Delay

All delay defined as delay sum is divided by summation of number of transfer packet.

All Delay = delay sum / sum of transfer packet 4.4

4.3.5 Average End-to-End Delay

End-to-End Delay represent time require to transfer packet from source node to target node. To compute End-to-End Delay:

Average E-2-E delay = received time - send time 4.5

4.3.6 Throughput

The throughput is defined as the sum of number of received packet per second over simulation time. The throughput is denoted by T,

Throughput = received node / simulation rime 4.6

4.4 Performance Analysis after Simulation

4.4.1 Network Lost Data Packet With Rushing Attack and After Prevantion

The below graph show the comparision of network lost data packet with rushing attack and after prevantion technique. In graph red line show the lost packet in presence of rushing attack while green line show the lost packet after prevantion technique. After prevantion technique packet losses is less than compared to presence of reshing attack in the network. In figure 6.1 show that the proposed algorithm decrese lost packet compared to AODV with rushing attack.

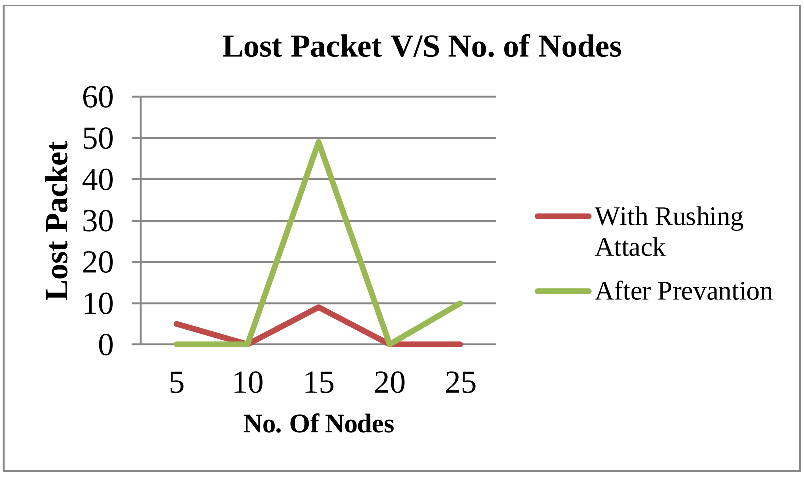

Figure 6.1 Comparision of Lost Data Packet With Rushing Attack and After Prevantion

4.4.2 Network Drop Data Packet With Rushing Attack and After Prevantion

The below graph show the comparision of network drop data packet with rushing attack and After Prevantion technique. In graph red line show the drop data packet in presence of rushing attack while green line show the drop data packet after prevantion technique. drop data packet in presence of rushing attack in the network is low and high after applied prevantion.

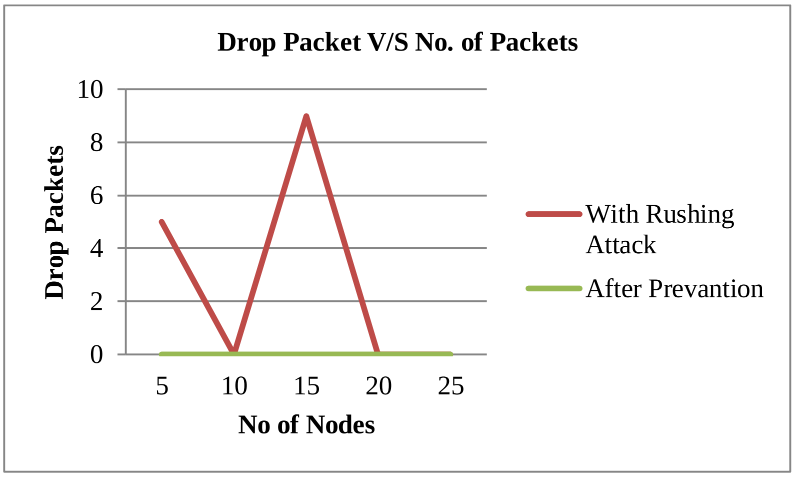

Figure 6.2 Comparision of Drop Packet With Rushing Attack and After Prevantion

4.4.3 Network Packe

In the below graph the number of nodes show on the x-axis and packet delivary ratio show on the y-axis. This graph show the comparision of network packet delivary ratio with rushing attack and after prevantion technique. red line show the packet delivary ratio in presence of the rushing attack. and green line show the packet delivary ratio after prevantion technique. The graph show that packet delivary ratio is low in presence of rushing attack and high after prevantion technique.

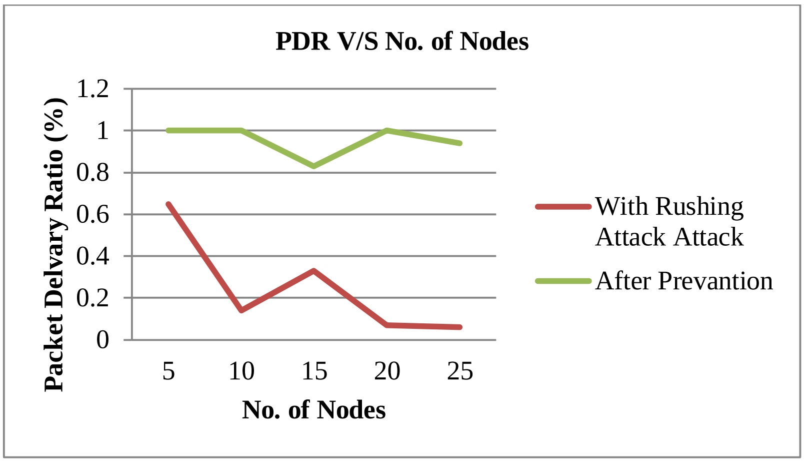

Figure 6.3 : Comparision of Packet Delivary Ratio with Rushing Attack and After Prevantion

4.4.4 Network All Delay With Rushing Attack and After Prevantion

In the below graph number of nodes show on the x-axis and All Delay show on the y-axis. This graph show the comparision of network All Dealy with Rushing attack and after prevantion technique. red line show the All Dealy in presence of the rushing attack. and green line show the packet All Dealy after prevantion technique. The below graph show that All Delay is high in presence of rushing attack and is low after prevantion technique.

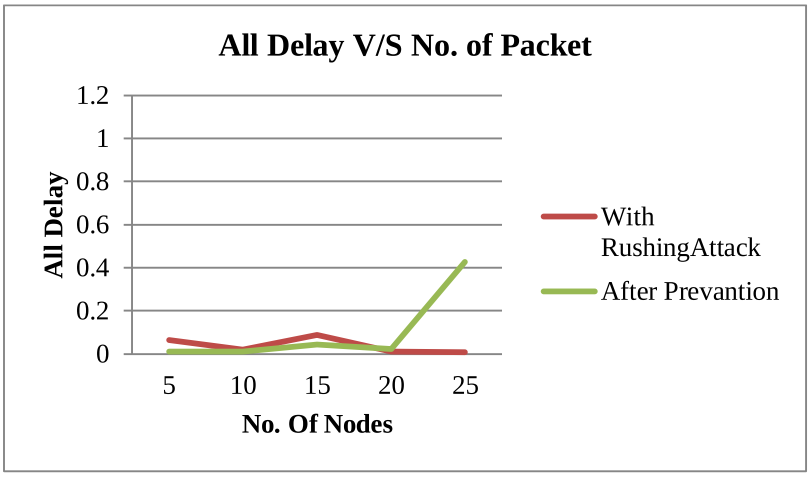

Figure 6.4 Comparision of All Delay With Rushing Attack and After Prevantion

4.4.5 Network Average End To End Delay With Rushing Attack and After Prevantion

In the below graph, the red line show Average End To End Delay in presence of Rushing attack and green line show the Average End To End Delay After Prevantion Technique. The below graph show that Average End To End Delay is high in presence of rushing attack and is low after prevantion technique.

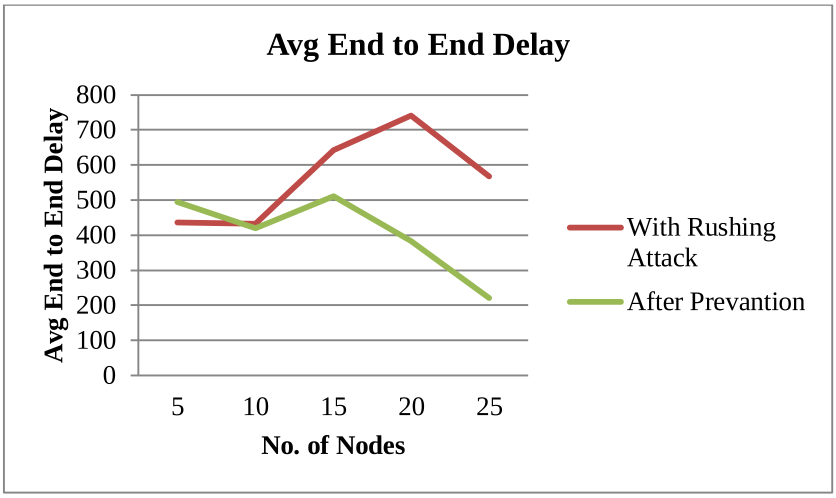

Figure 6.5 Comparision of Average End To End Delay With Rushing Attack and After Prevention

4.4.6 Network Average Throughput With Rushing Attack and After Prevention

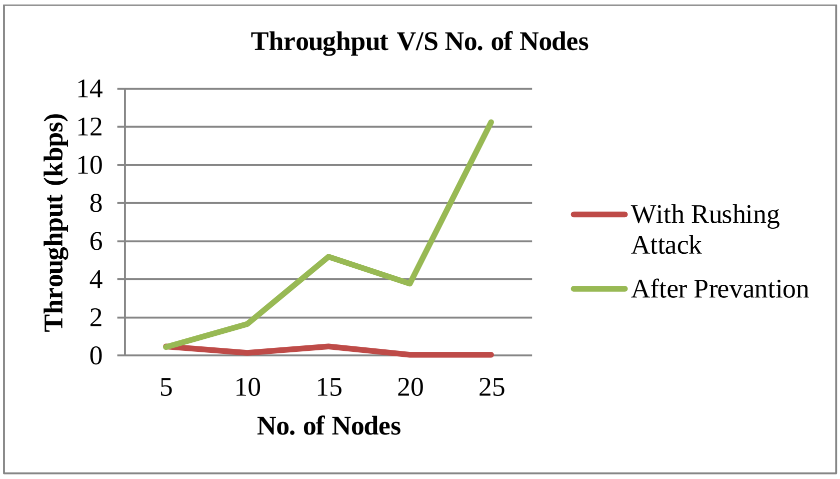

Figure 6.6 Comparision of Network Throughput With Rushing Attack and After Prevention

In the above graph, the red line show Throughput in presence of Rushing attack and green line show the Throughput After Prevention technique. This graph show the Comparision of Network Throughput With Rushing Attack and After Prevention . In figure 6.6 show that the proposed algorithm improved good throughput compared to AODV with rushing attack.

V. Conclusion and Future Work

5.1 Conclusion

In this proposed work, we use a secure technique which secure the network and increase the performance of network. In this work we do not use any special hardware. We have done is calculate the Round Trip Time for each path for compute the threshold value of RTT and also calculate the buffer length and delay for compute the threshold value of buffer length and delay. The proposed method is based on the decisional threshold. This technique is optimum for provide a securing network with increasing in performance of network. The simulation result shows that the performance of network in the form of Throughput, Packet Delivery Ratio, End-to-End Delay, Packet Drop and Packet Loss with prevention technique is better than the presence of rushing attack.

5.2 Future Work

In future, we can use this proposed method against the other routing protocol such as DSR to prevent effect of rushing attack in mobile ad hoc network. The system can be optimized for energy efficiency for long term of life time of network.

REFERENCES

[1] N. A. Noureldien, "A novel taxonomy of MANET attacks," 2015 International Conference on Electrical and Information Technologies (ICEIT), Marrakech, 2015, pp. 109-113.

[2] V. G. Mohite and L. Ragha, "Security agents for detecting and avoiding cooperative black hole attacks in MANET," 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, 2015, pp. 306-311.

[3] P. Kaneria and A. Rajavat, "Detecting and avoiding of worm hole attack on MANET using trusted AODV routing algorithm," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-5.

[4] S. Ghoreishi, S. AbdRazak, I. F. Isnin and H. Chizari, "Rushing attack against routing protocols in Mobile Ad-Hoc Networks," 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, 2014, pp. 220-224.

[5] Satyam Shrivastava, DharmendraMangal, "A New Technique to Prevent MANET against Rushing Attack" 2014 International Journal of Computer Science and Information Technologies, 2014, pp. 3460-3464.

[6] Sukiswo and M. R. Rifquddin, "Performance of AOMDV routing protocol under rushing and flooding attacks in MANET," 2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2015, pp. 386-390.

[7] U. Venkanna and R. L. Velusamy, "Black hole attack and their counter measure based on trust management in manet: A survey," 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011), Bangalore, 2011,pp.232-236.

[8] S. Lu, L. Li, K. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," 2009 International Conference on Computational Intelligence and Security, Beijing, 2009, pp. 421-425.

[9] V. K. Saurabh, R. Sharma, R. Itare and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in MANETs," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2017, pp. 489-494.

[10] S. J. Soni and S. D. Nayak, "Enhancing security features & performance of AODV protocol under attack for MANET," 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), Gujarat, 2013, pp. 325-328.

[11] H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra,Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET," 2016 10th International Conference on Sensing Technology (ICST), Nanjing,2016,pp.1-6.

[12] D. Khan and M. Jamil, "Study of detecting and overcoming black hole attacks in MANET: A review," 2017 International Symposium on Wireless Systems and Networks (ISWSN), Lahore, 2017, pp.1-4.

[13] P. K. Sharma and V. Sharma, "Survey on security issues in MANET: Wormhole detection and prevention," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 637-640.

[14] S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2017,

[15] B. K. Joshi and M. Soni, "Security assessment of AODV protocol under Wormhole and DOS attacks," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 173-177. pp. 2391-2394.

[16] N. Sharma and A. S. Bisen, "Detection as well as removal of black hole and gray hole attack in MANET," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 3736-3739.

[17] S. S. Narayanan and S. Radhakrishnan, "Secure AODV to combat black hole attack in MANET," 2013 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, 2013, pp. 447-452.

[18] S. Parbin and L. Mahor, "Analysis and prevention of wormhole attack using trust and reputation management scheme in MANET," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp.225-228.

[19] N. Purohit, R. Sinha and K. Maurya, "Simulation study of Black hole and Jellyfish attack on MANET using NS3," 2011 Nirma University International Conference on Engineering, Ahmedabad, Gujarat, 2011, pp. 1-5.

[20] A. Chaudhary, A. Kumar and V. N. Tiwari, "A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs," 2014 International Conference on Reliability Optimization and Information Technology (ICROIT),Faridabad,2014

[21]G. Singal, H. Garg, V. Laxmi, M. S. Gaur and C. Lai, "Impact analysis of attacks in multicast routing algorithms in MANETs," 2014 International Conference on Industrial and Information Systems (ICIIS), Gwalior, 2014, pp. 1-6.

[22] N. Arya, U. Singh and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," 2015 International Conference on Computer, Communication and Control (IC4), Indore, 2015, pp. 1-5.

[23] V. Desai and N. Shekokar, "Performance evaluation of OLSR protocol in MANET under the influence of routing attack," 2014 IEEE Global Conference on Wireless Computing & Networking (GCWCN), Lonavala, 2014, pp. 138-143.

[24] S. L. Agrwal, R. Khandelwal, P. Sharma and S. K. Gupta, "Analysis of detection algorithm of Sinkhole attack &amp; QoS on AODV for MANET," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2016, pp. 839-842.

[25] A. Sari and B. Rahnama, "Simulation of 802.11 Physical Layer Attacks in MANET," 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, 2013, pp. 334-337

[26] M. V. S. S. Nagendranath, B. A. Ramesh and V. Aneesha., "Detection of Packet Dropping and Replay Attacks in MANET," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, 2017, pp. 933-938

[27] S. P. S. Tomar and B. K. Chaurasia, "Detection and Isolation of Sinkhole Attack from AODV Routing Protocol in MANET," 2014 International Conference on Computational Intelligence and Communication Networks, Bhopal, 2014, pp.799-802.

[28] N. Soliyal and H. S. Bhadauria, "Preventing packet dropping attack on AODV based routing in mobile ad-hoc MANET," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, 2016,pp.1371-1375.

[29] L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, 2016, pp. 405-408.

[30] K. Laeeq, "RFAP, a preventive measure against route request Flooding Attack in MANETS," 2012 15th International Multitopic Conference (INMIC), Islamabad, 2012, pp.480-487.

[31] V. Trivedi and V. Preethi, "Depictive Analysis of MANETs under Black Hole Attack," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, 2017, pp. 1116-1120.

[32] K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks," 2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp 1-6

[33] P. Rajakumar, V. T. Prasanna and A. Pitchaikkannu, "Security attacks and detection schemes in MANET," 2014 International Conference on Electronics andCommunication Systems (ICECS), 2014, pp. 1-6.

[34] AatmprakashDwivedi, AbhishekPandey" An Approach to Provide Security Against Wormhole Attack in MANET", 2017 International Journal of Modern Engineering &Management Research, Volume 5 Issue 4,pp. 11-22.

[35] Dr.T.Pandikumar, HabtewoldDesta" RREQ Flooding Attack Mitigation in MANET Using Dynamic Profile Based Technique", 2017 International Journal of ComputationalScience and Engineering, Volume 7 Issue No.6,pp12700-12705.

[36] HarjinderKaur,Sukhjit Singh," Wormhole Attack Detection and Prevention in MANET Using Bait Scheme", 2017 International Journal of Engineering Science and Computing, Volume 7 Issue No.5,pp. 11640-11643.

[37] Satyam Shrivastava,” Rushing Attack and its Prevention Techniques”, 2013 International Journal of Application or Innovation in Engineering and ManagementComputing, Volume 2 Issue No.4, pp. 453- 456.

[38] NeelamJanak Kumar Patel,Dr.KhushbooTripati,”Trust Value based Algorithm to Identify and DefenceGray-Hole and Black-Hole attack present in MANET usingClustering Method” ,2018 International Journal of Engineering Science and Computing, Volume 4 Issue No.4, pp. 281-287.

[39] Monika Shivhare , Prof. Praveen Kumar Gautam” Prevention of BLACK HOLE attack in MANET Using Indexing Algorithm”, 2017 International Journal of Engineering Science and Computing, Volume 7 Issue No.6, pp. 12603-12606.

[40] Mr.Hardik N. Talsania, Prof. ZishanNoorani” A Survey on Techniques to Handle Black Hole Attack for AODV in MANET” 2018 International Journal of Innovative Research in Science and Technology, Volume 4 Issue No.10, pp. 33-37.

[41] R.Thilagarasi, D.Geetha” Prevention of Multiple Rushing Attack Nodes in Multicast MANET”, 2015 International Journal of Computer Trends and Technology , Volume 29 Issue No.2, pp. 64-68.

[42] H. Moudni, M. Er-rouidi, H. Mouncif and B. E. Hadadi, "Secure routing protocols for mobile ad hoc networks," 2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez, 2016, pp. 1-7.

[43] ManishaSood , Pooja Rani,” Removal of Black Hole Attack using AODV Protocol in MANET”, 2017 International Journal of Engineering Science and Computing, Volume 7 Issue No.3, pp. 72-75.

[44] Aakanksha Jain, Dr.SamidhaDwivedi Sharma” Rushing attack prevention algorithm for MANET using random route selection to make DSR and AODV more efficient” 2014 International Journal of Engineering and Computer Science Volume 3 Issue 6 June, 2014 Page No. 6520-6524.

[45] Shaveta Jain, KushagraAgrawal,” Prevention against Rushing Attack on MZRP in Mobile Ad-Hoc Networks” 2014 International Journal of Computer Science and technology, Volume 5 Issue No.3, pp. 124-128.

[46] NehaAgrawal, Krishna Kumar Joshi and Neelam Joshi “Performance Evaluation of Byzantine Rushing Attack in ADHOC Network” 2015 International Journal of Computer Applications, Volume 123 No.6, pp.1-4.

[47] A. Gupta, "Mitigation algorithm against black hole attack using Real Time Monitoring for AODV routing protocol in MANET," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 134-138.