Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 18 Issue 1 Version 1.0 Year 2018
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

ACO based AODV Method for Detection and Recovery of Misbehaving Node in MANET

By M. Sumathi & Dr. M.Gunasekaran

Abstract- Mobile ad-hoc networks (MANETs) can be described as a set of a huge variety of mobile nodes. MANET has the kind of applications such navy, disaster stuck regions and the characteristics of dynamic topology, no constant infrastructure, and many others. Nevertheless, there are a few protection issues and challenges in it. MANET is vulnerable to numerous attacks because of its open medium. As a result, there's need to examine in detail about the way to discover malicious or misbehaving node present inside the network. Ant algorithm is a set of rules this is most appropriate to be carried out in MANET environments than other algorithms. It can discover a most effective route, independent, decentralized, rapid adaptation, and multiple routes. Due to this motive, we use ant algorithm to enhance the overall performance of the proposed comfortable protocol. in this paper, Ant-primarily based Misbehavior node detection approach is carried out with ad-hoc On-demand Distance Vector (AODV) protocols and it figuring out the misbehavior node properly evaluate the parameters of packet delivery ratio, throughput and so on.

Keywords: AODV, ACO, misbehavior detection and recovery, MANET.

GJCST-E Classification: C.2.1, C.2.m

ACOBASEDAODVMETHODFORDETECTIONANDRECOVERYOFMISBEHAVINGNODEINMANET

Strictly as per the compliance and regulations of:

ACO based AODV Method for Detection and Recovery of Misbehaving Node in MANET

M. Sumathi [α] & Dr. M.Gunasekaran [σ]

Abstract- Mobile ad-hoc networks (MANETs) can be described as a set of a huge variety of mobile nodes. MANET has the kind of applications such navy, disaster stuck regions and the characteristics of dynamic topology, no constant infrastructure, and many others. Nevertheless, there are a few protection issues and challenges in it. MANET is vulnerable to numerous attacks because of its open medium. As a result, there's need to examine in detail about the way to discover malicious or misbehaving node present inside the network. Ant algorithm is a set of rules this is most appropriate to be carried out in MANET environments than other algorithms. It can discover a most effective route, independent, decentralized, rapid adaptation, and multiple routes. Due to this motive, we use ant algorithm to enhance the overall performance of the proposed comfortable protocol. in this paper, Ant-primarily based Misbehavior node detection approach is carried out with ad-hoc On-demand Distance Vector (AODV) protocols and it figuring out the misbehavior node properly evaluate the parameters of packet delivery ratio, throughput and so on.

Keywords: AODV, ACO, misbehavior detection and recovery, MANET.

I. Introduction

Wireless communication nowadays surrounds us in many colors and flavors, each with its specific frequency band, coverage, and variety of applications. It has matured to a large volume, and standards have advanced for personal area Networks, local area Networks in addition to Broadband wireless access. In Ad-Hoc networks, every node is inclined to forward data to different nodes, and so the determination of which nodes forward data is made dynamically based totally on the network connectivity. Minimum configuration and brief deployment make Ad-Hoc networks suitable for emergency situations like natural or human-caused disasters, navy conflicts, emergency medical situations and many others.

a) Routing in Ad Hoc Networks

Mobile ad-hoc Networks alternate their topology frequently and without previous observe makes packet routing in ad-hoc networks a difficult assignment. The cautioned procedures for routing can be divided into topology-based and position-based routing. Fig 1.1 represents the right category of ad-hoc routing Algorithms. Topology-based routing protocols use the information about the links that exist in the network to carry out packet forwarding. They may be further divided into proactive, reactive, and hybrid strategies.

Proactive algorithms rent classical routing strategies which include distance-vector routing (e.g., DSDV) or link-state routing (e.g., OLSR and TBRPF). They preserve routing facts about the available paths within the network even though those paths are not presently used. In response to this observation, reactive routing protocols had been evolved (e.g., DSR, TORA, and AODV). Reactive routing protocols maintain only the routes which are presently in use, thereby decreasing the load at the network when most effective a small subset of all available routes is in use at any time. however, they nonetheless have a few inherent barriers. Hybrid ad-hoc routing protocols along with ZRP integrate local proactive routing and international reactive routing with the intention to obtain a higher level of efficiency and scalability.

Position-based routing algorithms remove a number of the constraints of topology-based routing by using extra information. as a result does now not require the establishment or maintenance of routes. The nodes have neither to store routing tables nor to transmit messages to maintain routing tables updated. As an in addition benefit, position-based routing supports the delivery of packets to all nodes in a given geographic region in a natural way. This kind of provider is referred to as geocasting.

b) Attacks on Ad Hoc Networks

Wireless the structure of an Ad-Hoc network, or lack thereof, leads to a few special kinds of attacks. Especially attacks at the connectedness of the network which means that attacks on the routing protocol. A number of those attacks are Routing Loop, Black hole, gray hole, Partitioning, Blackmail, Wormhole, rushing attack, resource consumption, dropping Routing traffic, location disclosure and so forth.

Author α: Research Scholar, PG and Research Department of Computer Science, Government Arts College, Dharmapuri.
e-mail: sumathi.vedha26@gmail.com
Author σ: Assistant Professor & Head, PG and Research Department of Computer Science, Government Arts College, Dharmapuri.

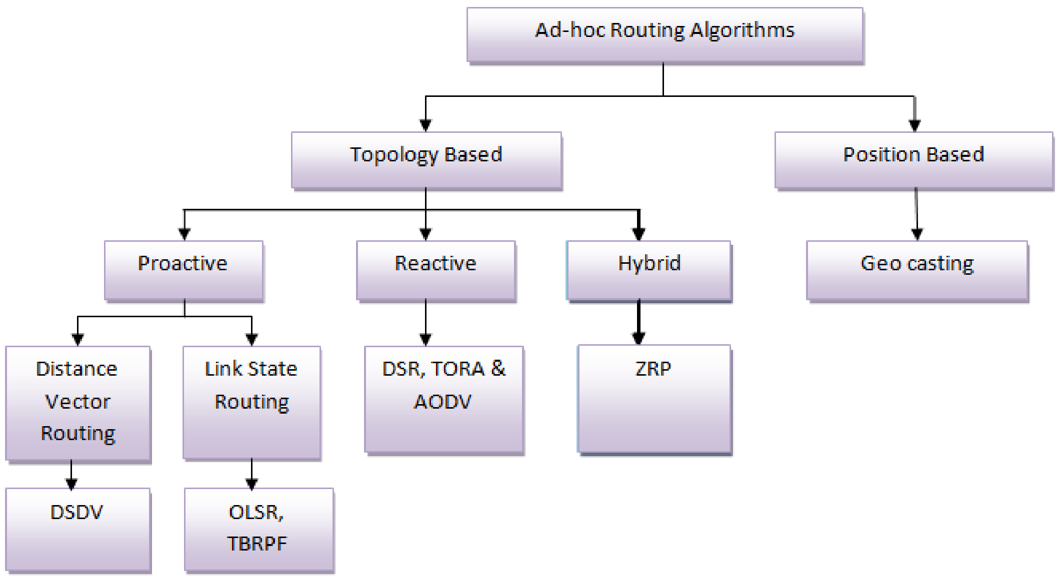


Fig.1.1: Classification of AD-Hoc Routing Algorithms

c) Security Model and Attributes

The sector of security is big and a few model to apply for attacking the problem is needed. Some of the attributes need to be considered for classifying the one of kind security desires of the applications of an Ad-Hoc network. Which can be Confidentiality, Authentication, Availability, Integrity, Non-Repudiation, fact of discovery, Isolation, lightweight computations, location, Self, Byzantine robustness and many others.

d) Security of Ad-Hoc Networks

Security vulnerabilities in ad-hoc networks are:

Limited computational capabilities: generally, nodes in ad-hoc networks are modular, independent, and restricted in computational functionality and consequently can also grow to be a source of vulnerability after they take care of public-key cryptography at some point of normal operation.

Limited power supply: due to the fact nodes generally use the battery as power supply, an interloper can exhaust batteries by developing extra transmissions or excessive computations to be performed by means of nodes.

Challenging key management: Dynamic topology and movement of nodes in an Ad Hoc network make key control difficult if cryptography is used within the routing protocol.

II. Review of Literature

Farid Bin Beshr et.al (2016), reveal about Adopting Intrusion Detection system (IDS) that allows the routing protocol to avoid misbehavior nodes and links. The IDS have to characteristic low overhead controlling packet, excessive accuracy degree and low price of both false alarms and missed detection rate. The proposed system primarily based on assigning a few nodes called “guard nodes” the obligation of overhearing and reporting the misbehaving nodes. The scheme is proposed to conquer the majority of the drawbacks related to the Watchdog strategies.[1]

Chinthanai Chelvan.k et.al (2014), describes EAACK(enhanced Adaptive Acknowledgement) demonstrates better malicious-behavior-detection rates in positive instances while does not greatly have an effect on the network performances. The Intrusion Detection systems named EAACK protocol in particular designed for MANETs and compared to different famous mechanisms includes, Watchdog scheme .The effects confirmed positive performances towards Watchdog in the cases of receiver collision and fake misbehavior record.[2]

A Al-Roubaiey et.al(2010) illustrates Adaptive ACKnowledgment (AACK), for fixing great issues: the limited transmission power and receiver collision. This mechanism is an enhancement to the TWOACK scheme where its detection overhead is decreased even as the detection efficiency is increased. The AACK mechanism may not work well on long paths with the intention to take a significant time for the end to end acknowledgments. This problem will deliver the misbehaving nodes more time for losing more packets.[3]

P.Nandhini Sri et.al (2016) decides that during this selfish node detection, data packet transmission among the nodes the routing path is mounted and maintained so long as it's far wished and routing overhead is substantially decreased. The simulation end result shows that the detection of the selfish node with a massive delay. Therefore shortcut tree routing (STR) protocol has been proposed in future work that is used for improving the overall performance of the selfish node and also route discovery overhead with low memory consumption and it provides the most appropriate routing path.[4]

Usha Sakthivel et.al (2011) finds out's selfish behavior of a node impacts the throughput of the network. The nodes may additionally choose a back down value of shorter duration. An algorithmic technique for misbehaving node detection and isolation in ad hoc networks by way of enhancing the protocol getting used inside the lower layers which consequently improves the performance of the network have been proposed. Similarly, studies can verify the practicality of the proposed concept.[5]

Kashyap Balakrishnan et.al (2005) defines network-layer acknowledgment-based schemes, termed the TWOACK and the S-TWOACK schemes, which can be honestly introduced-on to any source routing protocol. The TWOACK scheme detects such misbehaving nodes, after which seeks to relieve the problem with the aid of notifying the routing protocol to keep away from them in future routes. The schemes detect selfish nodes (links) so that other nodes may also avoid them in future route selections, with the goal of universal improvement in end-to-end packet delivery ratio.[6]

Suganya.N.R et.al(2013) evaluates, from the angle of reproduction allocation, we have a look at the effect of selfish nodes in a mobile ad hoc network that is termed as selfish replica allocation. In our method, every node computes credit risk facts on different related nodes personally to appraise the degree of selfishness. Our method can detect two unique kinds of routing manipulation even as keeping a low rate of false positives when showing the simulation effects.[7]

Rasika Mali et.al (2015) present different techniques for detection of misbehavior of nodes such as Watchdog, ExWatchdog, TWOACK, S-TWOACK, 2ACK and Adaptive ACKnowledgment (AACK), CONFIDANT, Record and Trust Based Detection. All techniques are analyzed with parameters like type of misbehavior, key mechanism used, advantages, limitations an performance evaluation using Packet Delivery Ratio (PDR) and throughput. Still the problem of receiver collision, limited transmission power and partial dropping are unsolved.[8]

III. Misbehaving Node Detection in MANET

An individual mobile node can also attempt to benefit from other nodes, however, refuse to proportion its own resources. Such nodes are known as selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior. One of the main sources of energy consumption inside the mobile nodes of MANETs is wireless transmission. A selfish node can also refuse to forward data packets to other nodes that allow you to conserve its very own energy.

a) *Misbehavior Detection and Mitigation*

To mitigate the unfavorable consequences of routing misbehavior, the misbehaving nodes need to be detected in order that these nodes can be avoided with the aid of all properly-behaved nodes. on this paper, we attention on the subsequent problem.

- Routing Misbehavior Model
- Detecting Router Misbehavior
- Detecting Flooding Attacks
- Packet Dropper Detection
- Path Tracing Algorithm
- Black hole attack Detection
- Hardware Assisted Detection
- Watchdog and Path rater
- Nodes Bearing Grudges

b) *Intrusion Detection in MANET*

An Intrusion Detection System (IDS) agent runs at each mobile node, and performs local data collection and local detection, while cooperative detection and international intrusion response may be triggered when a node reports an anomaly. Taken into consideration two forms of attack scenarios one at a time:

1) Abnormal updates to routing tables.
2) Detecting abnormal activities in layers other than the routing layer.

Each node does local intrusion detection independently, and neighboring nodes collaboratively work on a larger scale. individual IDS agents positioned on every and each node run independently and monitor local activities (which include consumer, structures, and communiqué activities within the radio range), locate intrusions from local traces, and provoke responses. Neighboring IDS agents cooperatively participate in global intrusion detection actions whilst an anomaly is detected in local data or if there's inconclusive proof.

i. *Resurrecting Duckling*

This mechanism can be adapted for node authentication in ad-hoc wireless networks. During the imprinting technique, the devices can trade cryptographic keys for signing messages. it is able to be possible to use the resurrecting ducking method to enforce a key distribution protocol to be used with IP sec or another security protocol.

ii. *Packet Dropping*

The concept of packet dropping committed via the misbehaving nodes. There are kinds of packet dropping carried out by using the misbehaving nodes, simple dropping, and selective dropping. As pointed out earlier than, the simple dropping is typically devoted to the aid of the selfish node, whilst the malicious node includes both simple dropping and selective dropping.

Global Journal of Computer Science and Technology (E) Volume XVIII Issue I Version I Year 2018

In simple dropping, the misbehaving nodes drop all of the packets now not to or from them; even as in selective dropping, the misbehaving nodes only drop data packets no longer to or from them while forwarding the control packets, including route request, route reply, and many others.

iii. *Packet Misrouting*

Within the MANET, a malicious node can misroute the data packets to its colluding partner or a randomly selected destination with the intention to mount further attacks to the networks or disrupt the regular communication. Throughout the detection process, the detection hardware can pay no attention to the destinations which receive misrouted data packets. All that the detection hardware cares is the misbehaving node misrouting data packets. If the detection hardware identifies that the node is committing packet misrouting, it's going to send out the warning message.

IV. Proposed Methodology

The proposed system is used to detect the misbehavior routing using 2ACK and additionally take a look at the confidentiality of the data message in MANETs environment. here, we used a scheme referred to as 2ACK scheme, wherein the destination node of the following hop link will send lower back a 2 hop acknowledgment known as 2ACK to suggest that the data packet has been acquired efficiently. The proposed work (2ACK with confidentiality) is as follows.

- If the 2ACK time is much less than the wait time and the original message contents are not altered at the intermediate node then, a message is given to sender that the link is working well.
- If the 2ACK time is more than the wait time and the unique message contents are not altered on the intermediate node, then a message is given to sender that the link is misbehaving.
- If the 2ACK time is more than the wait time and the original message contents are altered at the intermediate node, then the message is given to sender that the link is misbehaving and confidentiality is lost.
- If the 2ACK time is less than the wait time and the original message contents are altered at the intermediate node then, a message is given to sender that the link is working properly and confidentiality is lost.

At the destination, a hash code can be generated and in comparison with the sender's hash code to test the confidentiality of the message. Consequently, if the link is misbehaving, sender to transmit messages will now not use it in future and loss of packets may be avoided.

a) System Model

In the existing system, there is a possibility that when a sender chooses an intermediate link to send some message to destination, the intermediate link may give problems such as the intermediate node may not forward the packets to destination, it may take very long time to send packets or it may modify the contents of the packet. In MANETs, as there is no retransmission of packets once it is sent, hence care is to be taken that packets are not lost.

Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we have focused on the problem of detecting misbehaving links instead of misbehaving nodes using 2ACK scheme. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet. It will not be forwarded further. The result is that this link will be tagged. Our approach is used to discuss the significant simplification of the routing detection mechanism and also checking the confidentiality of the message in MANETs environment.

Module 1: Sender module (Source node). The task of this module is to read the message and then divide the message into packets of 48 bytes in length, send the packet to the receiver through the intermediate node and receive the acknowledgement from the receiver node through the intermediate node. After sending every packet the "Cpkts" counter is incremented by 1. 2ACK time is compared with the wait time. If 2ACK is less than the wait time, "Cmiss" counter is incremented by 1. The ratio of "Cmiss" to "Cpkts" is compared with the "Rmiss" (a threshold ratio). If it is less than "Rmiss", the link is working properly otherwise misbehaving.

Module 2: Intermediate module (Intermediate node). The task of this module is to receive a packet from the sender, alter/don't alter the message and send it to the destination. Get 2ACK packet from the receiver and send 2ACK packet to the sender.

Module 3: Receiver module (Destination node). The task of this module is to receive a message from the intermediate node, take out destination name and hash code and decode it. Compare the hash code of source node and the destination node for security purpose. Send 2ACK to source through the intermediate node.

b) Algorithm of 2ACK Scheme and Ant Implementation

We have used the triplet of N1 → N2 → N3 as an example to illustrate 2ACK's pseudo code. Where N1 is assumed as the source node, N2 is the intermediate node and N3 is the destination node. Note that such codes run on each of the sender/receivers of the 2ACK packets.

Nomenclature: {Cpkts = the number of the message packets sent, Cmiss = the number of the 2ACK packets missed, d = the acknowledgment ratio. WT = waiting time, i.e., the maximum time allotted to receive 2ACK packet}

Algorithm:

Step 1: Start the algorithm.

Step 2: Deploy the node 1000 x 1000 areas.

Step 3: If the node is failure in deployment move to Step 4.

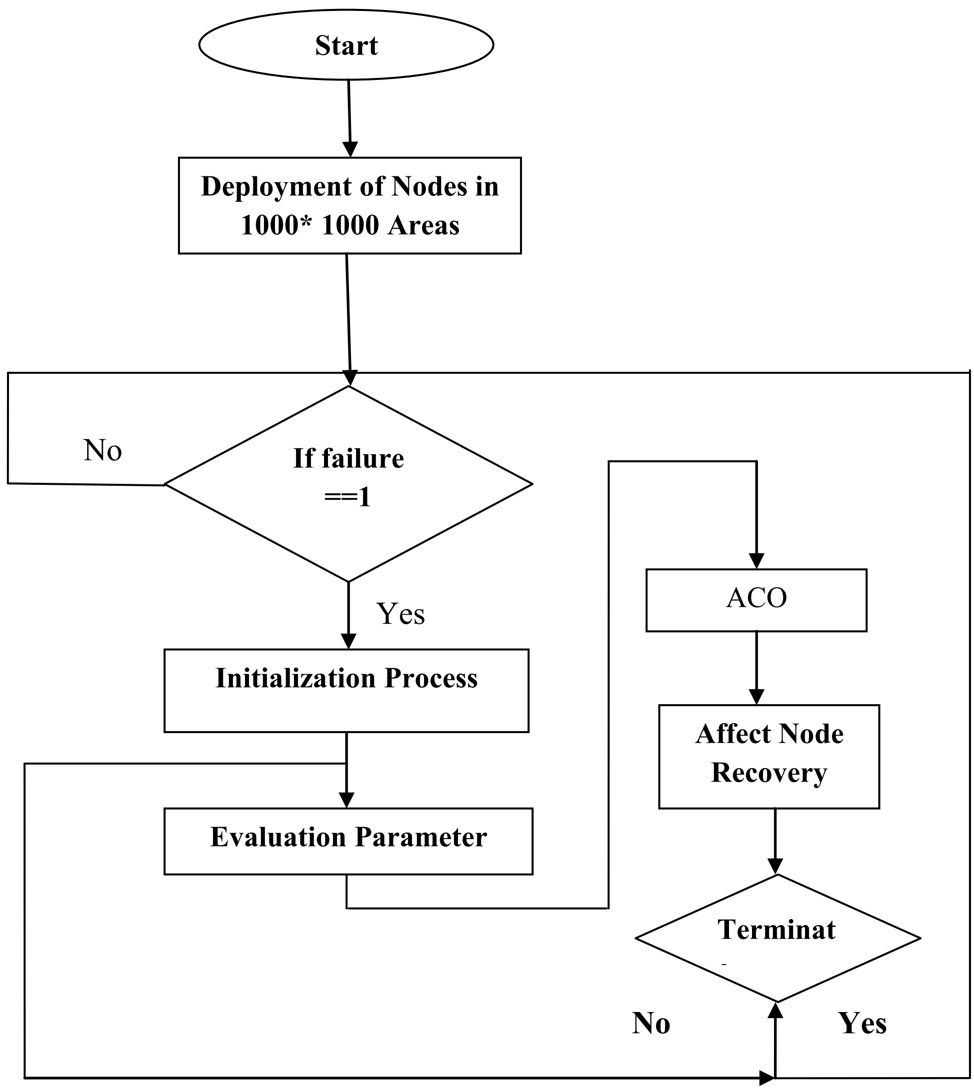
Step 4: Initialization of node failure identification.

Step 5: Evaluate the parameter for node identification.

Step 6: Perform ACO for node detection and routing.

Step 7: If the node is affected node then recover the node otherwise Step 8.

Step 8: Terminate the process.



i. *Ant node N1*

while (true) **do**

Read the destination address;

Read the message;

Find the length of the message. Cmiss=0, Cpkts=0, WT=20 ms, d=0.2.

2ACK Time=Current Time (Acknowledgement accepted time) – Start Time.

while (length > 48 bytes) **do** Take out 48 message packet; Length = length – 48;

Encode message using hash function; Send message along with the hash key; Cpkts++;

Receive 2ACK packet;

```
    if (2ACK time > WT) then
        Cmiss++;
 end
 end
if (length < 48 bytes) then
        Encode message using hash function; Send message along with the hash key; Cpkts++;
    Receive 2ACK packet;
   if (2ACK time > WT) then
    Cmiss++;
end
end end
     Routing Misbehavior Detection in MANETs Using 2ACK.
```

ii. *Ant node N2*

```
while (true) do
    Read message from source N1
if (Alter) then
    Add dummy bytes of characters;
    Process it and forward to destination N3; Receive 2ACK from N3 and send it to N1;
else if (Do not Alter) then
    Process it and forward to destination N3; Receive 2ACK from N3 and send it to N1;
End end
```

iii. *Ant node N3*

```
while (true) do
     Read message from N2;
     Take out destination name and hash code; Decode the message; Send 2ACK packet to N2;
end
```

iv. *Ant N1 and N3 parallel*

```
while (true) do
   if ((Cmiss/Cpkts)>d and (hash code of source msg) ! = (hash code of destination msg)) then
   Link is misbehaving and the confidentiality is lost;
end
if ((Cmiss/Cpkts)<d and (hash code of source msg) ! = (hash code of destination msg)) then
Link is working properly and the confidentiality is lost;
end
if ((Cmiss/Cpkts)>d and (hash code of source msg)
=(hash code of destination msg)) then Link is misbehaving;
end
if ((Cmiss/Cpkts)<d and (hash code of source msg)
=(hash code of destination msg)) then Link is working properly;
end end
```

V. Result and Discussion

We have used NS2 in our evaluation. We have selected 1000 * 1000m in AODV and 2500*2500m in Ant-Based AODV as our network size and generate 50 mobile nodes in both networks. To explain the various performance metrics required for evaluation of protocols, to reiterate the black hole attack, we begin with the overview of performance parameters that includes End-to-end delay, Throughput, Bit Error Rate and Packet Delivery Ratio. The parameters have to be measured against iteration.

Table 5.1: Simulation Parameters

Property	Value
Routing Protocols	AODV, Ant Based AODV
Area Covered(DSR)	2500*2500m
Area Covered(OLSR)	1000*1000m
Coverage Set	250m
No. of Nodes	50
Observation R Parameters	Throughput, End-to-End Delay, Bit Error Rate,Packet, Delivery Ratio and Iteration
Network Simulation	NS2
Optimization technique	ACO
No. Of Iteration	10
Population Size	500

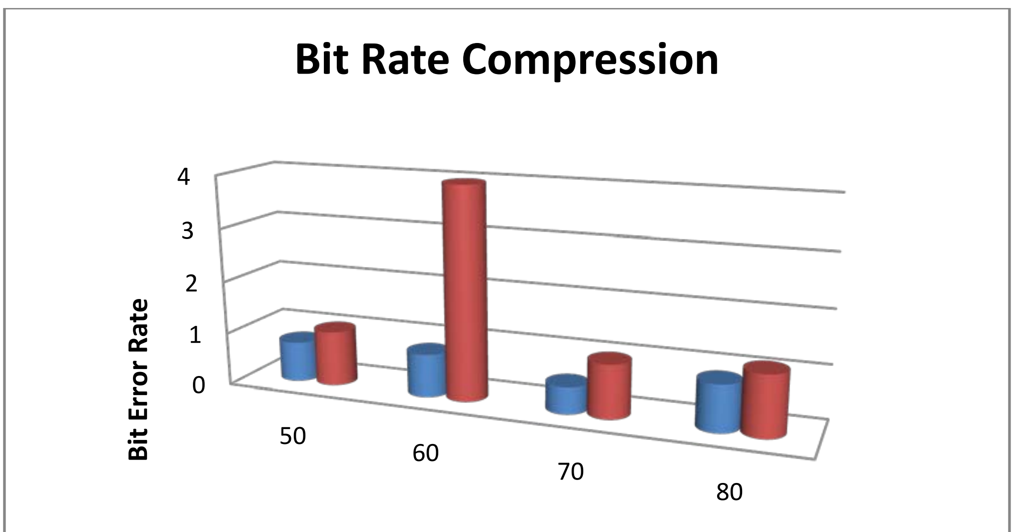
a) Results

The Result part is divided into two parts for two different protocols AODV and Ant-Based AODV and finally, their results have been analyzed in tabular form in table.

i. *Bit Error Rate*

Bit error rate is the percentage of bits with errors divided by the total number of bits over a given time period.

$$BER = \tfrac{1}{2}\,\mathrm{erfc}\sqrt{\frac{EB}{\text{No.of nodes}}}$$



	50	60	70	80
AODV	0.763	0.808	0.499	0.867
Ant Based AODV	1.044	3.984	1.003	1.133

Figure 5.1: Comparative Relation of Bit Error Rate

In Figure 5.1 shows the comparative relation of bit error rate in the presence of misbehaving attack and with optimization using ant colony optimization algorithm and shows that bite error measure is less with optimization as compared to the effect of attack in the network. This measure should be less for the efficient network.

ii. *Throughput*

The amount of data transferred from one place to another or processed in a specified amount of time.

Throughput = (Total No. of Bytes received/ Simulation time) * (8/1000)kbps.

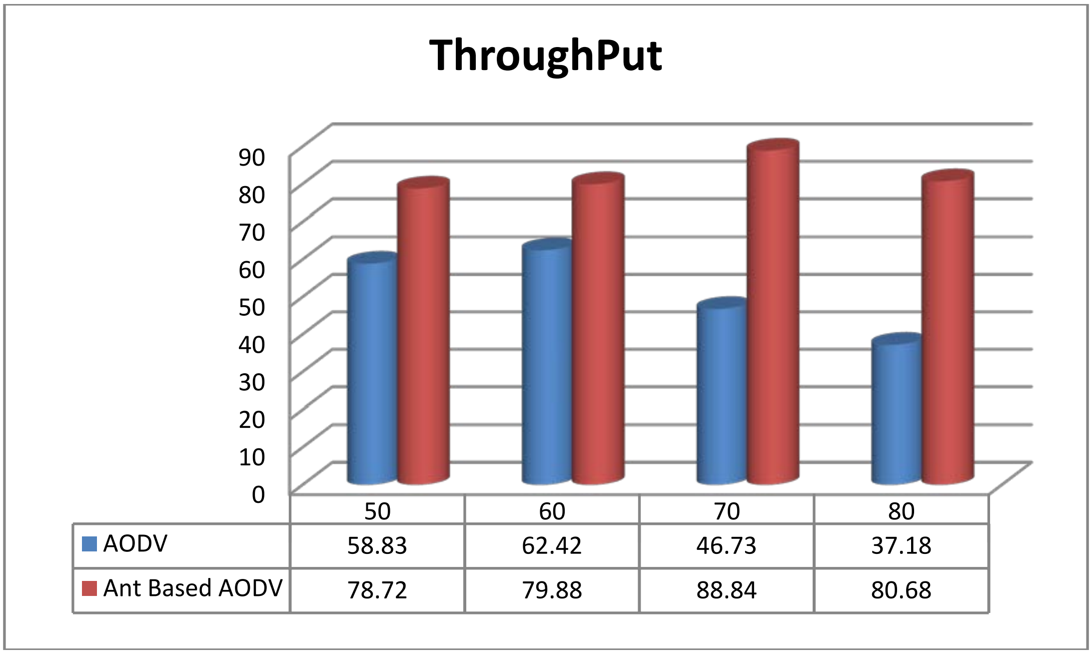


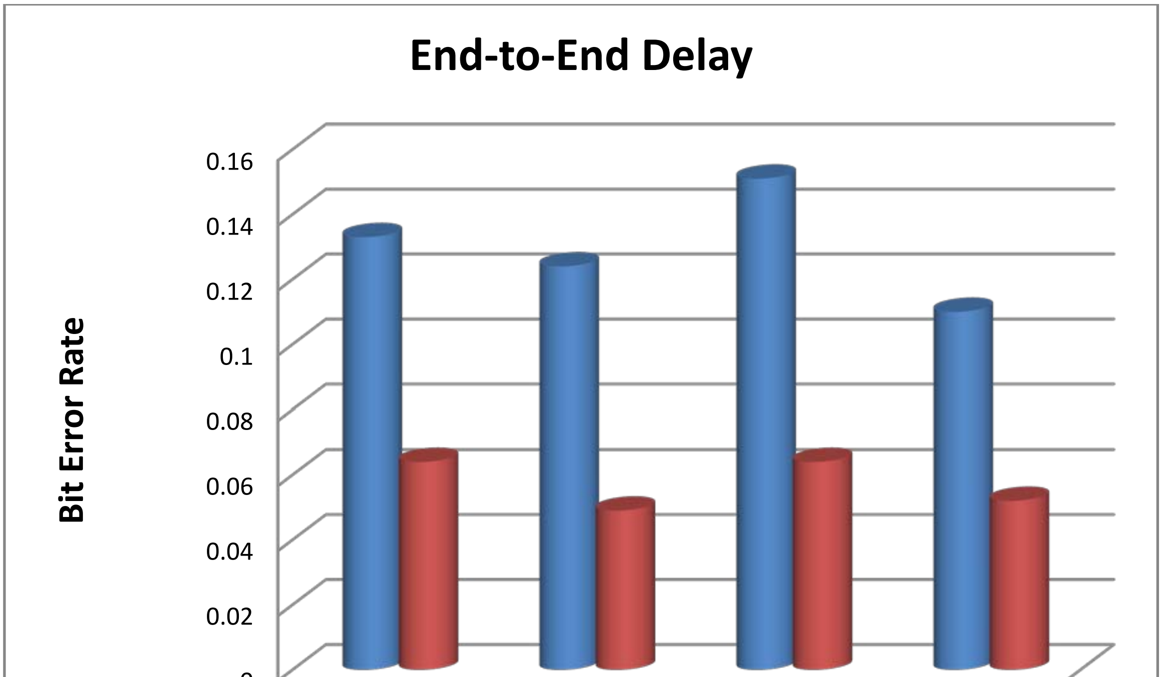
Figure 5.2: Throughput Measure with Attack and After Optimization

In Figure 5.2 shows the throughput measure with attack and after optimization and shows that this measure is having high throughput after optimization. The throughput is defined as the network performance with the successful delivery of the packets from source to the destination in an efficient manner.

iii. *End to End Delay*

End to End Delay refers to the time taken for a packet to be transmitted across a network from source to destination.

$$EED = \sum_{i=1}^{p} \text{Received} \; \frac{(\text{T Received} \; - \text{T Trasmission} \;)}{\text{P Received}}$$



	50	60	70	80
AODV	0.133	0.124	0.151	0.11
Ant Based AODV	0.064	0.049	0.064	0.052

Figure 5.3: End To End Delay Measure with Attack and After Optimization

In Figure 5.3 shows the End to End delay measure with attack and after optimization and shows the packets are delivered in less interval of time to increase the network lifetime. The end delay is defined as the number of packets received to the destination at fewer intervals of time with less error rate.

iv. *Packet Delivery Ratio*

Packet Delivery Ratio is defined as the ratio between the received packets by the destination and the generated packets by the source.

Global Journal of Computer Science and Technology (E) Volume XVIII Issue I Version I Year 2018

$$\text{PDR} = \text{P received} * 1000/ \sum_{i=1}^{n} \text{P generated}$$

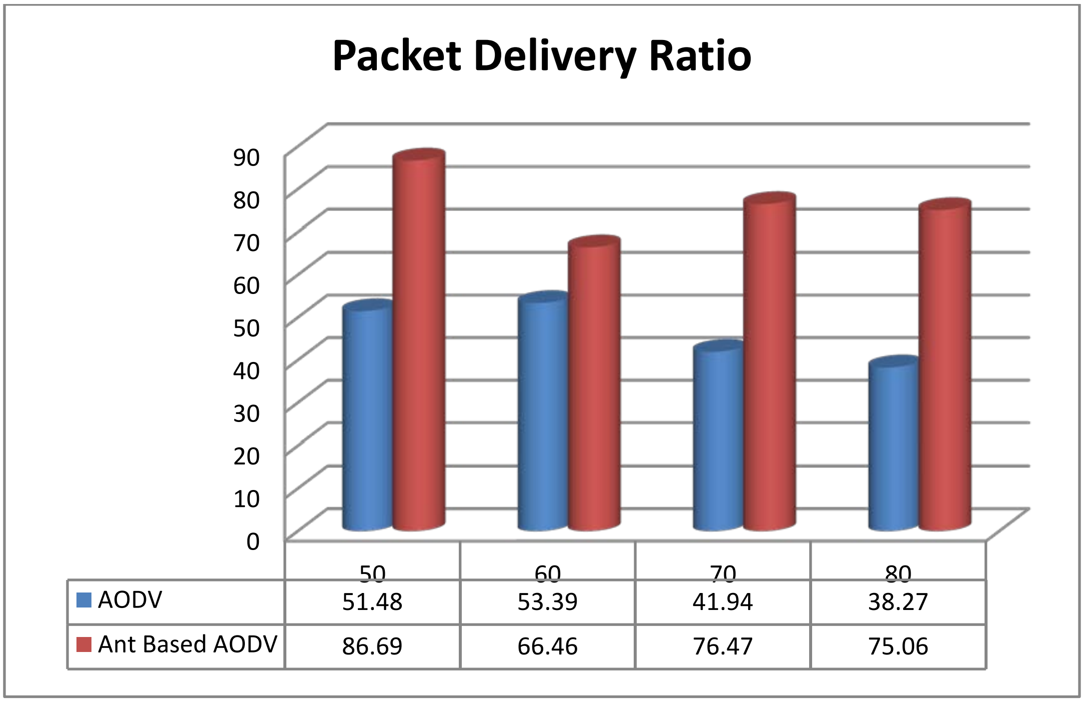


Figure 5.4: Packet Delivery Rate in the Presence of Attack and After Optimization

In Figure 5.4 shows the packet delivery rate in the presence of attack and after optimization with ant colony optimization and shows that the more packets are delivered in an efficient manner.

The packet delivery rate is defined as the number of packets successfully received to the destination node and the resulting graph of Ant AODV shows that the 15% more packets are delivered than the network in the presence of an attack.

b) Comparison of Aodv Routing Protocol using Aco

In table 1 we have compared the average values of AODV and AODV with ACO. In this, we have used the four different no. of nodes 50, 60, 70 and 80, and then we count the average value of all four parameters with 10 iterations for those nodes. At last the proactive and reactive routing protocols parameters with their nodes have been compared.

Table 5.2: Comparison of simulation Results

PARAMETERS	No. of Nodes							
	50		60		70		80	
	AODV	ANT AODV	AODV	ANT AODV	AODV	ANT AODV	AODV	ANT AODV
Throughput	58.83	78.72	62.42	79.88	46.73	88.84	37.18	80.68
End-to-End Delay	0.133	0.064	0.124	0.049	0.151	0.064	0.110	0.052
Bit Error Rate	0.763	1.044	0.808	3.984	0.499	1.003	0.867	1.133
Packet Delivery Ratio	51.48	86.69	53.39	66.46	41.94	76.47	38.27	75.06

For throughput on 50, 60, 70 and 80 no. of nodes the AODV performs 25%, 21%, 47% and 53% better results than the ANT BASED AODV Overall gives 36% improved results.

For end-to-end delay on 50, 60, 70 and 80 no. of nodes the AODV shows 51%, 60%, 57% and 52% better results than AODV. Overall ANT BASED AODV shows 50% better performance.

For Bit error rate on 50, 60, 70 and 80 no. of nodes the ANT BASED AODV shows 51%, 60%, 57% and 52% better results than AODV. Overall ANT BASED AODV shows 50% better performance. So AODV has high bit error rate.

For packet delivery ratio on 50, 60, 70 and 80 no. of nodes the ANT BASED AODV shows 41%, 19%, 45% and 49% better performance than AODV. The ANT BASED AODV deliver packets 34% faster.

VI. Conclusion and Future Enhancement

Node Misbehavior in MANET a serious issue in Mobile Ad-hoc Network. In the issue produce communication delay in Packet Delivery Rate, Throughput, and Overhead. We have investigated the performance degradation of the network because of a misbehaving node in MANET.

The AODV protocol with the Ant Optimization is used to detect the misbehaving node. The 2ACK scheme provides the detecting mechanism of misbehavior node from sender to receiver. The 2 ACK scheme tagged on the misbehaved node in the network. The receiver module identifies the 2 ACK has been tagged packet for retransmission. The retransmission has been performed in ACO optimized routing path. So the ACO Based AODV protocol performing better than AODV.

We have investigated the performance degradation caused by such misbehaving nodes in MANETs. We have analyzed and evaluated a technique, termed ACO, to detect and mitigate the effect of such routing misbehavior. We intend to simulate and analyze the effect of the attack in other routing protocols and can use ACO for better path detection with max-min optimization. In feature misbehaving node recovery with other optimization technique to be performed. There are many more other optimization techniques which perform better in future.

References Références Referencias

1. Farid Bin Beshr, Ahmed Bin Ishaq, Saeed Aljabri, and Tarek R. Sheltami, "A Guard Node (GN) based Technique against Misbehaving Nodes in MANET", Journal of Ubiquitous Systems & Pervasive Networks Volume 7, No. 1 2016 pp. 13-17.
2. Chinthanai Chelvan.K, Sangeetha.T, Prabakaran.V, Saravanan.D, "EAACK-A Secure Intrusion Detection System for MANET", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2014.
3. A Al-Roubaiey, T. Sheltami†, A. Mahmoud, E. Shakshuki, H. Mouftah, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.
4. P.Nandhini Sri, D.Karthikeyan, "Improving The Performance of Selfish Node Detection Using Watchdog Method in Manet" ,International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE), Volume – 2, Issue – 2. February 2016.
5. Usha Sakthivel and S. Radha," Misbehaving Node Detection in Mobile Ad Hoc Networks using Multi Hop Acknowledgement Scheme", Journal of Computer Science, 2011.
6. Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad-Hoc Networks", IEEE-2005
7. Suganya.N.R, Madhu.S Priya, "Detecting Selfish Nodes in a MANET through Fragmentation in Distributed Environment", International Journal of Science, Engineering and Technology Research (IJSETR),Volume 2, No 6, June-2013.
8. Rasika Mali, Sudhir Bagade, "Techniques for Detection of Misbehaving Nodes in MANET: A Study", International Journal of Scientific & Engineering Research, Volume 6, Issue 8, August-2015.