THE IMPACT OF NODE MISBEHAVIOR ON THE PERFORMANCE OF ROUTING PROTOCOLS IN MANET

Khaled Ahmed Abood Omer

Computer Science and Engineering Department, Faculty of Engineering/ University of Aden, Yemen

ABSTRACT

MANET is a cooperative wireless network in which mobile nodes are responsible for routing and forwarding packets from and to other nodes. Noncooperation is a challenge that definitely degrades the performance of MANET. A misbehaving or selfish node may make use of other nodes in the network, but decline to share its own resources with them. These selfish nodes may severely affect the performance of routing protocols in MANET.

In this paper, we compare the performance of four routing protocols under security attack of node misbehavior in MANET. We investigate AODV and DSR reactive routing protocols and OLSR and GRP proactive routing protocols using Riverbed Modeler simulator. The performance comparison is carried out using two types of misbehaving nodes. The metrics used are End-to-End delay, Packet Delivery Ratio, Data dropped and the Load. The experimental results show that AODV routing protocol performs better than the other routing protocols with higher packet delivery ratio. Further, OLSR routing protocol outperforms the other routing protocols with minimum End-to-End delay.

KEYWORDS

AODV, DSR, GRP , OLSR, Selfish Nodes, MANET.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are wireless networks without a predefined infrastructure, such that the nodes can communicate with each other directly without the requirement of support station. MANET consists of mobile wireless nodes that move randomly and form dynamic topologies. MANET is an autonomous system where each node operates as an end system and also as a router to forward packets from source node to destination node in the network. Therefore routing and network management are done cooperatively by all the nodes in the network. MANET networks are considered as challenging networks for communication due to its limited resources and many changes in the network topology.

Routing protocols used in MANETS are classified into three categories named as proactive or table driven, reactive or on demand and hybrid routing protocols. These routing protocols are designed such that all nodes participate willingly to forward data and control packets among the nodes in the network [1, 2].

Due to lack of a defined central authority in MANET networks, then securing the routing process becomes a challenging task thus leaving MANETs vulnerable to attacks. Further, the nature of the open structure and narrowly available battery-based energy, node misbehaviors may exist. A

DOI : 10.5121/ijcnc.2016.8209

misbehaving or selfish nodes may attempt to benefit from resources of other nodes, but refuse to share its own resources. However, the existence of misbehaving or selfish nodes in the network, may result in decreasing the network performance significantly [3].

This paper is organized as follows: In section 2, related work about routing protocols and misbehaving nodes are discussed. Section 3 includes simulation environment. Section 4 describes results and discussions. Finally the findings of the work are concluded in section 5.

2. ROUTING PROTOCOLS AND MISBEHAVING NODES

Routing protocols used in MANETS are classified into three categories named as proactive, reactive and hybrid routing protocols. Proactive or table driven routing protocols such as Optimized Link State Routing (OLSR) and Geographic Routing Protocol (GRP) protocols. In these routing protocols, the routes to all the nodes are maintained in routing table. Packets are sent over a predefined route specified in the routing table. Reactive or on-demand routing protocol such as Dynamic Source Routing (DSR) and Ad Hoc On Demand Distance Vector (AODV). In these routing protocols, the routes are not predefined for routing. A source node initiates route discovery phase to find a new route whenever there are packets to be sent to destination. The grouping of proactive and reactive approaches results in hybrid routing protocols such as Zone Routing Protocol (ZRP) [1, 2, 4]. In this paper, we consider AODV, DSR, OLSR, and GRP routing protocols for further investigation under misbehaving or selfish node security attacks.

2.1 Routing Protocols

Ad-hoc On Demand Distance Vector (AODV) is a reactive routing protocol where the routes are discovered only on demand when there is a need to send packets to destination nodes [5]. The routing table is used to store the information about the next hop to the destination and a sequence number received from the destination which indicates the received information is updated. The information about the active neighboring nodes is received during the discovery of the destination. The route discovery is achieved by broadcasting the RREQ message to the neighbors with the requested destination sequence number, which prevents the old information from being sent back to the request and also prevents looping problem. Passed nodes update their own routing table about the requested node. Therefore, the path that identifies the route is recorded in the routing table of the intermediate nodes. The destination node creates the route reply by using RREP message to be sent back to the source. The source starts sending the packets to the destination after receiving the route reply message. When the corresponding route breaks, then the route error RERR message is used to inform the neighbors.

Dynamic Source Routing (DSR) is a reactive routing protocol that uses the concept of source routing [6]. In source routing the source knows complete hop-by-hop route to the destination. In this protocol, every node possess route cache to store recently discovered path such that route entries are continuously updated. When a source desires to send packets to destination, it first checks for the path in the cache. If the path is present, then the source attaches its source address to the packet and uses that path to transmit the packet. If the path is not available or expired, then the source node initiates route discovery by flooding RREQ packet to its neighbors asking for a path to destination. Each node appends its own address when forwarding RREQ. As the route request packet arrives to any of the nodes, the node checks its neighbors or its cache about the destination. The node sends back RREP packet to source if route information is known, otherwise the node broadcasts RREQ packet to its neighbors. Once route is discovered, then data packets are sent from source to destination and this route is stored in the cache for future use. The destination node sends RREP packet on receiving the first RREQ packet on the route obtained by

reversing the RREQ path. All routes used are assured to be free of loops since the source node can avoid duplicate hops in the selected routes.

Optimized Link State Routing (OLSR) is a proactive routing protocol, so the routes are always immediately available when needed to send packets in the network [7]. OLSR utilizes Multipoint Relays (MPR) to minimize the overhead in the network. OLSR uses Hello message to find the information about the link status and neighboring nodes in the network. TC message is used to periodically broadcast information about advertized neighbors including the MPR selector list. The Hello messages are sent only one hop away but the TC messages are broadcast throughout the entire network. Also Multiple Interface Declaration (MID) message is broadcast throughout the entire network only by MPRs to inform other hosts that the announcing host can have multiple OLSR interface addresses. Also Host and Network Association (HNA) message provides the external routing information for routing to the external addresses.

Geographic Routing Protocol (GRP) is a location-based routing protocol [8]. GRP is a proactive, distance-based, greedy algorithm which uses the Global Positioning System (GPS) to mark the location of each node in the network. GRP selects the next hop on the path as a node geographically closest to destination. The network area is divided into square quadrants for routing so that every four quadrants of the lower level form a quadrant of a higher level. GRP maintains routing tables based on the geographical positions of the nodes in the network. Now if the source and the destination nodes are located in the same quadrant then the source sends a packet to its immediate neighbor geographically closest to the destination. Similarly, the intermediate node forwards the packet to its immediate neighbor closest to the destination, until the packet reaches the destination. If source and destination are not located in the same quadrant then the source sends the packet to its immediate neighbor closest to the highest-level quadrant where the destination exists. As the packet crosses the quadrant boundaries the location information about the destination becomes more specific and finally the packet arrives at the destination's quadrant and is routed to destination using precise location information.

Gulati1M. K. et al compared the performance of proactive and reactive routing protocols AODV, DSDV, and DSR using the NS-2 simulator [9]. The metrics used to compare the routing protocols are packet delivery ratio, average end-to-end delay, throughput, jitter, normalized routing overhead and normalized MAC overhead. The performance comparison is achieved by varying mobility speed, number of nodes and data rate. The experimental results show that AODV performs optimally well among the routing protocols under consideration.

Aujla G. S. et al studied the performance of AODV, DSR, TORA, OLSR, and GRP routing protocols using OPNET simulator where regular nodes are considered only without any security attacks [2]. The simulation results showed that AODV performs better than other protocols for video conferencing for lower number of nodes, and OLSR can be used for high number of nodes. Further OLSR protocol showed best performance for email traffic. GRP performance is better for small number of nodes but the performance degrades with increase in number of nodes. TORA showed poor results in both scenarios followed by DSR. In both scenarios GRP and AODV are suitable for small number of nodes whereas OLSR is better for large number of nodes.

2.2 Misbehaving Nodes

Since there is no defined central authority in MANET network, then securing the routing process becomes a difficult task and thus leaving MANETs vulnerable to security attacks. These attacks result in deterioration in the performance characteristics and the reliability of such networks. The authors presented an overview of the routing protocols in MANET networks, the known routing attacks and the proposed countermeasures to these attacks in various works [3].

Identification of misbehaving nodes in MANET networks is important to detect security attack in the network. Selfish nodes do not intend to directly damage other nodes in the network, but they do not cooperate with other nodes and saving battery life for their own communications. But malicious nodes do not have priority to save battery life, but intend to harm and damage other nodes in the network [10]. As the nodes in MANET network are battery powered, then energy becomes a valuable and limited resource, that makes the role of selfish nodes draws more attention in MANET networks.

Vijithanand J. et. al. surveyed a number of methods that deal with the selfish behaviour of the nodes in MANET networks [11]. Selfish nodes are considered as a real problem for MANET networks since they affect the network performance. The authors compared the available methods for reducing the effect of selfish nodes in MANET networks.

Gupta S. et. al studied the effect of selfish nodes concentration on the quality of service in MANET networks [12]. The experimental results showed that up to a concentration level of 10%, selfish nodes do not have remarkable negative effect on the network performance. As the concentration of selfish nodes increases, QoS decreases and becomes poorer in the network.
Mishra M. K. et. al studied and compared the behavior of three routing protocols AODV DSDV, and DSR under security attack using ns-2 network simulator. The simulation is carried out using two types of node misbehavior [13]. The experimental results indicated that DSDV is the most robust routing protocol under security attacks as compared to the other two routing protocols. In addition, the results discovered that a proactive routing protocol reduces the effect of security attack by excluding the misbehaving nodes from the routing process in advance, and thus minimizing their effect.

Agrawal S. et. al. compared two reactive routing protocols AODV and DYMO using ns-2 network simulator. The simulation is conducted using varying speed of node mobility and varying degree of malicious nodes in the network [3]. They compared the two routing protocols by varying percentage of misbehaving nodes that drop packets in MANET. The simulation results showed that DYMO routing protocol outperformed AODV routing protocol, because the increase in the mobility speed of the nodes results in the increase of the latency and hence the Jitter for AODV protocol.

Rao P. V. V. et al. investigated the impact of selfish node on the performance of AODV routing protocol by varying simulation time through OPNET Modeler version 17.5 [14]. Experimental results revealed that the impact of selfish node on performance of the throughput degrades by 40 times of the original AODV throughput. Similarly, the delay is reduced by more than 1000 times.

3. SIMULATION ENVIRONMENT

In order to measure the impact of selfish or misbehaving nodes on MANET network performance, we use Riverbed Modeler Academic Edition 17.5 [15] to simulate the four routing protocols with two types of misbehaving nodes: Type-1and Type-2 as described below:

1) Type-1 : partially selfish node : this node participates partially in the communication for few nodes only in the network. In fact, the selfish node saves its own battery energy, thereby still contributing to network.
2) Type 2 : fully selfish node : this node practically does not participate in the communication and stays idle in the network. This type does not participate in the activities like packet forwarding, packet receiving, route discovery, and network maintenance.

Using Type-1 and Type-2 misbehaving nodes in our simulation, we evaluate the performance of AODV, DSR, OLSR and GRP routing protocols, where a certain percentage of nodes behave as selfish nodes and the remaining nodes being regular nodes.

The Simulation parameters used in our scenarios are shown in Table 1.

Table 1 Simulation Parameters

Network Parameters	Values
Number of Mobile Nodes	20
Number of Misbehaving Nodes	1, 2, 3, 4, 5
Simulation Time	30 minutes
Simulation Area	1500 m x 1500 m
Routing Protocols	AODV, DSR, OLSR, GRP
Data Rate	11 Mbps
Mobility Model	Random waypoint
Speed	10 m/s
Pause Time	10 seconds
PHY Char.	PHY 802.11g
Simulator	Riverbed Modeler 17.5

The performance metrics that are used for evaluating and comparing the impact of node misbehavior or selfish node attack on AODV, DSR, OLSR and GRP network performance are as follow:

1. Packet Delivery Ratio (PDR): This is the ratio of total data received to total data sent from source to destination. It measures the loss rate in the network. (PDR= data delivered to the destination /data sent out by the source)
2. Average End-to-End Delay: This is the average End-to-end delay time that a packet takes to traverse from the source node to the destination node in a MANET network in seconds, i.e. the time elapsed between the creation of the MANET packet at the source node and the delivery of the packet to the destination node.
3. Data Dropped: This represents the total number of packets discarded by all nodes in the network. The total size of higher layer data packets (in bits/sec) dropped by all the WLAN MACs in the network due to full higher layer data buffer, or the greater size of the higher layer packet than the maximum allowed data size defined in the IEEE 802.11 standard.
4. Load: It signifies the entire load (in bits/sec) submitted to wireless LAN layers by all higher layers by all nodes of the MANET network.

4. RESULTS AND DISCUSSION

In this section we illustrate and discuss the experimental results obtained by simulation for three scenarios as follows.

4.1 Different percentages of Selfish nodes Scenario

In this scenario we study the performance of the routing protocols under considerations by increasing the percentage of selfish nodes in the network, starting from all regular nodes (0% of selfish nodes) to five selfish nodes (25%) of 20 nodes of the network.

Figure 1 shows that the End-to-End Delay slightly increases with the increase of selfish nodes in the network. Further, DSR protocol has maximum delay and OLSR protocol has the minimum delay.

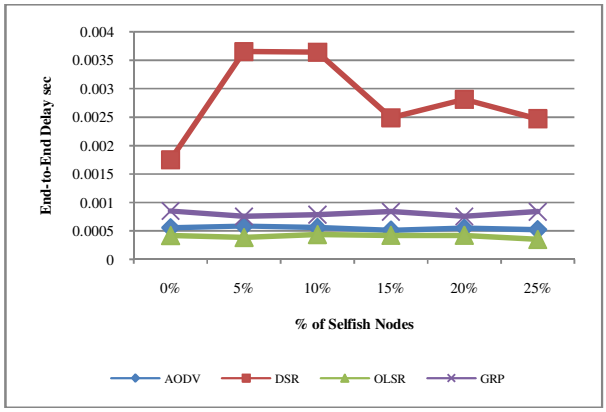

Figure 1 End-to-End Delay vs percentage of selfish nodes

Figure 2 shows that the data dropped (buffer overflow) increases with the increase of the percentage of selfish nodes in the network. It is clear that when there are no selfish nodes in the network, then the data dropped by all the routing protocols under consideration is zero. Also DSR protocol has higher data dropped compared to the remaining protocols, and OLSR protocol has the smaller data dropped.

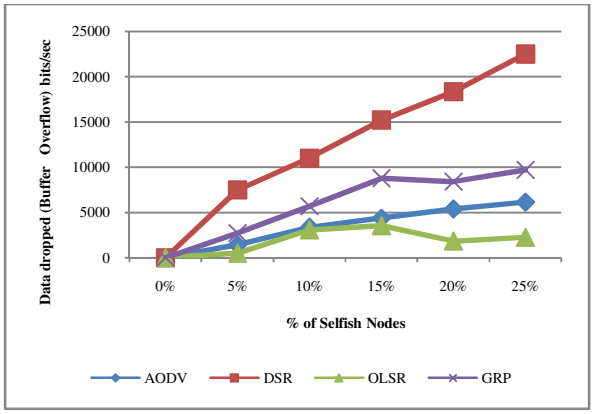

Figure 2 Data Dropped vs percentage of selfish nodes

Figure 3 shows that, the total load submitted to the network increases with the increase of the percentage of selfish nodes in the network . The figure shows that GRP protocol has maximum load compared to the other routing protocols, whereas OLSR protocol has the minimum load compared to the other routing protocols.

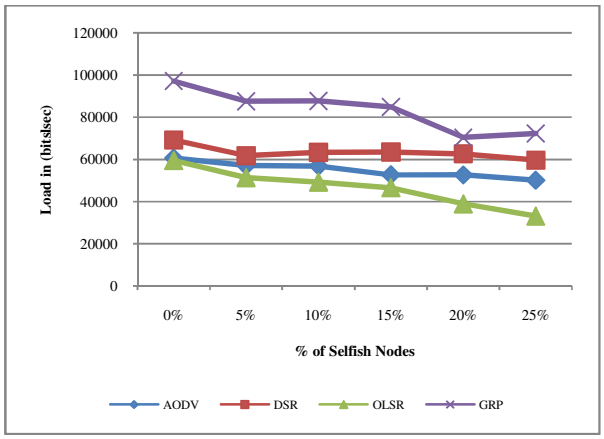

Figure 3 Load vs percentage of selfish nodes

Figure 4 describes that the packet delivery ratio that measures the loss rate in the network decreases with the increase of the percentage of selfish nodes. AODV protocol has the maximum Packet delivery ratio compared to the other protocols, whereas OLSR protocol has minimum Packet delivery ratio compared to the other protocols.

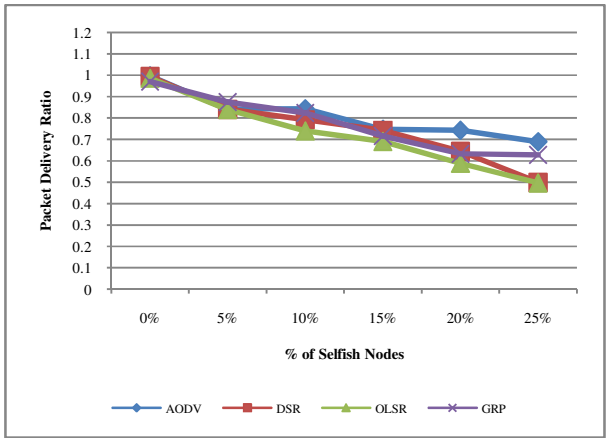

Figure 4 Packet Delivery Ratio vs percentage of selfish nodes

4.2 Impact of speed Scenario

In this scenario, we study the impact of increasing the speed of the mobile nodes on the performance of the routing protocols under investigation. We run the simulations for 10% selfish nodes in the network. One selfish node is of type-1 and the other one is of type-2 and the remaining nodes are regular nodes.

Figure 5 illustrates that the End-to-End delay increases with the increase of speed of the mobile nodes. DSR protocol has maximum End-to-End delay and OLSR has minimum End-to-End delay.

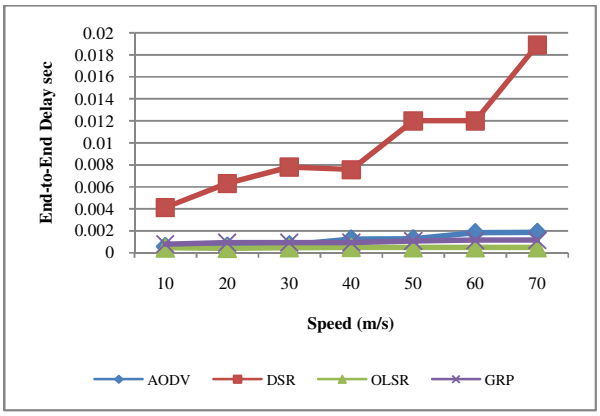

Figure 5 End-to-End Delay vs Speed

Figure 6 illustrates that the Packet delivery ratio slightly decreases with the increase of speed of the mobile nodes in the network. AODV protocol has maximum Packet delivery ratio and OLSR has minimum Packet delivery ratio.

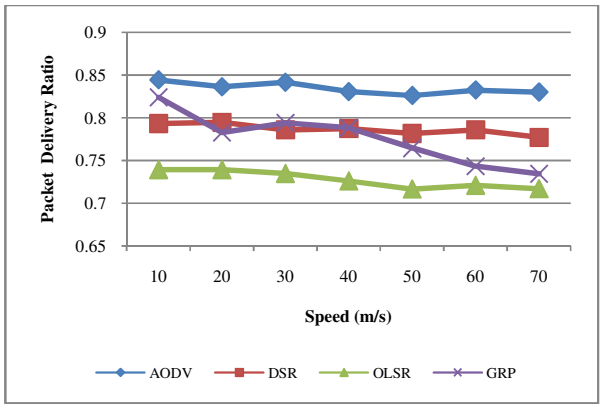

Figure 6 Packet Delivery Ratio vs. Speed

4.3 Impact of Pause Time scenario

In this scenario, we study the impact of increasing the pause time of the moving nodes on the performance of the routing protocols under consideration. We run the simulations for 10% selfish nodes in the network. One selfish node is of type-1 and the other one is of type-2 and the remaining nodes are regular nodes in the network.

Figure 7 illustrates that the End-to-End delay slightly increases with the increase of pause time of the mobile nodes. DSR protocol has maximum End-to-End delay and OLSR has minimum End-to-End delay.

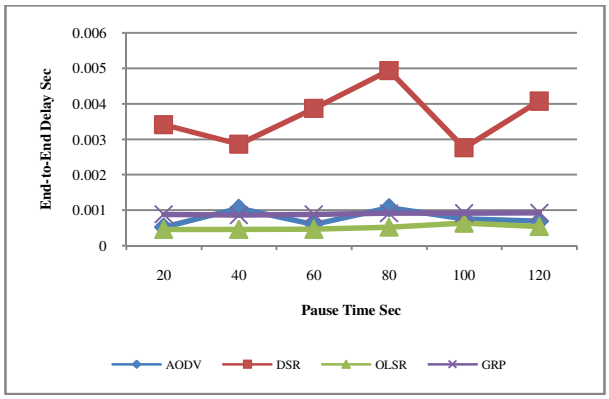

Figure 7 End-to-End Delay vs Pause Time in sec

Figure 8 illustrates that the Packet delivery ratio slightly decreases with the increase of pause time of the mobile nodes. AODV protocol has maximum Packet delivery ratio and OLSR has minimum Packet delivery ratio.

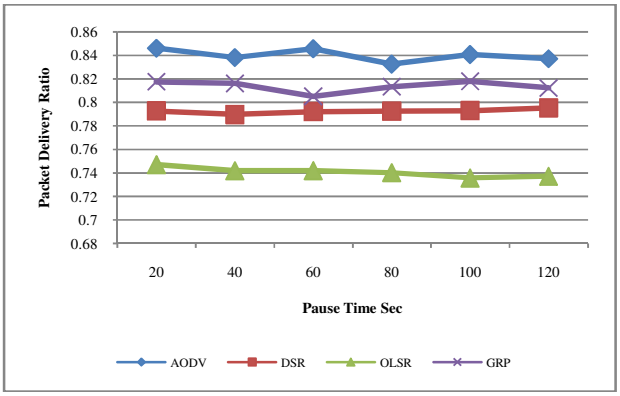

Figure 8 Packet Delivery Ratio vs. Pause Time in sec

5.CONCLUSION

In this paper, we have compared the performance of AODV, DSR, OLSR, and GRP routing protocols under the attack of node misbehavior using Riverbed modeler 17.5. This comparison is achieved by varying the number of selfish nodes in the MANET network, changing the speed of the mobile nodes, and varying the pause time of the mobile nodes.

The experimental results show that the performance of routing protocols under investigation is degraded with the increase of the percentage of misbehaving nodes in the MANET network. Further, the simulation results show that AODV routing protocol has higher packet delivery ratio while OLSR routing protocol has the smaller packet delivery ratio. Regarding to End-to-End delay, DSR protocol has maximum End-to-End delay and OLSR protocol has the minimum End-to-End delay.

REFERENCES

[1] M. Abolhasan, T. Wysocki and E. Dutkiewicz , (2004), " A review of routing protocols for mobile ad hoc networks", Elsevier Journal of Ad Hoc Networks, Vol. 2, No. 1, pp. 1-22.

[2] G. S. Aujla, S. S. Kang, (2013), "Comprehensive Evaluation of AODV, DSR, GRP, OLSR and TORA Routing Protocols with varying number of nodes and traffic applications over MANETs", IOSR Journal of Computer Engineering, Vol. 9, No. 3, pp. 54 -61.

[3] S. Agrawal, S. Jain, S. Sharma, (2011), "A Survey Of Routing Attacks And Security Measures In Mobile Ad-Hoc Networks", Journal Of Computing, Vol. 3, No. 1, pp. 41-48.

[4] P. Manickam, , T. Guru Baskar, M.Girija, Dr.D.Manimegalai, (2011), "Performance Comparisons Of Routing Protocols In Mobile Ad Hoc Networks", International Journal of Wireless & Mobile Networks, Vol. 3, No. 1, pp. 98-106

[5] C.E. Perkins and E.M. Royer, (1999), "Ad hoc on demand Distance Vector routing,", Proceedings. WMCSA '99. Second IEEE Workshop on mobile computing systems and applications, pp. 90 - 100.

[6] D. Johnson, D. A. Maltz, (1996), "Dynamic source routing in ad hoc wireless networks," in T. Imielinski and H. Korth,(eds.), Mobile Computing, (Kluwer Acad. Publ.,), pp. 152-181.

[7] T. Clausen and P. Jacquet, (2003), "Optimized Link State Routing Protocol (OLSR)." RFC 3626, IETF Network Working Group, October.

[8] Zhiyuan Li, (2009), "Geographic Routing Protocol and Simulation", Proceedings of International workshop on Computer Science and Engineering, pp. 404-407

[9] M. K. Gulati and K. Kumar, (2014), "Performance Comparison Of Mobile Ad Hoc Network Routing Protocols", International Journal of Computer Networks & Communications, Vol. 6, No.2, pp. 127-142.

[10] P. Michiardi and R. Molva., (2002), " Simulation-based analysis of security exposures in mobile ad hoc networks", In Proceedings of European Wireless Conference, pp. 107-121.

[11] J. Vijithanand, and K. S. Murthy, (2012), "A Survey on Finding Selfish Nodes in Mobile Ad Hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 3, No. 6, pp. 5454-5461.

[12] S. Gupta, C. K. Nagpal and Singla ., (2011), "Impact Of Selfish Node Concentration In Manets", International Journal Of Wireless & Mobile Networks 3(2), , 29-37.

[13] M. K. Mishra, B. K. Pattanayak, A. K. Jagadev, and N. Nayak, (2010), "Measure of Impact of Node Misbehavior in Ad Hoc Routing: A Comparative Approach", International Journal of Computer Science Issues, Vol. 7, No. 4, pp. 10-16.

[14] P. V. V. Rao, and S. P. Shetty, (2015), " Investigating the Impact of Selfish Node on AODV Routing Protocol in MANETs in the Context of Simulation Time", International Journal of Computer & Organization Trends , Vol. 21, No. 1, pp. 10-13.

[15] Riverbed Modeler Academic Edition 17.5, Riverbed Technologies: website www.riverbed.com

AUTHOR

Khaled Ahmed Abood Omer has done B.E Electrical & Electronics Engineering from Faculty of Engineering, Aden University, Aden, Yemen in 1994. He completed his M.Tech (Computer Engineering) from IIT Kharagpur, West Bengal, India in 1999. Also he completed his Ph. D. from SCSS, JNU, New Delhi, India in 2005. Currently he is working as an Associate Professor in Department of Computer Science at College of Sciences and Arts, Najran university, Sharurah, Saudi Arabia. His current research interests include Routing issues, Security issues, and performance evaluation of computer networks.