PERFORMANCE ANALYSIS IN COMPARISON OF CONVENTIONAL AODV AND GNDA

Ibrahim khider*

Khalid hamid**

ABSTRACT

Ad hoc Networks are variety of mobile nodes connected wireless without base station. In ad hoc networks, routes may be disconnected due to movement of nodes so route and topology are very difficult and challenging issues.In this paper, the effect of bad neighbor nodes in ad hoc routing is discussed and a method called Good Neighbor node Detection Algorithm (GNDA) is studied and reviewed. Ad hoc on-demand Distance Vector (AODV) supported with GNDA and conventional AODV are compared based on important performance metrics such as delay,throughput ,packet delivery ratio and routing load . Finally suitable results are obtained in different scenarios and the significant performance enhancement achieved..

Keywords: MANET, AODV, GNDA, Simulation.

* Sudan University of science and technology

** University of science and technology

1. Introduction

A Network is defined as the group of people or systems or organizations who tend to share their information collectively for their business purpose. In Computer terminology the definition for networks is similar as a group of computers logically connected for the sharing of information or services (like print services, multi-tasking, etc.). Initially Computer networks were started as a necessity for sharing files and printers but later this has moved from that particular job of file and printer sharing to application sharing and business logic sharing. Computer networks can be defined as a system for communication between computers. These networks may be fixed (cabled, permanent) or temporary. A network can be characterized as wired or wireless. Wireless can be distinguished from wired as no physical connectivity between nodes is needed. [1] Wireless technology, cellular or wireless LANs, is growing very fast and widely used. It can be found everywhere in universities, offices, and public areas.

The standard IEEE 802.11 defines two services in Wireless Local Area Networks (WLANs): Basic Service Set (BSS) and Extended Service Set (ESS). The Basic Service Set is wireless LAN with size of a building. It consists of mobile and stationary nodes and an optional device, called Access Point (AP). The BSS without an AP is called ad hoc and with an AP is an infrastructure. The ESS is formed by connecting two or more infrastructures, through a wired LAN (Distribution System). [2]

Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes [1]. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

2. Related work

Securing ad hoc routing protocols has become of critical importance so that several researchers have studied the problem of secure ad hoc network. Many papers and thesis have been published in this field. [3] identifies the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, the authors take advantage of the inherent redundancy in ad hoc networks — multiple routes between nodes — to defend routing against

denial of service attacks. They also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of their security framework. In [4] the authors has proposed improved neighbor detection algorithm for AODV routing protocol by using concept signal to noise ratio. The authors of [5] has discussed hop count based routing for providing life time link stability for residual lifetime of a link. [6] has suggested a method to decide to number of necessary nodes by considering size and transmission range of a network. [7] has analyzed that frequent interrupting of neighbor nodes can produce transmission delay and low quality in terms of data transfer. Cao Minh Trang [8] has suggested an effective approach for an intrusion detection system in AODV routing protocol. But this approach was not suitable against impersonation attack and also its accuracy decreases in case of high mobility. [9] presents a proposer to develop an Energy Efficient Secure Authenticated Routing Protocol (EESARP) for mobile adhoc networks, that uses a lightweight, attack resistant authentication mechanism. The protocol provides efficient security against route discovery attacks using hop-by-hop signatures. It quickly detects the malicious nodes, thus assisting the nodes to drop the invalid packets, earlier. It also uses an efficient node selection mechanism which maximizes network life time and minimizes delay. [10] provides a solution to detect malicious nodes normally operate during determination of a route over but modifies or drop data during data transmission or report wrong information regarding a normal node, using a report message and a report table that list reporter nodes and suspect nodes in AODV-based Mobile Ad Hoc Networks (MANETs). [11] describes a unified network-layer security solution in ad hoc networks, which protects both routing and packet forwarding functionalities in the context of the AODV protocol. To address the unique characteristics of ad hoc networks, the authors take a self-organized approach by exploiting full localized design, without assuming any a priori trust or secret association between nodes. In [12] an approach is proposed to combat the Cooperative/ Multiple Black-hole attack by using negotiation with neighbors who claim to have a route to destination. As the authors claimed, the Simulation's results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and overhead. [13] presents four new mechanisms as tools for securing distance vector and path vector routing protocols. For securing distance vector protocols, a hash tree chain mechanism forces a router to increase the distance when forwarding a routing table entry. For securing path vector protocols, a cumulative authentication mechanism authenticates the list of routers on the path in a routing update, preventing removal or reordering of the router addresses in the list; the mechanism uses only a single authenticator in the routing update rather than one per router address.an approach so as to increase the performance of network rapidly by considering good nodes into the account. The classification of good and bad nodes depend on

signal strength and the flow capacity of nodes. The performance evaluation can be achieved using AODV routing protocol.

3. Good Neighbor nodes Detection Algorithm (GNDA)

In GNDA performance of network increases by take good nodes into the account. Classifications of good and bad nodes rely on signal strength and flow capacity of nodes. Furthermore, how rapid each node can receive the full information. In AODV, two nodes are said to be neighbors if the received transmission power of one of them and exceeds some given maximum power threshold. It has been analyzed that performance of ad hoc network gradually decreases due to transmission range of node is larger than transmission range of network, neighbor node is flooding unnecessary reply request messages to other nodes, time is high to reach hello messages between two nodes and packet dropping ratio of a neighbor node is maximum. All these four cases show that presence of any one case decreases performance of on demand routing protocol. In GNDA, all nodes have their own transmission range. Firstly, transmission range of each node present in the network is compared with the total transmission range of the network. Determination of transmission power is obtained to send a message between two neighbors. It can be measured by calculating the received power of hello message. When node receives hello messages from a neighbor node, it can estimate the minimum power level needed to reach its neighbor by comparing the received power of hello message with maximum transmit power. GNDA is improved by adding parameters in the neighbor table such as flow capacity; signal strength into the neighbor table based on their transmission range.GNDA is best solution for finding good nodes. Classification of nodes is based on performance metrics (transmission range and power of node, signal strength, capacity of node for high packet forwarding and relative position of node). Neighbor routing table maintains address of node for maintaining record of the entire nodes. These stored nodes are used for data transmission and forwarding. Any node can forward data to other node if they exist within the transmission range of the network. , location of node can be verified by using routing table.

4.Simulation Environment

Neighbor node detection in mobile ad hoc network is identified and its results' are compared with existing AODV routing protocol using ns-2.34 on linux platform (Ubuntu 10.10). Initially it has been assumed that all nodes have their own transmission range with dynamic movement.

Mobility models were created for the simulations using Random WayPoint Mobility Model (RWPMM) with 25 and 50 nodes, pause times of 0,10,20,30,40,50,60,70,80,90,100 seconds, maximum speed of 20m/sec, topology boundary of 500x500 m^2 and simulation time of 100secs.Random traffic connections

of TCP and CBR can be setup between mobile nodes using a traffic-scenario generator script. For the simulations carried out, traffic models were generated for 25 and 50 nodes with CBR traffic sources, with maximum connections of 25 and 50, respectively, at a rate of 4kbps. A simulation scenario is carried out using GNDA and AODV with the simulation parameters, shown in Table 1.the performance matrices are include packet delivery ratio, routing overhead ,end to end delay and throughput.

Table 1: Simulation parameters

Parameter	**Value**
Platform	Ubuntu 10.10
Simulator	ns-2.34
Simulation time	100 sec
Terrain area	500*500 m^2
Number of nodes	25, 50
Node maximum speed	20 m/sec
Mobility Model	RWPMM
Propagation Model	Two-Ray Ground
Antenna type	Omni-directional
Transmission range	250m
MAC layer protocol	IEEE 802.11
Traffic	CBR
Packet size	512 Byte
Packet rate	4 packets/sec
Routing protocol	AODV, GNDA

5.Results and Discussion

The simulation results are shown in the following section in the form of graphs. The performance of AODV and GNDA, based on the varying the number of nodes (25 and 50 nodes), is done on parameters like PDR and throughput.Figure.1 highlights the PDR performance metric of AODV and GNDA with 25 nodes. Figure 2, highlights the PDR performance metric of AODV and GNDA with 50 nodes. From figures 1 and 2, it is observed that AODV delivers lesser percentage of the originated data (70% - 98%) than GNDA (98% - 100). Also it is observed that the PDR of GNDA becomes lesser with increasing the number of nodes.Figure 3 highlights the average end-to-end delay performance metric of AODV and GNDA with 25 nodes. Figure 4 highlights the end-to-end delay performance metric of AODV and GNDA with 50 nodes.

From figures 3 and 4, it is observed that AODV has a greater end-to-end delay (15 – 57 msec) than GNDA (11 – 40 msec). Also it is observed that the end-to-end delay of both protocols, AODV and GNDA, becomes greater with increasing the number of nodes.Figure5 highlights the normalized routing load performance metric of AODV and GNDA with 25 nodes. Figure6 highlights the normalized routing load performance metric of AODV and GNDA with 50 nodes.From figures 5 and 6, it is observed that AODV has a greater normalized routing load value (0.24 – 0.7) than GNDA (0.22 – 0.37). Also it is observed that the normalized routing load value of AODV becomes greater with increasing the number of nodes. In the other side, increasing the number of nodes has a little effect on GNDA.Figure 7 highlights the throughput performance metric of AODV and GNDA with 25 nodes.From figures 7 and 8, it is observed that AODV always has lesser throughput than GNDA. Also it is observed that throughput of both protocols, AODV and GNDA, becomes greater with increasing the number of nodes. This is due to the increased sent data over the network.

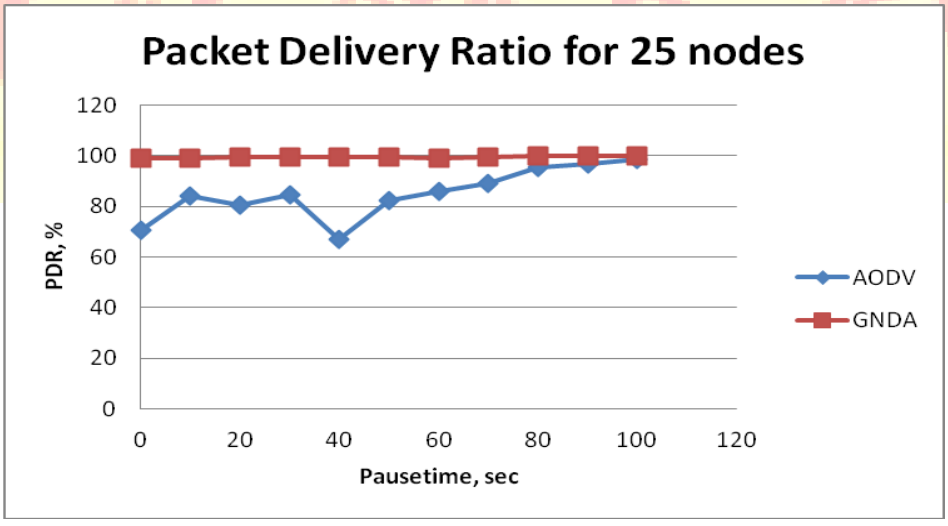

Figure 1: Packet Delivery Ratio versus Pause-time for 25 nodes

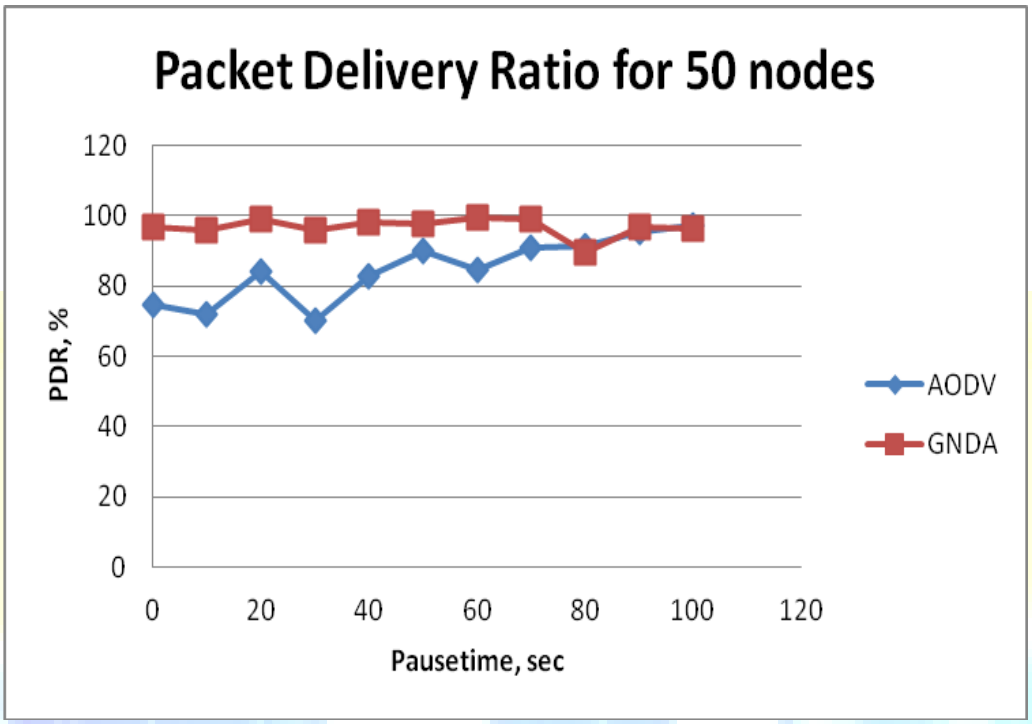

Figure 2: Packet Delivery Ratio versus Pause-time for 50 nodes

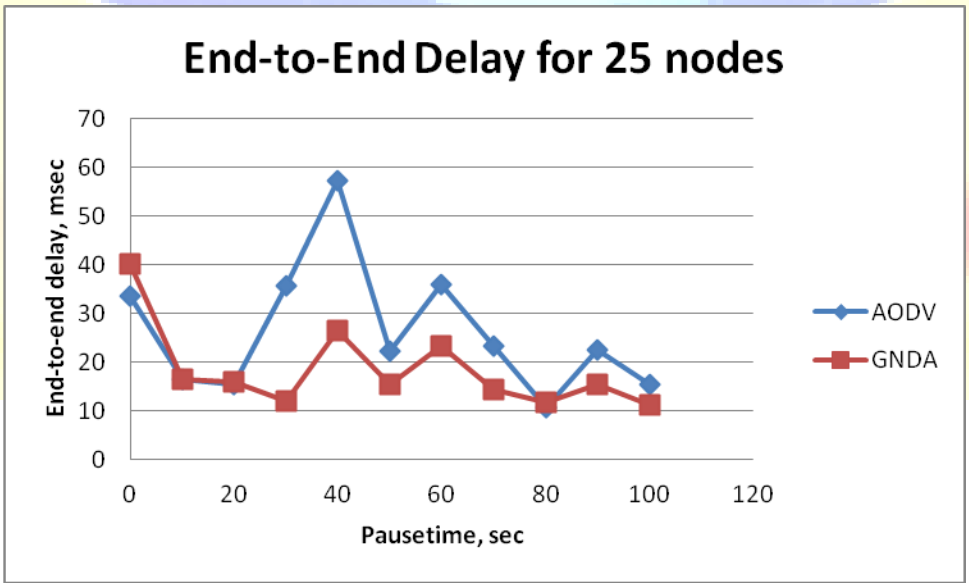

Figure 3: End-to-End Delay versus Pause-time for 25 nodes

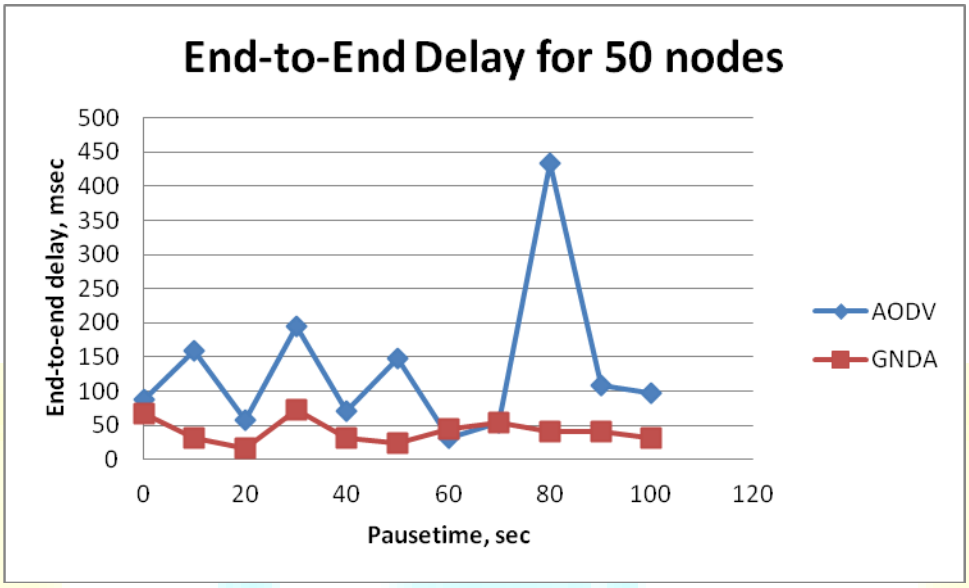

Figure 4: End-to-End Delay versus Pause-time for 50 nodes

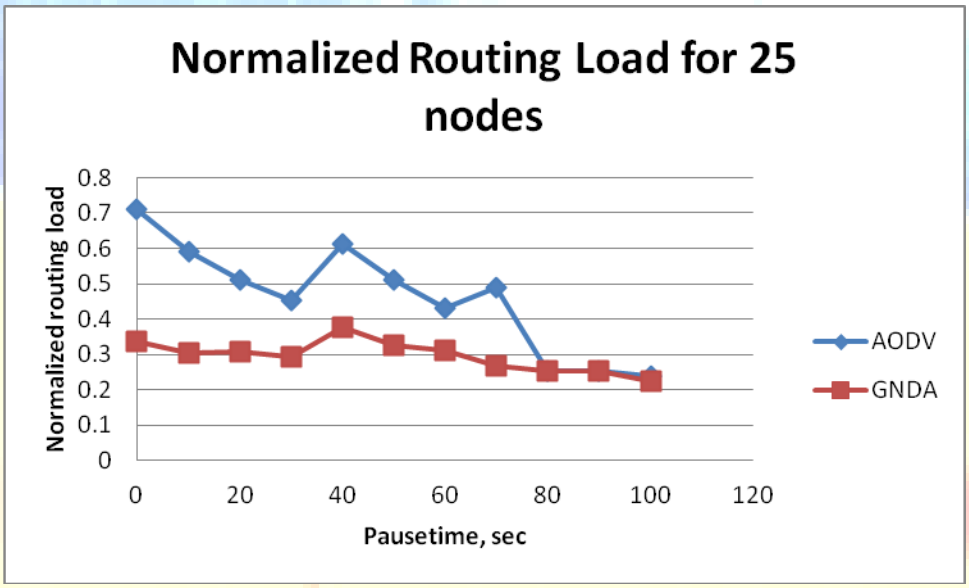

Figure 5: Normalized Routing Load versus Pause-time for 25 nodes

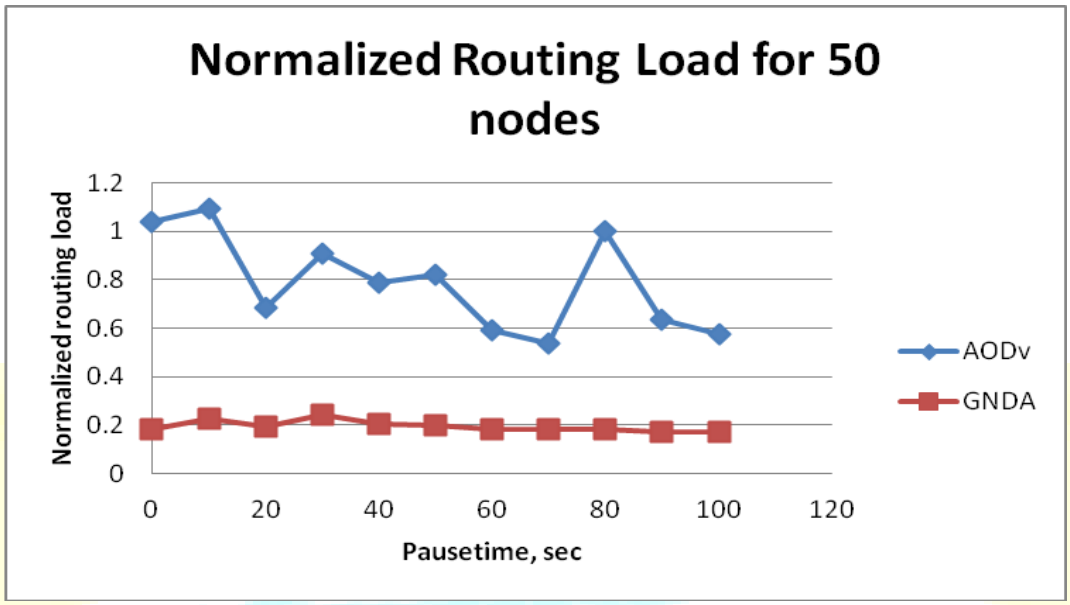

Figure 6: Normalized Routing Load versus Pause-time for 50 nodes

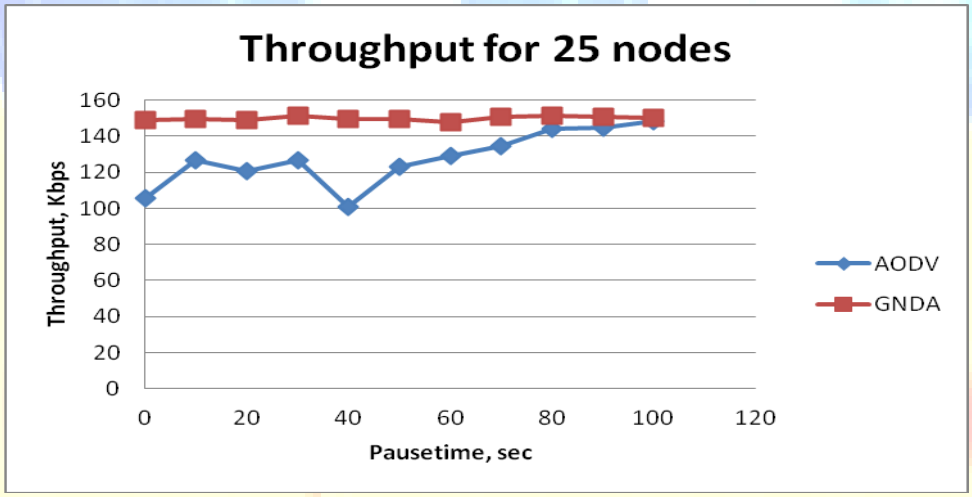

Figure7: Throughput versus Pause-time for 25 nodes

Figure 4-15 highlights the throughput performance metric of AODV and GNDA with 50 nodes

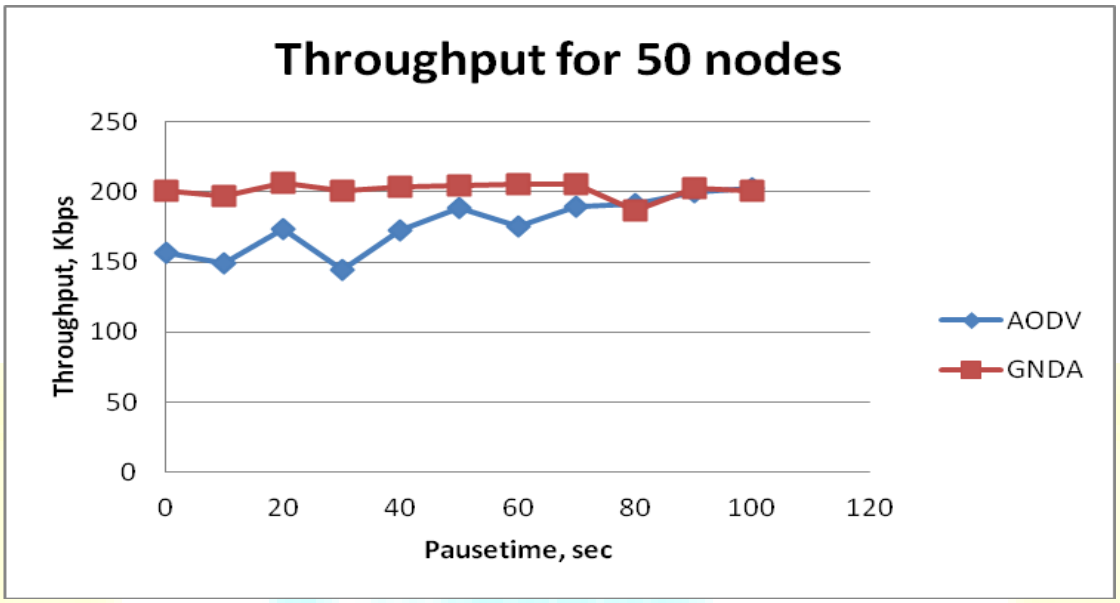

Figure 8: Throughput versus Pause-time for 50 nodes

6. Conclusion

This paper presented the effects of bad and good neighbor nodes in ad hoc routing . GNDA is an optimal solution for finding good nodes. Neighbor routing table maintains address of node for maintaining record of the entire nodes. These stored nodes are used for data transmission and forwarding. This approach minimizes energy consumption of node and increases its battery life. Thus any node can forward data to other node if they exist within the network range. .The evaluation of GNDA and AODV are conducted on a linux platform (Ubuntu 10.10) using ns2.34. The simulation results have shown that GNDA always has good performance over AODV

References:

[1] Krishna Gorantala ,"Routing Protocols in Mobile Ad-hoc Networks", UMEA University, Department of Computing Science, SE-901 87 UMEA, SWEDEN, June 15, 2006.

[2] Behrouz A. Forouzanwith Sophia Chung Fegan, "Data Communications and Networking", forth edition, Mc Graw Hill.,2007.

[3] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks", Department of Computer Science, School of Electrical Engineering, Cornell University Ithaca, NY ,1999.

[4] Srdjan Krco and Marina Dupcinov, "Improved Neighbor Detection Algorithm for AODV Routing Protocol", IEEE COMMUNICATIONS LETTERS, VOL. 7, NO. 12, DECEMBER 2003

[5] Sridhar K N and Mun Choon Chan, "Stability and Hop-Count based Approach for Route Computation in MANET", IEEE, 2005.

[6] Youngrag Kim, Shuhrat Dehkanov, Heejoo Park, Jaeil Kim, Chonggun Kim, "The Number of Necessary Nodes for Ad Hoc Network Areas ", IEEE Asia-Pacific Services Computing Conference, 2007.

[7] Qing Li, Cong Liu, Hang Hong Jiang, "The Routing Protocol of AODV Based on Link Failure Prediction", ICSP2008 Proceedings, 2008 .

[8] Cao Minh Trang, Hyung- Yun Kong, Hong Hee Lee, "A Distributed Intrusion Detedtion System For AODV", 2006.

[9] M. Rajesh Babu and S. Selvan, "An Energy Efficient Secure Authenticated Routing Protocol for Mobile Adhoc Networks", American Journal of Scientific Research , pp.12-22 Issue 9(2010).

[10] Jongoh Choi, Si-Ho Cha , GunWoo Park, and JooSeok Song, "Malicious Nodes Detection in AODV-Based Mobile Ad Hoc Networks", GESTS Int'l Trans. Computer Science and Engr., Vol.18, No.1,2005

[11] Hao Yang, Xiaoqiao Meng, Songwu Lu, "Self-Organized Network-Layer Security in Mobile Ad Hoc Networks" Department of Computer Science University of California, Los Angeles, WiSe'02, September 28, 2002.

[12] Mehdi Medadian, Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol", European Journal of Scientific Research Vol.69 No.1 , pp.100-110, 2012

[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Efficient Security Mechanisms for Routing Protocols. Network and Distributed SystemSecurity Symposium, NDSS '03, San Diego, USA, , 57-73, 2003