Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419

# DESIGN AND DEVELOPMENT OF THE MANET CONGESTION CONTROL AODV PROTOCOL USING CRYPTOGRAPHY

**Dr.J.Rajaram**
Postdoctoral Research Fellow, Department of Computer Science and Engineering,
Srinivas University Mangalore, Karnataka, India.

**Dr. Nethravathi P**
Professor& HOD, Department of Computer Science and Engineering, Srinivas University,
Mangalore, Karnataka, India

**Abstract:-**
Mobile ad hoc networks are types of decentralized communities where cell nodes can communicate with each other without a controller. Due to the lack of effective management, safety and service quality are our top concerns for the community. The largest green routing protocol is Ad Hoc On-demand Distance Vector AODV. It is most efficient to use the AODV routing protocol to transfer data from device to destination. In this picture, the AODV protocol is designed to avoid network congestion. The proposed method is mainly based on the back propagation algorithm, where the error is calculated for each operation from delivery to source. Choose the best route in its class with the fewest errors, or the route with the least probability of collision in a nearby area. Both the proposed algorithm and existing algorithms are used in NS2 and the analysis shows that the proposed system performs well with no difference to the current law.
**Keywords:** AODV, Cryptography, Active attack detection, Throughput, packet Delivery Ratio

## I. INTRODUCTION

A mobile ad hoc network, also known as a wireless media network or ad hoc wireless network, is a self-managed, self-configuring, and infrastructure less mobile wireless network. During this system; nodes can move in a random order. Therefore, each node acts as a router. In MANET, routing can be a method of choosing a route in the network. It has two tasks: Find the best path and send the given package on the road. The Ambient On Demand Distance Vector (AODV) routing protocol is an associate degree optional protocol, that is, it is based on the victim's method of finding the route. Because of its options, Eduard Manets is well suited for planetary applications where the topology changes rapidly. Nodes in MANET become part of the network and leave the network dynamically expressing their free behavior and their own usage. In this huge network, there is no need for any infrastructure and central management setup. Nodes are connected to each other via wireless interfaces [7].

### Objective

The aim of this study is to improve the results by analyzing the following parameters:
- Package delivery
- Delivery

### AODV Protocol

Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419

AODV is a special form of a distance vector request designed for unplanned mobile networks. AODV can be a reactive technique capable of non-broadcast and multicast routing [11]. AODV is a form of on-demand communication in which the routing process is initiated between the provider and the destination of the request. During this process, each node manages its routing information across multiple routing tables with a single access to any destination. AODV uses a sort position to ensure routing freshness and loop independence. AODV defines 3 messages: Redirect Request (RREQ), Redirect Error (RERR), and Redirect Response (RREP). These messages are used to find and manage routes from senders to destinations on the network. [5]. The provider sends the request path to its neighbors. If a neighbor has no information about the location, it sends a message to one or all of its neighbors, and so on.When a request reaches a destination containing information about the destination (either the destination itself or some of the available routes to the destination), the node sends a response to the originator of the Request Forwarding message [15]. At intermediate nodes (nodes that forward the routing request message), information about the origin and destination from the routing request message is stored. Also record the address of the neighbors to which the request was sent. Initializer given a unique ID. When a node receives a redirect request, it checks the originator's ID and address and sends the message if it has successfully completed the request [14].AODV can be a packet routing protocol designed for Mobile Unscheduled Networks (MANET) suitable for networks with thousands of nodes has two levels: discovery process and repair process

**Route Discovery**

Two languages: RREQ and RREP Sources of RREQ messages. If the node is not a resource, an RREQ is sent. Return the pointer to the creator. The target generates the RREP message. RREP returns a recovery pointer generated from the middle of the given error.

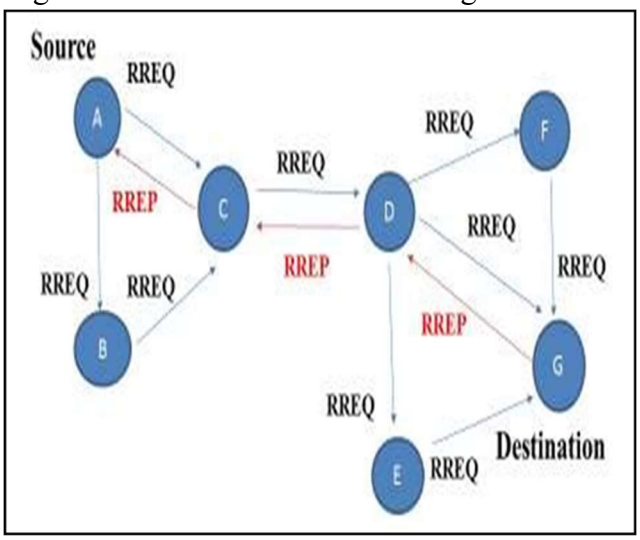



**Fig. 2.1: Routing DiscoveryinAODV**

**Route Maintenance**

Route Maintenance – 2 languages: how-to and RERR Hello message is used for connection status view like: if neighbor node2. The neighbor's connection is down. When a node detects that the

Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419

connection with its neighbor is down, it broadcasts the RERR message if it receives a RERR from one or more of the neighbor's active paths. [5].

**Sequence Number**

AODV differs from other on-demand systems in that it uses serial numbers to calculate resource updates. Each entry in the table is associated with an array [11]. Range is used as a routing term to provide a new routing type. After receiving the RREQ packet, the downstream intermediate node compares the sequence number with the number in the RREQ packet. If the currently saved array is greater than the array in the bundle, the current path is updated.

The registration number is greater than the number in the package and the current route is up to date.

**Performance Parameters in MANET**

**Package Delivery Rate**

- The ratio of packages delivered to the destination to the packages delivered by the destination.
- Throughput The number of data sent or received on the network per unit time.

## II. LITERATURE SURVEY

Guvin Wasser, Garima Guy and Pushpind Singh Paseja. New Intrusion Detection Algorithm: AODV Routing Protocol for Nodes. It faces many problems due to the uncertainty of the network topology i.e. security and congestion.In this article, we propose a new algorithm to detect intrusion, denial of service (DoS), vampire and user-to-root (U2R) attacks in the MANET environment. Intrusion detection is done by analyzing profile (behavior) and confusion matrices (true positive, negative, negative, negative). The performance of the standard Adhoc On-Demand Distance Vector (AODV) routing protocol against 4 types of attacks in the Network Simulator-2(ns-2) environment has been reported. To the best of the authors' knowledge, this is the first article to introduce a new access detection algorithm using the AODV protocol for behavior analysis in a MANET environment [1]. Ravinder Ahuja, Alisha Banga Ahuja, Pawan Ahuja "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANET Under Wormhole Attack" Designing wireless networks is an important task to help nodes send and receive packets. Security in mobile ad hoc networks is very difficult because there is no centralized control. Traditionally, routing protocols were designed purely for efficiency, without considering security issues. Therefore, it both creates new rules with security and incorporates security parameters into the existing routing process. There are many types of attacks against the system and one of them is a wormhole attack. We will evaluate the performance of AODV and DSR routing protocol under wormhole attack and compare the performance of protocols without wormhole attack. Performance metrics include average end-to-end latency, throughput, and packet delivery rate (PDR). Neelam Janak Kumar Patel, Dr. Khushboo Tripathi, in "An Enhanced AODV Protocol for Detecting and Preventing Black Hole Attacks in Mobile Ad Hoc Networks," Mobile Ad Hoc Networks (MANET) is a unique set of nodes; they are infrastructureless and wireless [2]. In MANET, nodes can leave and leave the network at any time. MANET, wormholes, black holes,

Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419

collisions, etc. It is vulnerable to many types of security attacks, such as Therefore, at MANET, security is the most important issue in ensuring secure communication and mobile transmission. The black hole attack is one of the most devastating effects of MANET routing at the network layer. A black hole is an evil mind where the attacker provides a way to happily represent each location, sending packets from every location to there. A black hole node sends illegal data claiming to have the best path and does another good at sending data over that path. The malicious node drops all the packets it receives instead of sending it. In this research paper, we use the IDSAODV routing protocol to increase the security of MANETs. It is a reactive ad hoc arbitrary distance vector (AODV) routing protocol for avoiding black hole attacks. Use the standard routing protocol (idsAODV) to detect and avoid black hole attacks. It is considered an upgrade to the AODV protocol. Use the network simulator NS-2. In Figure 35, we obtained test results showing improvements in throughput, packet delivery speed (PDR) and end-to-end latency using the idsAODV routing protocol, and in the presence of black hole attacks, the results were compared to AODV routing. procedures. Satyam Kumar Sainy, Ravi Rai Chaudhary, Ajay Kumar "Evaluation of the Performance of Routing Protocols Based on Different Models in MANET" Construction of Mobile Ad-hoc Networks is independent of wireless-affected mobile stations to form a system. The system can model the image without data. Adhoc networks are point-to-point, multi-hop networks in which packets travel point-to-point via nodes (acting as routers). The performance of these three pathways was performed in the Glomosim simulator and we concluded that in all three cases LAR1 was better compared to the AODV and DSR routing protocols. Packet rate behavior is similar, LAR1 has better PDR compared to AODV and DSR [3]. The packet loss rate is similar to PDR, in fact it is different from PDR, so we can say that LAR1 has lower packet loss than AODV and DSR. AODV and DSR have lower latency compared to LAR1. The LAR1 routing protocol has a high latency and it is seen that as the number of nodes increases, the time delay and motion delay also increase. Called the Cognitively Enhanced Interim On-Demand Distance Vector (CIAODV) (CRAHN), it aims to eliminate the overhead, resource consumption, and asset utilization (AODV) process that is calculated to be the most optimal and less suitable for integration. The simulation results prove that compared to the (AODV) protocol, the (CIAODV) protocol outperforms in terms of throughput, end-to-end latency and overhead [3]. Neelam Janak Kumar Patel, Dr. Khushboo Tripathi Enhanced AODV Protocol for Detecting and Preventing Black Hole Attacks in Mobile Ad Hoc Networks A mobile ad hoc network (MANET) is designed as a unique node network; these are wireless infrastructures. In MANET, nodes can leave and leave the network at any time. MANET, wormholes, black holes, collisions, etc. It is vulnerable to many types of security attacks, such as Therefore, at MANET, security is the most important issue in ensuring secure communication and mobile transmission. The black hole attack is one of the most devastating effects of MANET routing at the network layer. The black hole is evil, and the attacker gives a happy path, representing everything from every piece of the black hole to the packets sent to him. The malicious node drops all the packets it receives instead of sending it. In this research paper, we use the IDSAODV routing protocol to increase the security of MANETs.

Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419

It is a reactive ad hoc arbitrary distance vector (AODV) routing protocol for avoiding black hole attacks. Use the advanced routing protocol (idsAODV) to detect and avoid black hole attacks.

## III. PROBLEM STATEMENT

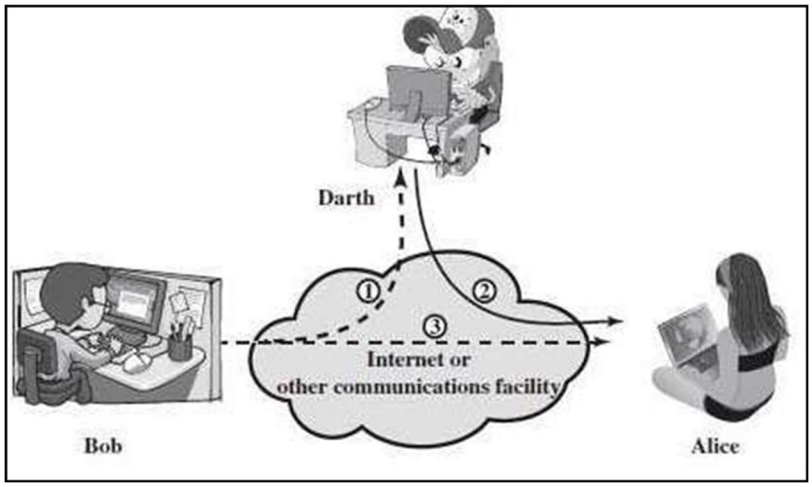
Most existing algorithms do not pay attention to security factors during routing, and mobile ad hoc networks have congestion, a problem that degrades the performance of the network. In this study, the AODV protocol was developed for congestion management and security against active intrusion detection.

## IV. WHAT IS CONGESTION CONTROL

When media traffic is heavy, the situation occurs at the network layer, thus reducing network latency. The effect of congestion slows down and performance drops. If the latency increases, retransmissions will occur, making things worse. When the number of packets at the edge increases, the limitation of network resources and the ability to cope with poor performance of the network is called congestion. Congestion is an undesirable situation where a network is faced with traffic that exceeds its capacity. Congestion means overcrowding or congestion due to overload. Édouard Manet was impressed by limited resources. Due to shared radio and communication quality, transmitted packets will be intercepted and interrupted. Mistransmission can cause a heavy load on the network due to retransmission of packets on the network. Congestion control technology is a method of distributing network traffic across multiple end-to-end connections [8]. The congestion will often be the cost based on congestion management or baseless congestion management.

### What is Active Attack Detection?

He was involved in some modification of the information flow or the creation of false water. These struggles are not easy. It is difficult to protect as there are many physical, software and network vulnerabilities. The aim is to detect the attack and repel it by interrupting or delaying the attack.



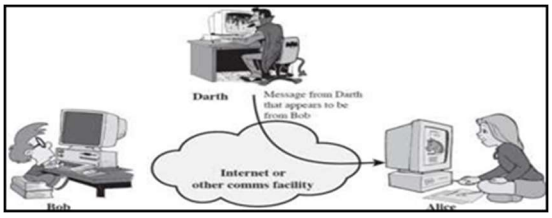

**Attacks can be divided into four types:**

1) Masquerade

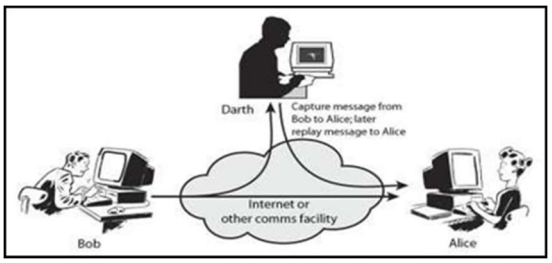
Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419

2) Replay
3) Message modification
4) Denial of service

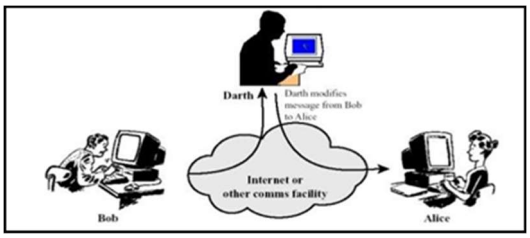
**Masquerade:**
When an organization pretends to be a private organization, sometimes one of every type of attack happens.



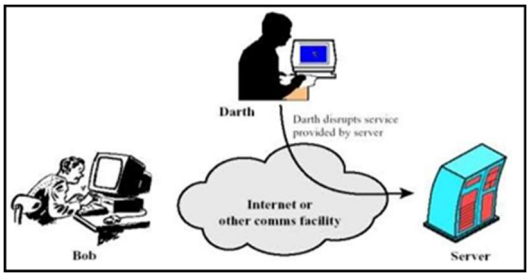

**Replay:**
Includes passive capture of information units associated with retransmissions that cause illegal interference



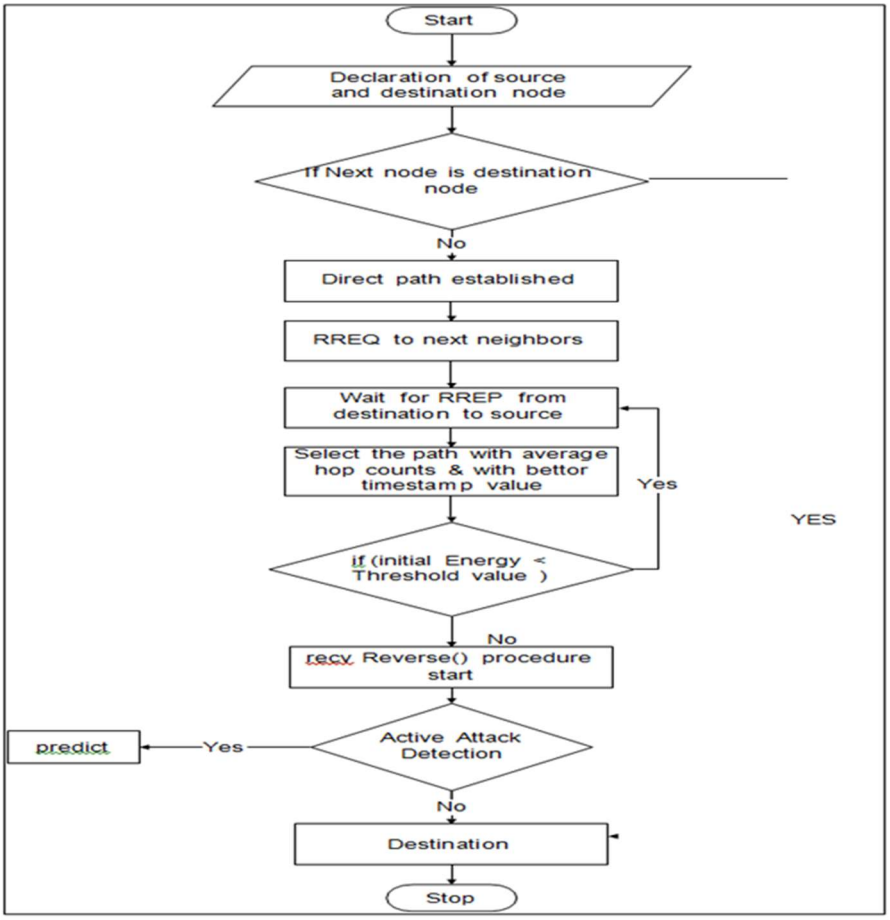

**Modification of Messages:**
Part of the correct message has been changed or reordered with suspended or unauthorized results.




**Denial of Service:**
prevent or restrict routine use or control of communication facilities



Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419




The AODV protocol first broadcasts a multipath from source to source and sends DES encrypted and next node to establish a direct route. The flowchart of the explanation is shown in the figure. After RREQ, go to the next nearest location. Wait for RREP from target to target, if output power is lower than threshold, choose route with average number of hops and better time value, and yes, wait for RREP from target to ground, not vice versa, the program starts and stops actively, so guessing that the attack will stop without going directly to the ground is done.

**SIMULATION PARAMETERS**

| *Parameters* | *Value* |
|---|---|
| *Simulator* | *NS-2(Version2.34)* |
| *Channel type* | *Wireless* |
| *MAC Type* | *Mac/802.11* |
| *Mobility model* | *Random way point mobility model* |
| *Number of mobile node* | *40,60 Nodes* |
| *Traffic Type* | *CBR* |
| *Routing Protocols* | *AODV* |
| *Simulation Time* | *300ms* |
| *Simulation area* | *1000*500m* |
| *Packet Size* | *512byets* |

## V. RESULTS

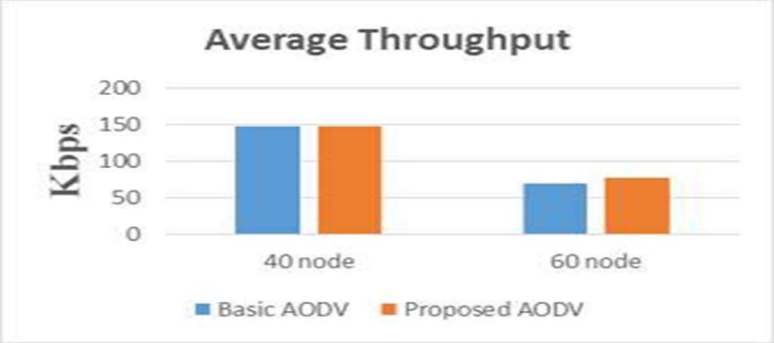
### Package Delivery Rate

The ratio of packages delivered to the destination to the packages delivered by the destination. indicates improved packet delivery compared to against 40 nodes. 60 node automatic AODV vs. improve AODV.

Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419


**Average Burn**

Number of packets sent or received on the network per unit time. represents an average increase and improved AODV for the 40-node and 60-node level.




## VI. Conclusion

We conclude that the AODV protocol is improved with congestion control and also provides security against attacks which provides better performance for networks using large numbers of nodes.

## REFERENCES

[1] "Gurveen Vaseer, Garima Ghai and Pushpinder Singh Patheja.", "Intrusion Detection Algorithms: AODV Routing Protocol," 978-1-5386-1356-6/17 $31.00 © 2017 IEEE.

[2] "Ravinder Ahuja, Alisha Banga Ahuja, Pawan Ahuja", "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANET Under Wormhole Attack", 978-1-4673-6101-9/ 13EE © 2010. .

[3] "Satyam Kumar Sainy, Ravi Rai Chaudhary, Ajay Kumar", "Evaluation of Performance of Routing Protocols Based on Different Models in MANET", 978-1-5090-0774-5/16/$31.00 © 2016 IEEE .

[4] "Li Shibao, Jia Wei", "Research on AODV Routing Protocol Based on Enhanced ERS Algorithm", 978-1-4244-5849-3/10/$26.00 ©2010 IEEE.

[5] "Priya Mankotia1 and Private.Amandeep Kaur2", "Design and Improvement of AODV Protocols for Congestion Avoidance in MANETs Using Neural Networks", Vol 6, Issue 5, Sep-Oct 2017 ISSN 2278-6856.

[6] "Neelamaj Janak. Khumar Patel Thiab Dr. , "Mitigation Method for Black Hole Attack Based on Route Discovery Mechanism in AODV Protocol", 978-1-4799-1597-2/13/$31.00 ©2013 IEEE.

Catalyst Research Volume 23, Issue 2, July 2023 Pp. 2411-2419

[8] "Mr. Hardik N. Talsania thiab Prof. Zishan Noorani", "Techniques for Handling AODV Black Hole Attacks in MANET", IJIRST – International Journal of Innovation and Technology Research Cilt. 4Lub Peb Hlis 10, 2018.

[9] "Rajaram Jatothu, Dr. RP Singh", "Efficient Routing and High Security Transport Using AODV and Distributed Protocol Key Generation Using Dual RSA", International Journal of Applied Engineering Research ISSN 0973-4562 vol 12, Issue 23 (2017).

[10] "Vivek Soi and Dr.Dhaliwal, B.S., Performance Comparison of DSR and AODV Routing Protocols in Mobile Private Networks, ISSN 0973-1873, Vol. 13, no. 7 (2017), p. 1605-1616 © Research India Publications.

[11] "Rada Rani Gupta, Mahindra Ku.Mishra thiab Manish Srivastava", "Ib Lub Zog Efficient Routing Protocol rau Ad Hoc Networks Raws li AODV", International Journal of Computer Applications, Vol 85 – Issue 19, January 2014.

[12] "Rasha Eltayeb, Adel Gaafar", " Cognitively Txhim kho AODV "Routing Protocols for Cognitive Radio Ad Hoc Networks", (IJISSET) ISSN 2455-4863 (Online) Vol: 3 Issue: 10 October 2017.

[13] "Abdelhafid Abouaissa1, Riri Fitri Sari2, thiab Pascal Lorenz1" , "Security and Performance Optimized AODV Routing Protocol", Copyright © 2014 John Wiley & Sons, Ltd.com). DOI: 10.1002/dac.2837ib.

[14] "Madhup Shrivastava, Monica Sahu, M.A. Rizvi and Khaleel Ahmad", "An Enhanced AODV Routing Protocol for MANET", International Journal of Advanced Research in Computer Science, Vol 9, Issue 2, March-April 2018.

[15] "Tanya Koohpayeh Araghi, Mazdak Zamani , Azizah BT Abdul Mnaf", "Performance Evaluation of Reactive Routing Protocols in Wireless Mobile Private Networks Using DSR, AODV and AOMDV", 978-0-7695-5133-3/13 $26.00 © 2013 IEEE.

[16] "Uma Rathore Bhatt, Abhishek Dangarh, Akanksha Kashyap, Aishwarya Vyas", "Performance Analysis of AODV and DSR Routing Protocols for MANET", 978-1-4799-3070-8/14 $31.00IEEE © 2014

[17] "Mohamed S. El-azhari, Othman A. Al-amoudi, Mike Woodward ve Irfan Awan", "Performance Evaluation of AODV-Based MANET Protocol", 978-0-7695-3639-2/09 $25 .