Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Analysis for the Effect of Selfishness Attack on AODV Protocol

Gajiyani Rizwana[1], Prof. Ghada Wasim[2]

[1]Computer Engineering, B. H. Gardi College of Engineering & Technology
[2]Computer Engineering, B. H. Gardi College of Engineering & Technology

Abstract* —A Mobile Ad-hoc Network (MANET) is the system of self-designing hubs without having any settled base and topology. In portable specially appointed system all the hub have restricted battery and lifetime in the system. There is numerous directing conventions depend on presumption that each hub forward parcels to other hub however a few hubs are make trouble or non-helpful which is known as selfish hub. In this paper we examined about the distinctive IDS system to distinguish the selfishness hub in the mobile ad hoc network. Then after we implement the Selfishness attack based on energy and compare it with original AODV protocol.

Keywords-introduction; characteristics and application; aodv routing protocol; selfishness attack; literature survey; performance parameter analysis;

I. INTRODUCTION

Mobile ad hoc network (MANET) is gathering of versatile hubs having dynamic topology, interconnected by means of remote connections, which consent to coordinate and forward each other's parcels. One of the fundamental presumptions in the interest of the configuration of steering conventions in MANETs is that each hub is straightforward and helpful however basically it is impractical in light of the fact that large portions of them go about as a childish hub. They take an interest in the system however don't co-work with other hub since they spare their assets for their own particular use. The base is not settled that is changing with element topology. All the hub in the versatile specially appointed system have constrained battery, data transfer capacity and life time. Every hub require the assistance of other hub to forward their bundle. Because of the portability and element nature of the MANET, system is not secure. There is numerous difficulties in the MANET like multicast steering, power utilization, unwavering quality, Security, versatility and so on.

II. CHARACTERISTICS AND APPLICATIONS

2.1 Characteristics

- Autonomous behavior means each node act as a both host & router.
- Multi-hop transmission means when data packet send from source to destination with the help of one or more intermediate nodes.
- Dynamic topology means change in topology frequently because of mobile nodes.
- Infrastructure less means there is no any fixed infrastructure in the mobile ad hoc network.
- Light weight means nodes in the network having less CPU processing capability, small memory size, and low power storage.

2.2 Applications

- Military Communication
- Emergency services
- Commercial and civilian
- Education
- Entertainment
- Home and enterprise

III. AODV ROUTING PROTOCOL

AODV is supported by both unicast and multicast routing. It is reactive routing protocol. AODV build up courses between various hubs as required by source hubs. There are three messages Route Errors (RERRs), Route Request (RREQs) and Route Replies (RREPs) which is characterized by AODV, for finding and keeping up courses in the system. These three messages are utilized, by utilizing UDP bundles from source to destination. AODV stays away from the checking to-endlessness issue of other separation vector conventions by utilizing grouping numbers on course upgrades. AODV responds generally rapidly to the topological changes in the system. It is also find the latest updated route to reach the destination. AODV protocol have the routing table which contain the no of fields like Destination IP address, Destination Sequence Number, Valid Destination Sequence Number Flag, Other state and routing flags, Network Interface, Hop Count (needed to reach destination), Next Hop, Precursor List, Lifetime (route expiration or deletion time).There are two phases Route Discovery & Route Maintenance. Each node maintains a routing table with knowledge about the network. AODV deals with route table management.

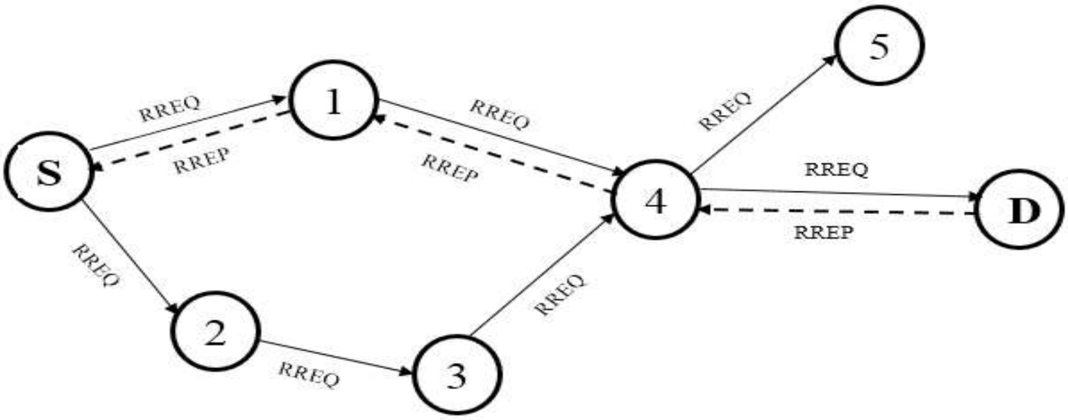
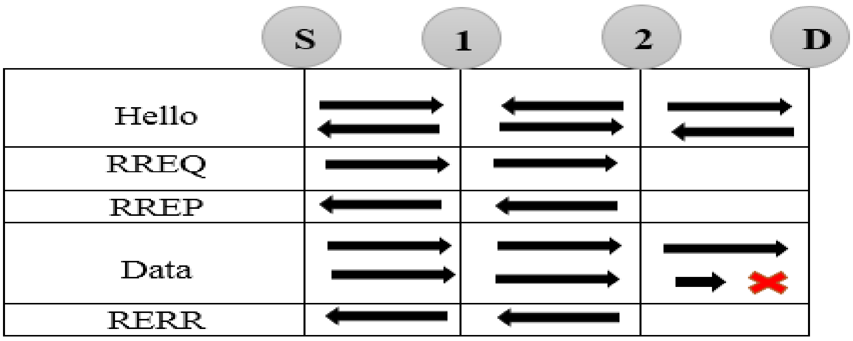


Figure 1. AODV Routing Protocol



Hello	→ ←	← →	→ ←
RREQ	→	→	
RREP	←	←	
Data	→ →	→ →	→ → ✖
RERR	←	←	

Figure 2. AODV Protocol Message

IV. SELFISHNESS ATTACK

In the mobile ad hoc network all the node consume energy in active state and sleep state. When node send or receive the packet at that time it is in active state and when it is in idle mode it is in sleep state. The largest source of the energy consumption in the network when node send the packet. There is also energy consumed when node is in idle state means it is not participating in any communication. Mobile Ad-hoc network is only successful if there is cooperation between nodes. All the node have limited resource like bandwidth & energy because of that some nodes stop forwarding the packet or dropping the packet or stop to forward the route request or route reply for saving their resource for their own purpose. This type of actions is called selfish behavior & this node is called the selfish node. There is mainly two types of uncooperative nodes like malicious node & selfish node.

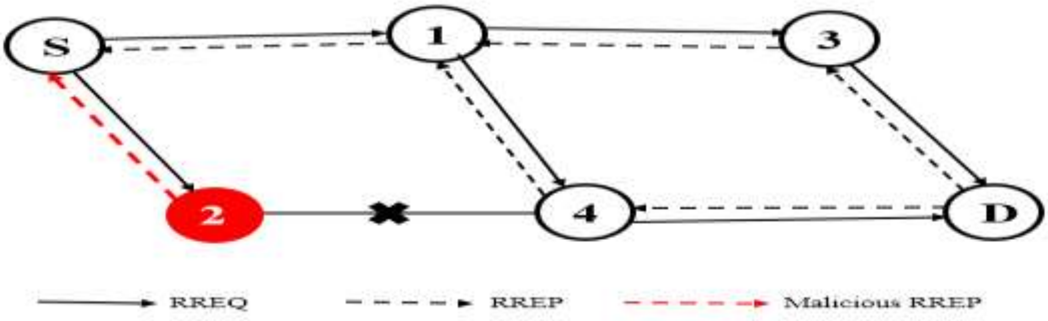


Figure 3. Selfish node in network

V. LITERATURE SURVEY

Author discussed in this paper [4] about TBUT means token based umpiring technique. This technique is based on the foundations of two systems proposed by Kathirvel and Srinivasan, namely self-umpiring system (SUS) and enhanced triple umpiring system (ETUS). In the TBUT, each node is issued with a token at its inception. The token consists of three fields: NodeID, status, and reputation. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single-bit flag. Initially, the status bit is preset to zero indicating a green flag. Initially, reputation value is zero, i.e., positive. The token with a green flag and positive reputation is a permit issued to each node, which confers it the freedom to participate in all network activities. It Increase throughput & PDR, but there is many assumption in this techniques like source & destination are not selfish node, bidirectional communication link etc.

Author discussed in this paper [5] about AMMDM means Audit Misbehavior Detection and Monitoring Method. This system consists the three major factors such reputation, route discovery, and an audit monitoring process. This reputation system identifies and isolates the misbehaving nodes from the network to ensuring the reputed packet transmission via trustworthy nodes in MANET. For this it use firsthand information & second hand information. The audit system is responsible for identifying the set of nodes that misbehave in a particular path and also identify the single or multiple misbehaving node. It find both continuous & selective packet dropper.

Author discussed in this paper [6] about RTBD means record & trust based technique. In this paper, the trustworthiness of a node is evaluated based on their behavior. The basic idea is to build a trust model that provides a mechanism to evaluate the trust of its neighbors. In this framework, every node maintains a global trust state for all selfishly behaving nodes in the network. Trust state is maintained in the form of a trust table. A trust table contains two fields, namely n-id (node id) and t-val (trust value). When a node receives a new trust certificate, the trust state of a node is updated. It Reduce the throughput during the high load.

Here we study the no of research paper & then make the comparative study table for the different techniques to avoid selfishness in MANET.

5.1 Comparative Study

Features	Watchdog	Pathrater	CONFIDENT	CORE	OCEAN	SORI	2ACK
Design	Distributed	Distributed	Distributed	Distributed	Distributed	Distributed	Distributed
Underlying Protocol	DSR	DSR	AODV	DSR	DSR	AODV	AODV
Layer	Data link & Network	Data link & Network	Network	Network	MAC & Network	Network	Network
Observation	Passive	Passive	Passive	Passive	Passive	Passive	Active
Detection	Single node	Single node	Single node	Single node	Single node	Single node	Single node
Punishment	No	No	Yes	Yes	Yes	Yes	Yes
Computational Overhead	Low	Low	Low	Low	Low	Low	Low
Communication Overhead	Low	Low	Low	Low	Low	Low	high
False positive	High	High	Yes	Partially Restricted	High	Low	High
Robustness Against collusion	No	No	Yes	No	no	No	no
scalability	yes	Yes	Yes	Yes	yes	Yes	yes
Second chance Mechanism	No	No	No	No	yes	No	No
Inspection source to neighbor	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Inspection Neighbor to Other	No	No	No	No	No	No	Yes

Table 1. Comparative Study

5.2 Survey Table

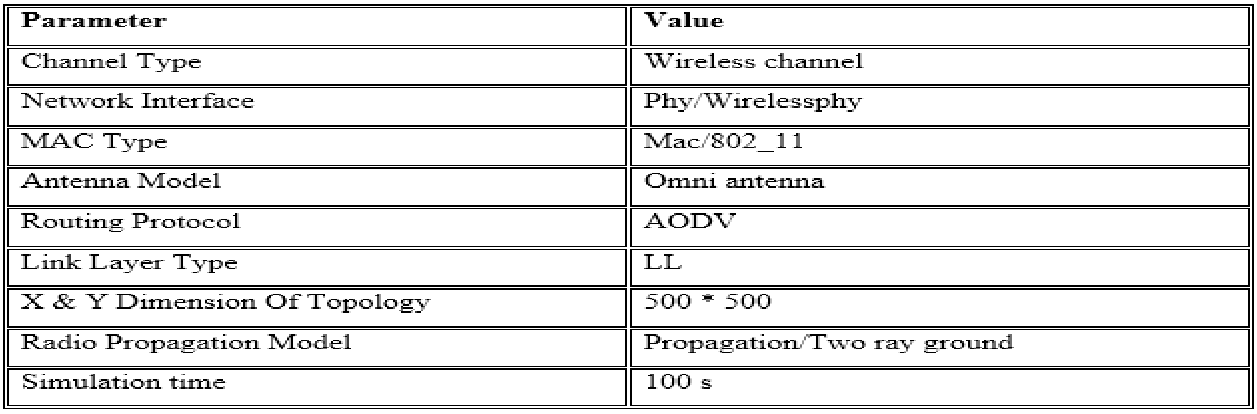
Sr no	Paper Title	Year & Publication	Method	Parameter Improve
1	A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT	2015, Springer	TBUT technique is the combination of two technique Self umpiring system & enhanced triple umpiring system. All the node initially have status, node id & reputation value. Status have two single bit value 0-green flag & 1-Red flag and reputation value have two value 0-positive & -1-negative.	PDR increase, Communication overhead decrease
2	Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks	2015, elsevier	AMDM (audit monitoring & detection method) have mainly three component: Reputation, Route discovery & audit monitoring. It is also used the 1st hand info & 2nd hand info also audit monitoring identify the set of misbehaving node in the path.	No of packet drop decrease
3	A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique	2014, Springer	Every node collect the neighbor info like energy, packet count & queue size. Based on this it calculates the trust value & detect the selfish node.	PDR increase. Average detection & packet dropping rate decrease
4	Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks	2009, ICGST-CNIR Journal	2ACK is the network layer technique which is detect the misbehaving link. When node 1 successfully forward data packet to node 2, at that time destination of node 2 send special 2-hop ack called 2ACK	PDR & Throughput increase
5	Intrusion Detection of Selfish and Malicious Nodes in MANET	2015, NCRACCESS	CONFIDENT contain main four components Monitor, path manager, trust manager & reputation system. Node monitor behavior of the neighbor node if any node misbehave then it send alarm to reputation system and update the table & send it to the path manager.	Selfish node detection time decrese
6	Mitigating routing misbehavior in mobile ad-hoc networks,	2000, ACM	In this paper two method are discussed Watchdog & Pathrater. Watchdog detect the misbehaving node through neighbor monitor. If any node drop the packet then it act as a selfish node. Pathrater mechanism give the rate to path according to packet drop or forward to the next node. Watchdog detect the selfish node but it has many drawbacks.	Throughput Increase, Overhead increase
7	Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks	2010, IEEE	This paper proposed two techniques which is the improved version of the Watchdog detection technique. The Warning Mode (WM) operation is proposed to prevent false accusations caused by radio and packet collision errors. In the RFM mode, if a link failure is detected, the rating of the relay node is reset to 0.5, i.e. the initial rating assigned to a node that becomes known for the pathrater for the first time and the number of faults is reset to 0.	Increase overall network performance, Decrease number of incorrect accusations, PDR increase

8	SORI	2004, IEEE	Authors propose a Secure and Objective Reputation-based Incentive (SORI) scheme to encourage packet forwarding and discipline selfish behavior. Different from existing schemes, under our approach, the reputation of a node is quantified by objective measures, and the propagation of reputation is efficiently secured by a one-way-hash-chain-based authentication scheme. Armed with the reputation-based mechanism, we design a punishment scheme to penalize selfish nodes. The experimental results show that the proposed scheme can successfully identify selfish nodes and punish them accordingly.	Reduced overhead, Increased throughput
10	CORE	2002, CMS	CORE (COllaborative Reputation instrument), has a watchdog component. However it is complemented by a reputation mechanism that differentiates between subjective reputation, indirect reputation, and functional reputation, which are weighted for a combined reputation value that is used to make decisions about cooperation or gradual isolation of a node. CORE permits only positive secondhand information, which makes it vulnerable to spurious positive ratings and misbehaved nodes increasing each other's reputation.	

Table 2. Survey Table

VI. PERFORMANCE PARAMETER ANALYSIS

In order to validate analysis in result we have conducted a simulation experiment. We have used NS2 network simulator version 2.35. Table shows the parameter used in our experiments. Here we used random way point mobility model. An extensive simulation model having scenario of n (user defined) mobile nodes. Here we implement the selfish AODV that is S_AODV protocol. When nodes have very less energy at that time it drop the packets and save the energy which is used for their own use. To implement the S_AODV protocol we change the aodv.cc & aodv.h file. After implementing the S_AODV protocol we compare its performance parameter like throughput, Goodput, PDR & end to end delay with original AODV protocol. Below graphs show this comparison result. From this graph we conclude that performance parameter Throughput, Goodput & PDR decrease when there is selfish node in the network and End to End delay increase when there is selfish node in the network.



Parameter	Value
Channel Type	Wireless channel
Network Interface	Phy/Wirelessphy
MAC Type	Mac/802_11
Antenna Model	Omni antenna
Routing Protocol	AODV
Link Layer Type	LL
X & Y Dimension Of Topology	500 * 500
Radio Propagation Model	Propagation/Two ray ground
Simulation time	100 s

Table 3. Simulation Parameter

- **Throughput**

Throughput is a measure of the date rate (bits per second) generated by the application. It is defined as the average no of packet received by the destination node per second. Throughput is equal to the total data transferred divided by the total time it took for the transfer.

$$\text{Throughput (kbps)} = \frac{\sum(\text{Packet Size})}{(\text{Packet Arrival Time} - \text{Packet Start Time})}$$

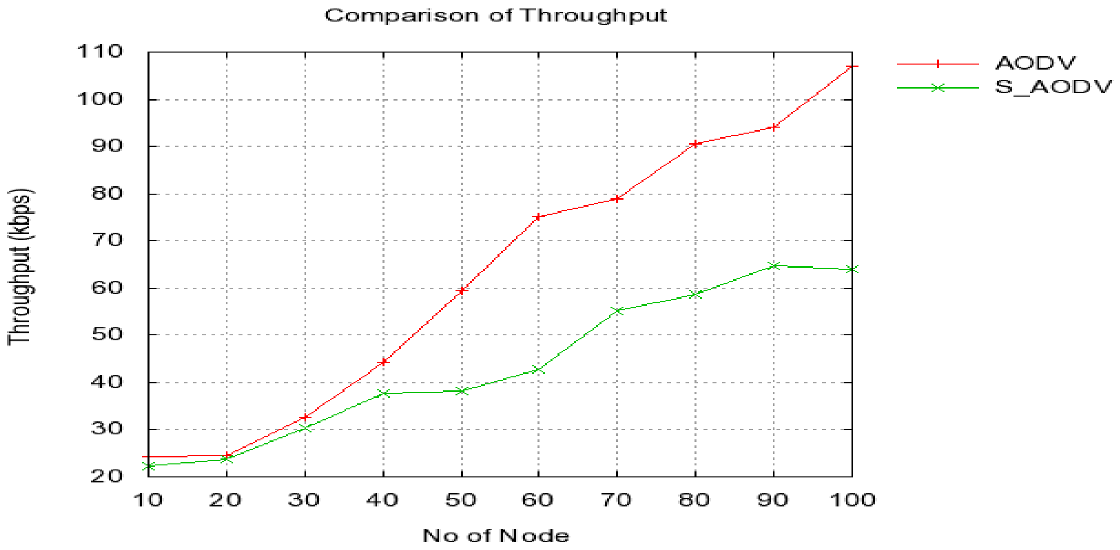


Figure 4. Compare Throughput of AODV with S_AODV

- **PDR**

Packet delivery ration is the ratio of the total number of packet received by destination to total number of packet sent by source.

$$\text{PDR (\%)} = \frac{\sum(\text{Number of packet received})}{\sum(\text{Number of packet sent})}$$

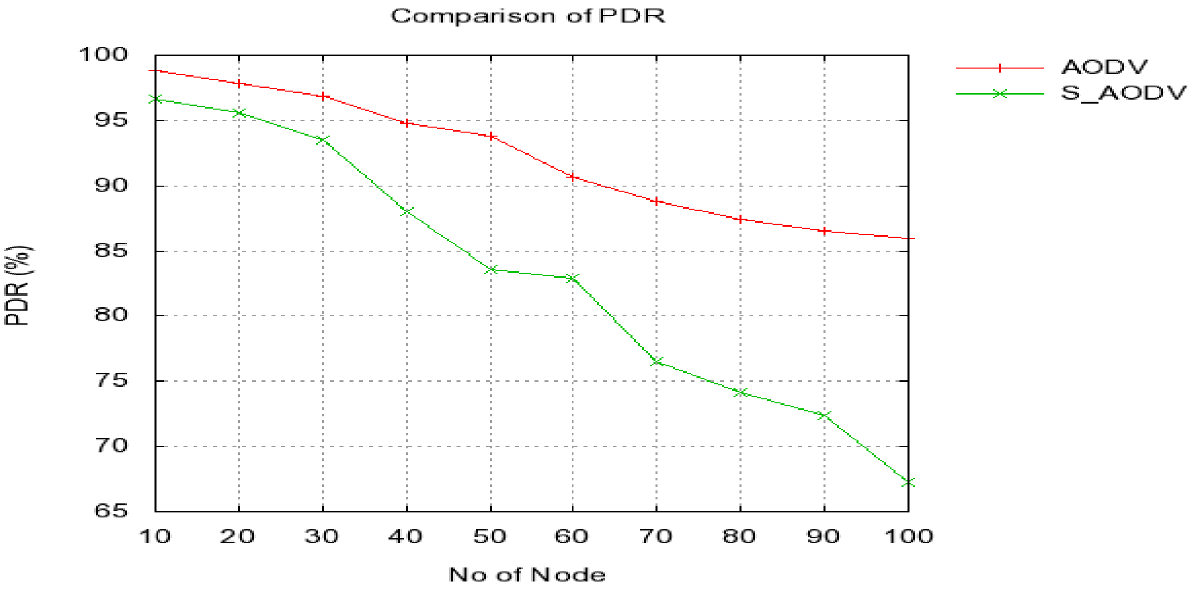


Figure 5. Compare PDR of AODV with S_AODV

- **Goodput**

Goodput is a measure of the date rate (bits per second). Goodput measurement will always be less than or equal to the throughput.

$$\text{Goodput (kbps)} = \frac{\sum(\text{Size of transmitted file} - \text{Size of Header file})}{(\text{Packet Arrival Time} - \text{Packet Start Time})}$$

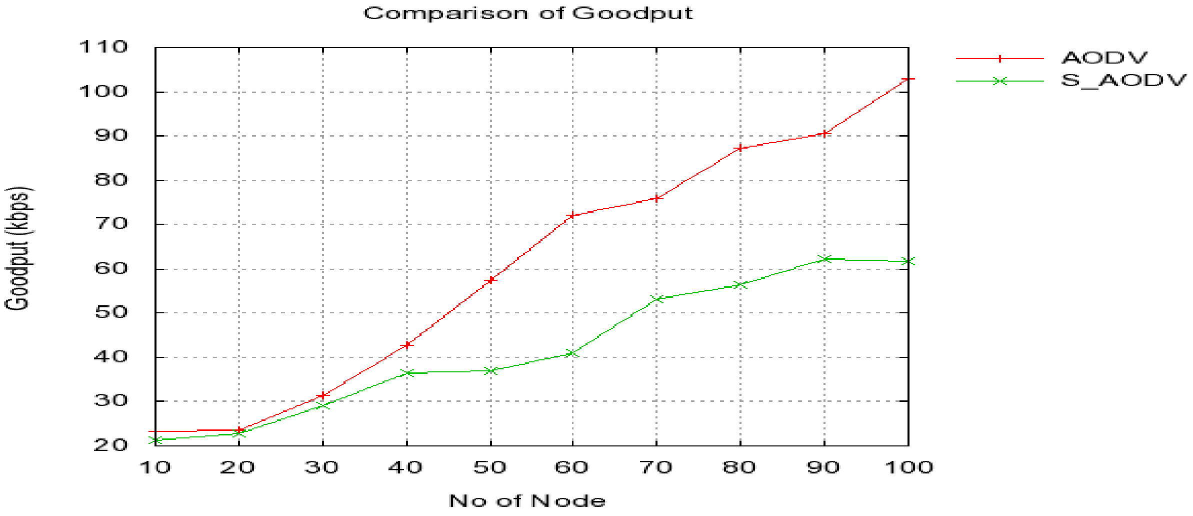


Figure 6. Compare Goodput of AODV with S_AODV

- **End to End Delay**

It is defined as time taken for packet to reach the destination from the source node.

$$\text{End to End Delay (ms)} = \frac{\sum(\text{Delay of each entities data packet})}{\text{Total number of deliverd packet}}$$

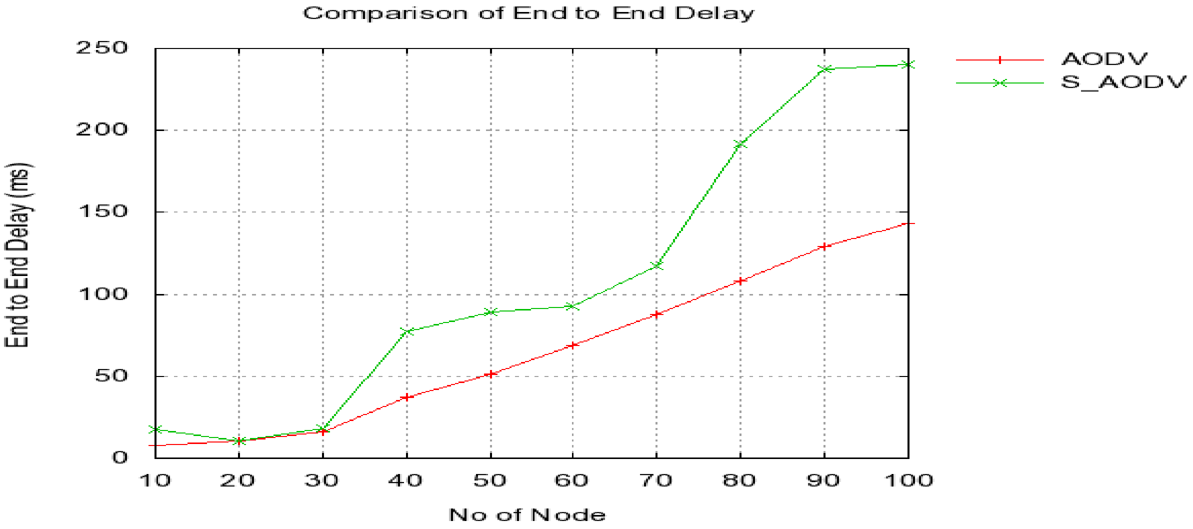


Figure 7. Compare End to End Delay of AODV with S_AODV

VII. CONCLUSION AND FUTUREWORK

In mobile ad hoc network some nodes are not cooperate in the network because they have limited Resources and life time. They save the resources for their own use, these nodes are called the selfish node. Here we discussed about the no of techniques to avoid the selfishness attack. After implementing the selfish ness attack in ns2.35 and compare it with the original AODV protocol and conclude that presence of selfish node in the network decrease the performance of the network by decreasing the throughput, goodput and PDR. In future we make a new mechanism to detect the Selfish node and prevent from it and also increase the performance of the network.

REFERENCES

[1] Rashid Sheikh, Mahakal Singh Chandee, Durgesh Kumar Mishra “Security Issues in MANET: A Review” 7th International Conference on Wireless And Optical Communications Networks (WOCN), December, IEEE 2010

[2] Datuk Prof Ir Ishak Ismail, Mohd Hairil Fitri Jaafar “Mobile Ad Hoc Network Overview” Asia-Pacific Conference On Applied Electromagnetics Proceedings, IEEE 2007

[3] Priyanka, Vinti, Rahul “ MANET: Vulnerabilities, Challenges, Attacks, Application” International Journal of Computational Engineering & Management, Vol. 11, January 2011

[4] Josh, Ayyaswamy, Namaskaram, Perumal, Subramaniam “A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT” EURASIP Journal on Wireless Communications and Networking, Springer 2015

[5] Vijayakumar.Aa, Selvamani Kb, Pradeep kumar “Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks” International Conference on Intelligent Computing, Communication & Convergence (ICCC), April 2015

[6] Senthilkumar, William, Subramaniyan “A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique” EURASIP Journal on Wireless Communications and Networking, Springer 2015

[7] T.V.P.Sundararajan, Dr.A.ShanmugamPerformance “Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks” ICGST-CNIR Journal, Vol. 9, Issue 1, July 2009

[8] N.Sridivya, I.Sibiya, D.Suvitha, A.Ashokraj “ Intrusion Detection Of Selfish And Malicious Nodes In Manets” NCRACCESS 2015

[9] Sergio marti, t.J. Giuli, kevin lai, and mary baker “Mitigating Routing Misbehavior In Mobile Ad Hoc Networks” International Conference on Mobile Computing & Networking ACM, 2000

[10] Alberto Rodriguez-Mayol, Javier Gozalvez “Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks” IEEE October 2010.

[11] Qi He, Dapeng, Pradeep Khosla “SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks” WCNC IEEE Communications Society 2004

[12] Pietro, Refik “CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks” Sixth IFIP conference on security Communication & Multimedia, CMS 2002

[13] S.Senthilkumar, J.William “A Survey On Reputation Based Selfish Node Detection Techniques In Mobile Ad Hoc Network” Journal of theoretical and applied information technology, Vol. 60 No.2 February 2014

[14] Gaurav Soni, Kamlesh Chandrawanshi “A Novel Defence Scheme Against Selfish Node Attack In MANET” International Journal on Computational Science & Application Vol. 3, No.3, June 2013

[15] Alberto Rodriguez-Mayol &Javier Gozalvez “Reputation based selfishness prevention techniques for mobile ad-hoc networks” TELECOMMUNICATION SYSTEMS, October 2014

[16] Amir Khusru Akhtar, G. Sahoo “Classification of Selfish and Regular Nodes Based on Reputation Values in MANET Using Adaptive Decision Boundary ” Communications and Network, August 2013

[17] Sagar Padiya1, Rakesh Pandit2 & Sachin Patel “Survey Of Innovated Techniques To Detect Selfish Nodes In Manet” International Journal Of Computer Networking, Wireless And Mobile Communications (Ijcnwmc) Vol. 3, Issue 1, Mar 2013

[18] Hemang Kothari and Manish Chaturvedi “ Effect of Selfish Behavior on Power Consumption in Mobile Ad Hoc Network” Proceedings of the Asia-Pacific Advanced Network – APAN, Vol. 32, 2011

[19] Martin schütte “detecting selfish and malicious nodes in manets” Seminar: sicherheit in selbstorganisierenden netzen, hpi/universität potsdam, 2006

[20] Joni Birla, Basant Sah “Performance Metrics in Ad-hoc Network” International Journal of Latest Trends in Engineering and Technology Vol. 1 Issue 1 May 2012