Indian Journal of Science and Technology, *Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/79928, December 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Efficient Secured Localization based Optimized Energy Routing for MANET

K. Vinoth Kumar[1]* and S. Bhavani[2]

[1]Karpagam University, Coimbatore - 641021, Tamil Nadu, India; vinodkumaran87@gmail.com
[2]Department of ECE, Karpagam University, Coimbatore - 641021, Tamil Nadu, India; bhavanisns@yahoo.com

Abstract

Background/Objectives: Secure Localization is a major issue in MANET which is mainly focusing on keeping confidential information about mobile nodes and data packets. Several approaches have been proposed to obtain location information and node authentication. However, it is some lagging in balancing energy consumption and location authentication. **Methods/ Statistical Analysis:** In this research, location based secure routing is proposed for location authenticity among mobile nodes. It contains three phases. In first phase, multipath route determination. In second phase, reliable nodes are chosen for packet forwarding towards destination node. In third phase, destination with secure location update is determined to secure nodes. **Findings:** For simulation, the network simulator tool (NS 2.34) is used. Based on the simulation result, the proposed work achieved that secured location authenticity and minimum energy consumption. **Applications:** This work can be suggested as real time approach in battlefield approach, disaster applications and earthquake issues.

Keywords: Energy consumption, Location Update, Location Authenticity and Balancing Energy Consumption, Secure localization

1. Introduction

An ad hoc network is a collection of wireless mobile nodes dynamically forming a network without the aid of any network infrastructure. A MANET can be a stand-alone network or it can be connected to external networks (Internet). Alternate or multipath routing has typically lent itself to be of more obvious use to connection-oriented networks; call blocking probability is only relevant to connection oriented networks. In packet-oriented networks, like the Internet, multipath routing could be used to alleviate congestion by routing packets from highly utilized links to links which are less highly utilized. The drawback of this approach is that the cost of storing extra routes at each router usually precludes the use of multipath routing.

MANETs are low cost networks which are composed of small, low-power and inexpensive mobile devices so having GPS installed on them are not feasible. GPS are thus introduced in order to detect MN's location in MANETs. Several positioning techniques have been introduced to make nodes capable of estimating their positions without using GPS. Positioning system is a system employed to estimate the location of a mobile node (MN). Positioning system can be both indoor and outdoor. Therefore, localization techniques with good accuracy outdoors may not perform well indoors. The Global Positioning System (GPS) is the basic way of getting location information. However, GPS performs poorly in indoor environments due to its weak signal reception inside the buildings[1].

In MANETs, existing anonymous routing protocols can be divided into two categories: redundant traffic[2] and hop by hop encryption. Public key based encryption and high traffic causes to generate significantly high cost, many of approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources. Additionally, many of the approaches in MANETs cannot provide all of the aforementioned anonymity protections. In existing protocol, ALARM cannot protect the location anonymity of source and destination[3], SDDR protects the location

*Author for correspondence

anonymity of source and destination but cannot provide route anonymity, and ZAP[4] only destination anonymity. Many anonymity routing algorithms[5] are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing GPSR that greedily forwards a packet to the node closest to the destination. However, the strict relay node selection of the protocol makes it easy to reveal the source and destination and to analyse traffic.

2. Related Work

Durgesh Pyati and Rekha proposed the protocol provides security in terms of location and identity anonymity to source, destination as well as routes[6]. It used the dynamic partition and random selection of nodes it establishes a dynamic routing path for different packet transmissions. A packet in anonymous protocol includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination.

Kapesh et al. analyzed that the requirement of some critical issues to be handled carefully while implementing MANETs in reality[7]. Routing is one of the most critical issues in MANETs. defined Location awareness means that each mobile host uses a positioning device to determine its current physical location. If the mobile hosts' locations are known, it can accurately describe their geometric relationship. Without such information, a manet can be represented by depicting the hosts' connectivity.

The optimal load balancing scheme proposed by Sasikala et al. and its performance can be evaluated by distributing load across different nodes in the network[8]. Each node is based on the locations of the node's one-hop neighbors and location of the packet destination as well. If certain nodes are frequently changing their mobility characteristics, it makes sense to frequently broadcast their updated position. The Adaptive Position Update (APU) strategy generates higher delay in estimating the neighbor positions and due to frequent updates using beacons packets the network becomes overloaded. To overcome the traffic load due to periodic beaconing, it has been identified that there is a need to adapt the beacon update policy employed in geographic routing protocols to the node mobility dynamics and the traffic load.

Archana Yadhav et al. proposed the Nearest Neighbor Query in Location-aware focused on routing protocols to support communications among mobile nodes connected to each other by one-hop/multi-hop links[9]. This method reduced the traffic required for processing KNN queries. And it achieves both reduction in traffic and accuracy of the query result. A. Xavier et.al proposed the Residual energy of wireless nodes[10].He was considered along with the hop count to avoid unbalanced energy consumption of wireless nodes. This causes path failure because of a certain path to the source node that is attacked or lacks energy, which causes path failure.

In location based routing protocols, the main goal was to reduce the flooding area by using request zone[11]. In this design, the flooding area is reduced as much as possible using narrow request zone. Due to this request zone or forwarding region becomes narrow and packet forwarding is highly directional. Making request zone narrower, the control overhead gets reduced to a great extent.Boomaranimalany et.al presented a comparative study of existing routing algorithms for MANET[12]. Various location based routing schemes are compared and analyzed the performance of location accuracy and packet delivery rate.

H. Shen et al. proposed an Anonymous Location-based Efficient Routing protocol (ALERT) for adhoc networks[13]. It's provides high secure communication throughout the network. It partitions the network field into smaller zones and randomly selects nodes as intermediate forwarder nodes, which form a untraceable anonymous route. It hides the data Transmitter/receiver to improve the source and destination anonymity protection. Thus, ALERT achieves anonymity protection to sources, destinations, and path. It also secured the network from counter intersection and timing attacks.

Karim El Defrawy et al. proposed an anonymous routing framework (ALARM) for MANET[14]. It uses locations of the every node to find the secured location map. It's based on the current location on the each nodes, each node can decide neighbour nodes for communication. ALARM uses private and public key for data encryption and decryption to achieve node authentication, data integrity, anonymity, untraceability and unlinkability. It also offers resistance to certain insider and outsider attacks.

Namrata et al. proposed the routing scheme based on Location Aided Routing schemes to improve privacy and secure communication[15]. All nodes acquire public and private keys for data encryption and decryption from the cluster head. When a node wants to communicate, will calculate the approximate Radius and the flood angle of the destination node. The source then creates a Route request message (RREQ), and broad casts it in the calculated direction only.

Our aim is to arrive at a secured multipath protocol which attains to make a balance between location authenticity and energy consumption.

3. Location based Secure Routing Scheme

In the proposed scheme, multipath route is deployed to improve the load balancing and network lifetime. The reliable mobile node choosing approach is proposed to provide more packet delivery rate and high localization accuracy. Destination nodes are chosen with more confidential to improve network authentication.

3.1 Stability based Multipath Route Determination

The number of mobile nodes in its neighbourhood is without relying on a single node to forward a message. If message arrival is failure, it can be sent on alternative path or on multipath routing is illustrated. Once the data packets are assigned to multiple paths, even if the source node is captured within the network, the entire packet information will not leak the complete information of data. And source node is established by zigzag path on the primary path; even source is attacked, and the packet transmission will automatically avoid the failure nodes, and source node will continue information transmission to the destination through the zigzag path. This information can enhance the ability of network capacity attack and improve the efficiency of data transmission.

The following procedure is for message forwarding in multipath routing. The working of multipath routes is optimized because of a certain path to the source node that is attacked or lacks energy, which causes path failure that then continues and to transmit data through a zigzag path. The failure path routing maintenance mechanisms are approved to repair in time, detailed in two different conditions as follows.

- If a source node in the path fails, neighbor nodes automatically sense and from the maintenance of information in the routing table.
- Based on the multipath route maintenance, if the path or the source node appears to be problem, it can be restored or replaced in time.

3.2 Reliable Node Selection

All the neighbor nodes communicate with the destination node within the transmission range. If the number of the communicated neighbor node increased, then the reliability will be more. The procedure for Reliable node selection is given as follows:

Step 1: Set the location of the destination node and the neighbor nodes. It is to confirm that the distance between destination node and neighbor node which is less than the wireless transmission range

Step 2: Set the route between the destination node and neighbor node is only one hop to ignore the influence of multipath routing.

Step 3: The communication process is installed by sending the data packets from neighbor nodes to the destination node at a constant bit rate.

Step 4: Verify the record of data packets at the destination node and neighbor nodes, and compute the packet loss rate at the destination node.

Step 5: The routing table records number of sending packets, the number of receiving packets, and the ID of every packet, packet loss rate, node stability rate and packet delay etc. The whole reliability is calculated as the probability of a message to successfully reach the destination node from the source node.

In network, it is required to find a shortest path from source to destination node and then node reliability of this path is represented by the multiplying of reliability of each node including the node stability in all paths. If there is no stable path from the source to the destination node, the reliability of this configuration is zero.

3.3 Obtaining Sink Node Location Information

In the critical situation, if the destination had moved out of reliable node's region, the source node is not able to delivered packets to the destination node. Therefore, to improve the packet delivery ratio, update the location information of the DN to the latest location information based on the NNs' information are required.

The location information update of destination node works as follows.

Step 1: Reliable Node (RN) receives a data packet, It normally selects the next reliable forwarding nodes

based on its own neighbor node's information and the location information of the destination in the packet header and it forwards the data packet.

Step 2: Reliable Node (RN) uses the information in the routing table to select the next Reliable nodes. It updates the location information of the Destination Node (DN) in the packet header to the information in the routing table.

Step 3: On the other hand, if an Reliable Node (RN) has not changed the location information of the Destination Node (DN) in its routing table, it deals with a packet based on the erroneous location information in the packet header. Consequently, if all RNs lose track of the DN, the Source Node (SN) may need to rediscover the Destination Node (DN).

3.4 Proposed Packet Format

In Figure 1, the proposed packet format is shown here. The source and destination node ID carries 4 bytes. The location authenticity status induces the whether the mobile Nodes are securely located with anchor nodes. It occupies 8 bytes. In fourth field, the location estimate is indicated to maintain memory requirement of unknown mobile nodes which occupies 8 bytes. In fifth, the energy consumption is allotted to ensure more energy efficiency that occupies 4 bytes. The last filed Cyclic Redundancy Check which is for error correction and that occupies 4 bytes.

4. Performance Analysis

We have simulated our results using NS2.34 simulator. It is an object oriented discrete event simulator to identify the performance of proposed scheme. The Backend language of NS2.34 is C++ and front end is Tool command language (Tcl). NS2.34 is user friendly and easy to fabricate our own protocol. Tcl is a string-based command language. The language has only a few fundamental constructs and relatively little syntax, which makes it easy to learn. The syntax is meant to be simple. Here we made the assumption that adopted for simulation is all nodes are moving dynamically including the direction and speed of nodes In either way, the tool helps to prove our theory analytically.

Source Node ID	Destination Node ID	Location authenticity Status	Location estimate	Energy consumption	Cycle Redundancy Check
4	4	8	8	4	4

Figure 1. Proposed Packet format.

In our simulation, 300 mobile nodes move in a 1200 meter x 1200 meter square region for 100 seconds simulation time. All nodes have the same transmission range of 200 meters. Our simulation settings and parameters are summarized in Table-1.

Performance Metrics

We evaluate mainly the performance according to the following metrics.

4.1 Average Packet Delivery Ratio

It is the ratio of the number of packets received successfully to the total number of packets transmitted.

4.2 Communication Overhead

The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets. It suppresses the communication between the source and destination nodes.

End-to-End delay, a packet depends on the routing discovery latency, additional delays at each hop and number of hops.

4.3 Node Degree

Node degree is defined as the network performance based on network topology. If the node degree is very low, the collision between the source and destination should be very small.

Table 1. Simulation Settings and parameters

No. of Nodes	300
Area Size	1200 × 1200
Mac	802.11g
Radio Range	200m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitted power	150 pJ/bit/m^2
Initial Energy	100 Joules
Package rate	4 pkt/s
Protocol	DSR

4.4 Network Connectivity Ratio

It is defined as the numbers of nodes are connected in the intermediate region. Its increases the communication performance.

We compared our proposed protocol ELOER with ALARM[14], and our previous work Efficient Multipath Location Aware Routing Protocol (EMLARP)[16]. The results are examined based on the performance metrics namely node degree, communication overhead, end-to-end delay, packet delivery ratio, and network connectivity ratio.

In Figure 2, we vary the mobility from 5 to 25. Reliability is achieved by means of stability and mobility. Both are integrated in the routing to stabilize the network performance. The probability of reliable links is maximum in the proposed protocol compared to the previous schemes. Connectivity of the link is maximum in the proposed routing. While increasing the mobility, the connectivity ratio of proposed algorithm is higher than the existing schemes.

In Figure 3, time is varied as 50, 100 …. 200 (msec). When we increase the time, the mobility is also getting increasing. Mobility of nodes will lead to network partition. In our proposed model, mobility is kept less dynamic. Nodes transmit the packet towards the destination with less delay. Packets propagating delay and transmission delay are kept low. The proposed protocol has low end to end delay per packet than the existing routing schemes.

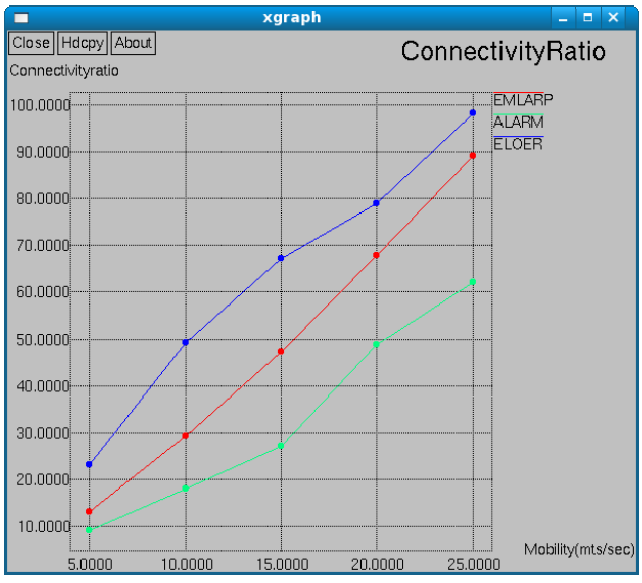

Figure 2. Mobility Vs Connectivity Ratio.

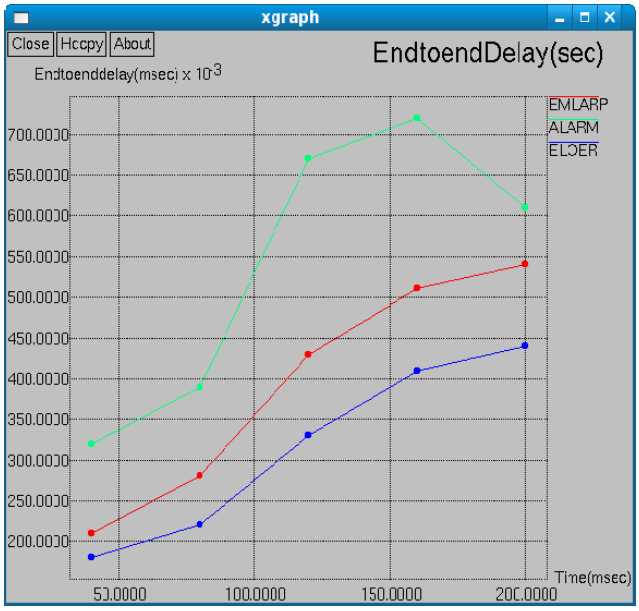

Figure 3. Time Vs End to end delay.

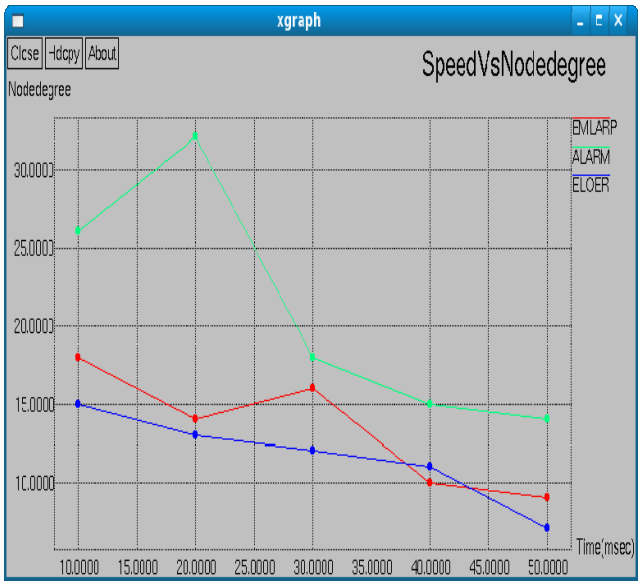

Figure 4. Speed Vs Node degree.

In Figure 4, Speed is varied from 10 to 50 msecs. While increasing the speed, packets are moving randomly with variable transmission rate towards destination. In our proposed model, we schedule the packets through link. Accordingly, packets are arrived at the destination. The problem of congestion overflow and packet dropping is decreased. So the proposed scheme achieves less control overhead instantaneously.

In Figure 5, we vary the mobility from 50 to 200. While increasing the number of nodes, the communication overhead of proposed algorithm is lower than the existing scheme.

In Figure 6 shows the result of throughput Vs Packet Delivery Ratio. From the results, our proposed scheme achieves high packet delivery ratio than the existing schemes because of stability deployed in the reliable multipath routing.

The performance comparisons of proposed and existing schemes are summarized in Table 2.

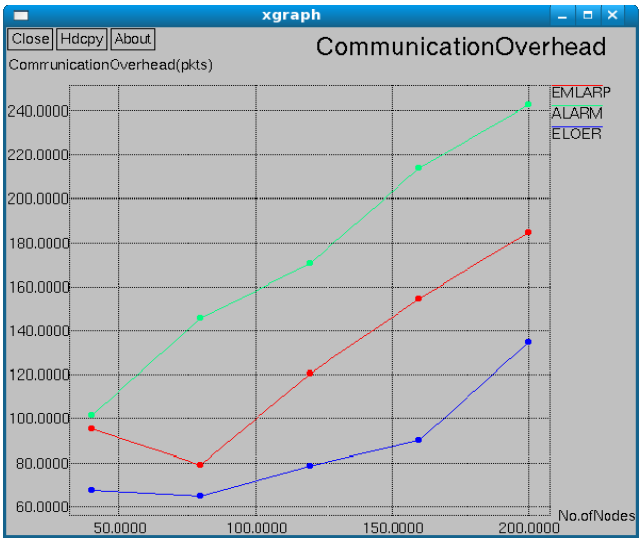

Figure 5. No. of Nodes Vs Overhead.

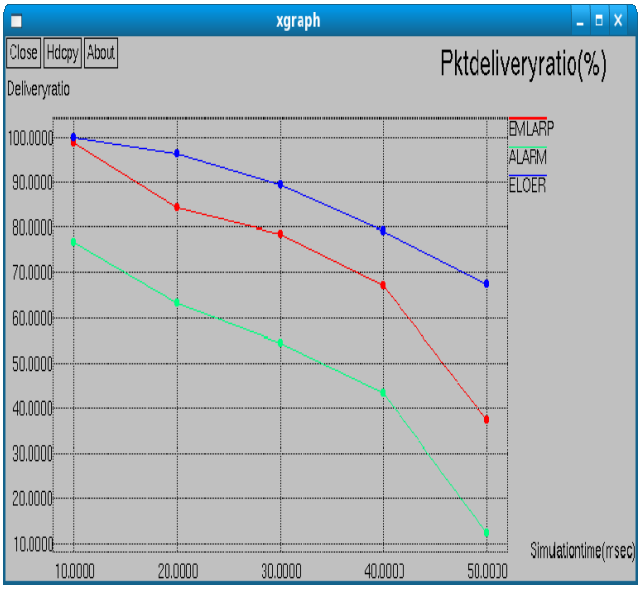

Figure 6. Throughput Vs Packet Delivery Ratio.

Table 2. Performance Comparison

Performance Metrics	ALARM	EMLARP	ELOER
Detection efficiency (%)	12–22	16–32	25–45
PDR (pkts)	3–18	5–27	15–33
Network L_time (Secs)	150–250	223–440	350–647
End to end delay (msec)	0.968–2.15	0.798–1.76	0.678–1.47
Overhead (pkts)	45–90	37–78	26–42
Packet Integrity Vs Speed	53–32	87–65	98–76

5. Conclusion

In this research work, we have developed a secured location based multipath routing which attains to make a balance between location authenticity and energy consumption among mobile nodes. In the first phase of the scheme, stability based multipath routing is proposed. In second phase, reliable nodes are chosen for packet forwarding towards destination node. In third phase, destination with secure location update is determined to secure nodes. In fourth phase, packet format is proposed. Based on the simulation result, the proposed work achieved that secured location authenticity and minimum energy consumption and also proposed protocol has high network lifetime, high location update rate, low end to end delay and low overhead than the existing schemes.

6. References

1. Sathish T, Raja R, Batt TH. Anonymity Set Location Privacy Scheme in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2014 Feb; 4(2):52–5.
2. Wu x. AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol. IEEE Trans Mobile Computing. 2005 Jul-Aug; 4(4):335–48.
3. El-Khatib K, Korba L, Song R, Yee G. Anonymous Secure Routing in Mobile Ad-Hoc Networks. Proc Intl Conf Parallel Processing Workshops (ICPPW). 2003.
4. Ratnasamy S, Karp B, Shenker S, Estrin D, Govindan R, Yin L, Yu F. Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table. Mobile Network Applications. 2003 Aug; 8(4). p. 427–42.

5. Zhi Z, Choong YK. Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy. Proc Third Intl Workshop Mobile Distributed Computing (ICDCSW). 2005 Jun 6-10; 646–51.
6. Pyati D, Rekha S. High Secured Location-based Efficient Routing Protocols in MANET's. International Journal of Recent Development in Engineering and Technology. 2014; 2(4):78–84.
7. Popat KP, Sharma P, Molia HK. Location Aware Routing Schemes for Mobile Ad hoc Networks. International Journal of Advance Research in Science and Engineering. 2015; 4(1):1814–18.
8. Sasikala M, Sangeetha M, Nithya MR, Indhumathi P. Optimal Load Balancing Scheme for Geographic Position Updates in Manet. National Conference on Research Advances in Communication, Computation, Electrical Science and Structures. 2015. p. 44–9.
9. Yadhav MD, Rajalakshmi R. Nearest neighbor query in location aware mobile ad-hoc network. International Journal of Computer Science and Mobile Computing. 2015 Mar; 4(3):51–5.
10. Xavier A, Sankar SP. Modified DSR Protocol for Power Saving In Mobile Ad Hoc Networks. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2015; 4(4):2045–52.
11. Nikama V, Chavanb GT. Improving Performance Using Narrow Request Zone in MANET. International Journal of Advanced Research in Computer Science Engineering and Information Technology. 2015; 5(3):384–92.
12. Boomaranimalany A, Bharathi S, Premanand V. A location based terminode routing in manets. International Journal of Engineering Research and Technology (IJERT). 2015 Jan; 4(1):80–5.
13. Shen H. Anonymous Location-Based Efficient Routing Protocol in MANETs. IEEE Transactions on Mobile Computing. 2013 Jun; 12(6):1079–93.
14. El-Defrawy K, Tsudik G. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs, IEEE Transactions on Mobile Computing. 2011 Sep; 10(9):1345–58.
15. Leelaipushpam P, Namrata K. A reactive protocol for privacy preserving using location based Routing in MANETs. International Journal of Computer Science and Network. 2013; 2(2):108–13.
16. Rajaram A, Vinothkumar K. Efficient Multipath Location Aware Routing Protocol for Mobile Ad Hoc Networks. Journal of Theoretical and Applied Information Technology, Scopus Indexed. 2014; 59(1):130–38.