IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Convention for Detecting Multiple Blackhole and Greyhole Attack on a Chaotic Map

Syeda Ummulhuda Hashmi[1], Deepak G[2]

PG Student, Department of CSE, Dayananda Sagar College of Engineering, VTU, Bengaluru, Karnataka, India[1]

Assistant Professor, Department of CSE, Dayananda Sagar College of Engineering, VTU, Bengaluru, Karnataka, India[2]

ABSTRACT: The specially appointed on-request separation vector (AODV) is a comprehensively utilized directing convention for portable impromptu systems (MANETs), it is defenseless against a blackhole and greyhole assault. Dark opening and dim gap assault is one of the security danger in which the traffic is diverted to such a hub, that really doesn't exist in the system. A safe MANET steering convention called BGP-AODV to address the security shortcoming related with the first SAODV convention and to cure the blackhole greyhole attack.BGP-AODV convention can ensure against blackhole and greyhole assault performed by a malevolent hub during the directing cycle. Be that as it may, it can't avoid the helpful blackhole and greyhole assault, in which two hubs are taking an interest together to mount such assault. Accordingly, this paper proposes a protected MANET steering convention called BGP-AODV to defeat the security breaks identified with the SAODV convention alongside the first AODV convention. Moreover, the BGP-AODV can ensure against an agreeable blackhole assault and grayhole assault propelled during the directing cycle and prepares for the blackhole assault and grayhole assault that may happen during the sending cycle. The BGP-AODV is created by expanding the usefulness of the AODV convention alongside using the turbulent guide highlights. The BGP-AODV convention is safer than the SAODV convention and can viably battle the blackhole and grayhole assault accomplished by a pernicious hub or helpful malignant hubs during the steering cycle.

KEYWORDS: BGP-AODV, MANET, cooperative blackhole and greyhole attack,SAODV

I. INTRODUCTION

WSNs are a gathering of self-sufficient sensors that are spatially circulated and are sent to screen certain ecological or physical boundaries, for example, mugginess, sound, temperature, pressure, water level, and so forth and to effectively communicate the gathered information to the principle area by means of the system. The systems that are conveyed these days are more present day and bi-directional, accordingly permitting the control of the exercises that are associated with the sensors. The principle inspiration driving the presentation of remote sensor systems was applications in the field of the military, for example, target recognition, adversary following, checking of fringes, assault location, and so forth,.; yet starting today remote sensor systems are being applied in different shopper and mechanical applications, for example, water level observing, transportation, following of items, security, and so on..

AODV: Ad hoc On Demand Network and MANETS

The Ad hoc On-Demand Distance Vector (AODV) protocol used when two end point do not have a valid active route to each other .It is dynamic, multi hop routing among mobile nodes wishing to establish and maintain an ad hoc network. AODV allows for the construction of routes to specific destination and does not require that nodes keep these routes when they are not in active communication .AODV avoid the “counting to endless” problem by using destination sequence number This make AODV lop off. The following type of message is in AODV.

- RREQ: Route Request Message-used to initiate the route finding Process.
- RREP: Route Reply Message-messages are used to conclude the routes.
- RERR: Route Error message-messages are used to notify the network of a link breakage in an active route.

BLACK HOLE ATTACKS

Black-hole attacks happen at the Network nodes that it has the shortest route to their destination node. The malicious node will drop all data packets or implement man-in number sends fake routing information by advertising that it has

the shortest path to the destination node .When the node wants to send a packet data to the node , it will initiate route discovery. The malicious node intercepts the RREQ pa the sender node.If the reply from the malicious node reaches the source first, then the sender node disregards all other RREP messages and start sending packets through node. Therefore, all packets are lost.The black hole node convinces the source node that it has a valid, short, and fresh route to the destination node, although it does not actually have any route to the destination node.

GREY HOLE ATTACKS

The grey-hole attack takes place at the network layer and can be used as a slow poison in the network side. A grey-hole attack happens when a destination node with the intention of intercepting data packet. However instead of forwarding the data packet, the malicious node (i.e. the grey three ways:

• Drops packets sent by specific nodes while forwarding packets sent by the other nodes.
• The malicious node drops all packets received within a specific period of time and forward packets later.
• The grey-hole drops the intercepted packets randomly and grey-hole attack is more difficult to detect than the black hole attack in which the malicious node drops all the packets received.

II. RELATED WORK

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks [4, 9].

Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9].

In [3] a path based detection method is proposed, in which every node is not supposed to watch every other node in their neighborhood, but in the current route path it only observes the next hop. There is no overhead of sending extra control packets for detecting Black Hole attack.

In any network, the sender wants its data to be sent as soon as possible in a secure and fast way, many attackers advertise themselves to have the shortest and high bandwidth available for the transmission such as in wormhole attack, and the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes [12]

Different kinds of attacks have been analyzed in MANET and their affect on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [14].

III.PROPOSED WORK

A protected MANET directing convention called BGP-AODV to beat the security penetrates identified with the first AODV convention. The BGP-AODV is created by expanding the usefulness of the AODV convention alongside using the riotous guide highlights.The BGP-AODV convention is safer than the SAODV convention and can successfully battle the dark gap and dim gap assault accomplished by a pernicious hub or agreeable noxious hubs during the steering cycle.

IV. IMPLEMENTATION

Implementation Modules

Topology Module

This section contains description of functionality of the scripts used in building topology. This module involves building Wireless Network topology, topology consisting of mobile nodes, each node working with multiple channels. This module consists of following steps:

- **Setting up Wireless Network Topology:** This includes environmental settings, node configuration, and topology creation.
- **Setting the bandwidth and threshold:** Each and every node in the network topology will be assigned with certain bandwidth and topology.

- **Identifying the neighbors:** In order to identify the neighbors for a particular node Euclidian distance concept is used.
- **Specifying the data transmission through single and multi hop:** From which node the data has to be sent and which node must receive the data will be specified. Also how much amount of data has to be sent along with the time interval of sending the data will be specified.
- **Specifying the simulation start time and end time:** In NS 2 the entire transaction takes place within fraction of seconds. The transaction can be viewed through the NAM window at any time. For this the simulation start time and end time will be specified.

Node Deployment Algorithm

This algorithm is responsible for deployment of nodes in a particular area. This will position the nodes in the given area.

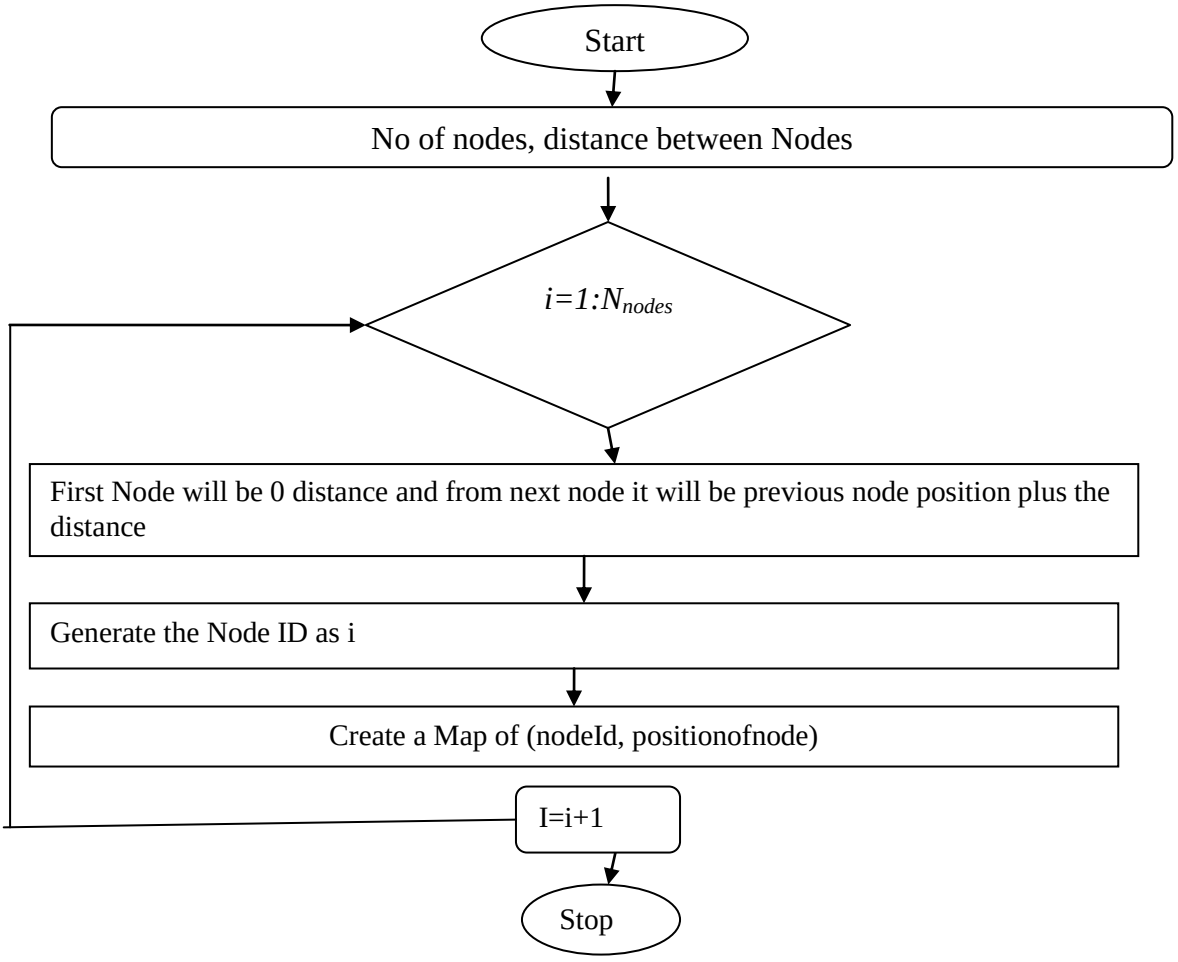

Fig 1: Node Deployment Algorithm

Fig shows the Node Deployment Algorithm. The input to this algorithm contains Number of Nodes and Distance between Nodes. The output contains the map of NodeID and Position of Node.

Routing Table Formation

The Routing table formation algorithm is used to form the routing table's for the nodes which contains the node ids , distance and reachable flag. The routing table will contain information about other nodes in the network in terms of node id and distance of each node w.r.t other nodes in the network.

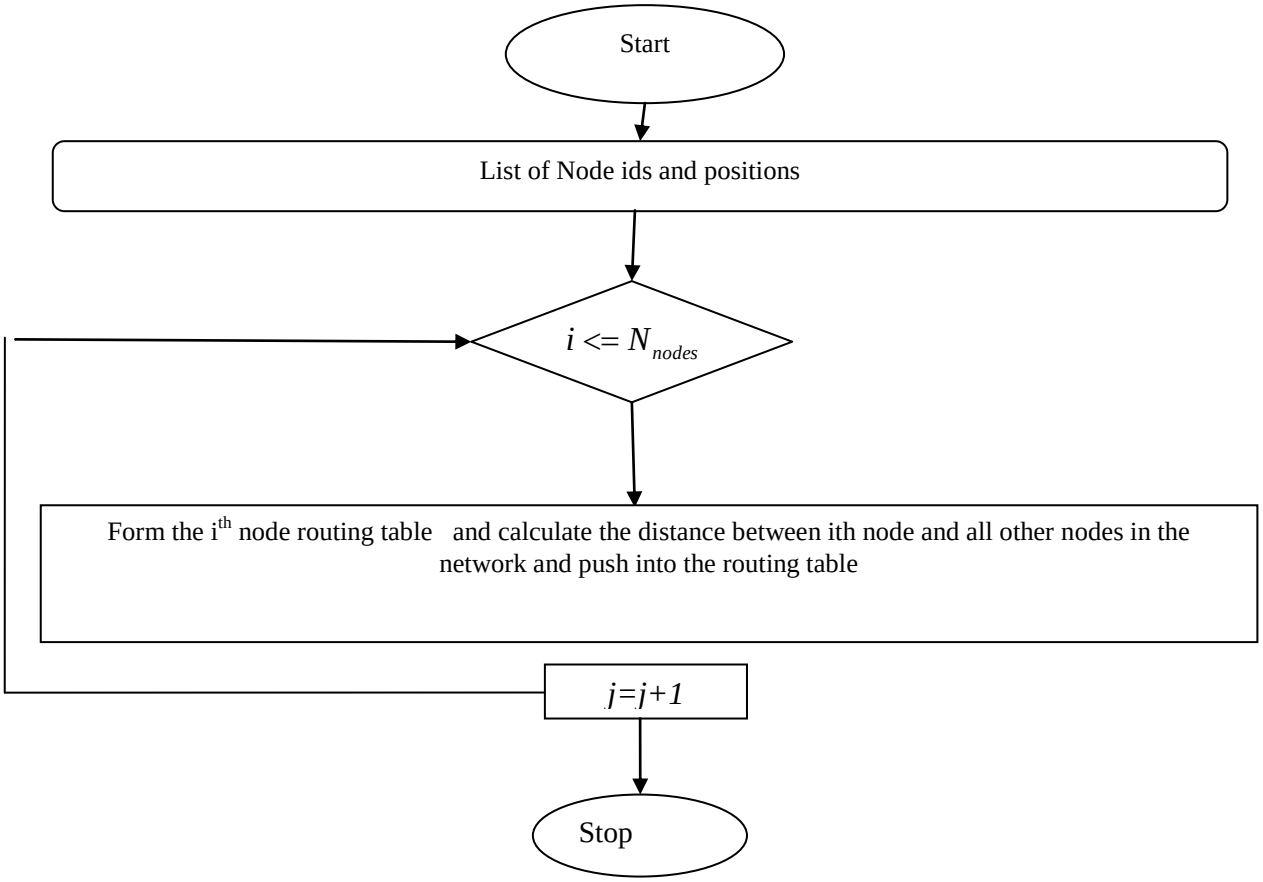

Fig 2: Routing Table Formation Algorithm

V. SIMULATION RESULTS

PERFORMANCE METRICS

In the performance evaluation of a protocol for MANETs, the protocol should be tested under realistic conditions. We perform extensive simulations using NS-2 simulator. To reiterate the black hole attack, we begin with the overview of performance metrics that used by us are Overhead,End-to-end delay, Throughput,Packet delivery ratio.

SIMULATION USING NETWORK ANIMATOR

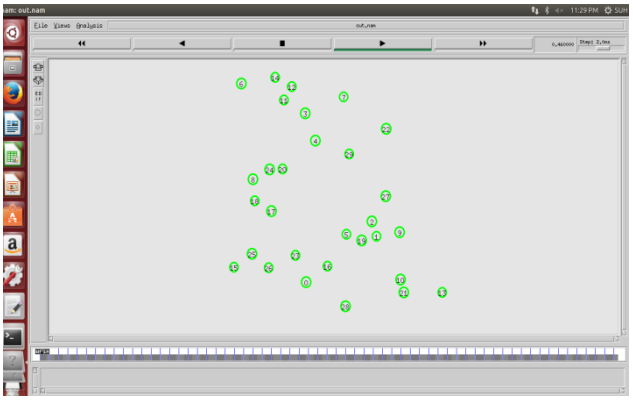

Fig.3. Network deployment

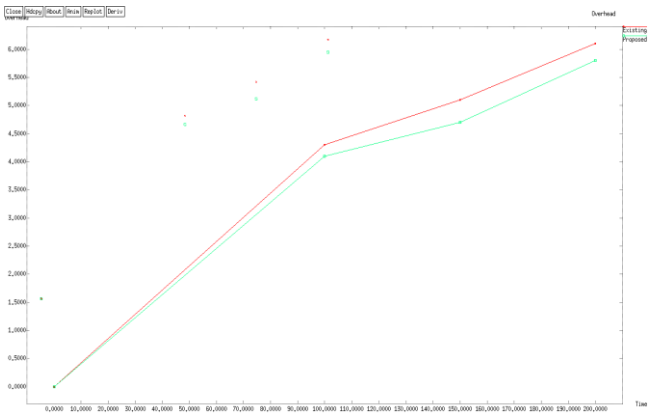

Fig.4.Overhead graph of existing and proposed system

Fig. 5. Delay graph of existing and proposed system

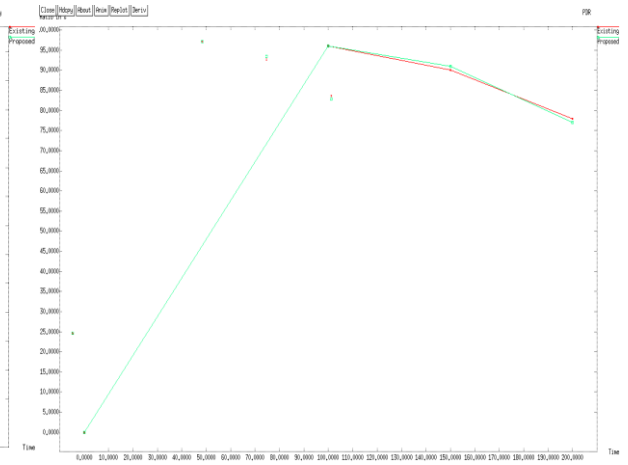

Fig 6. PDR graph

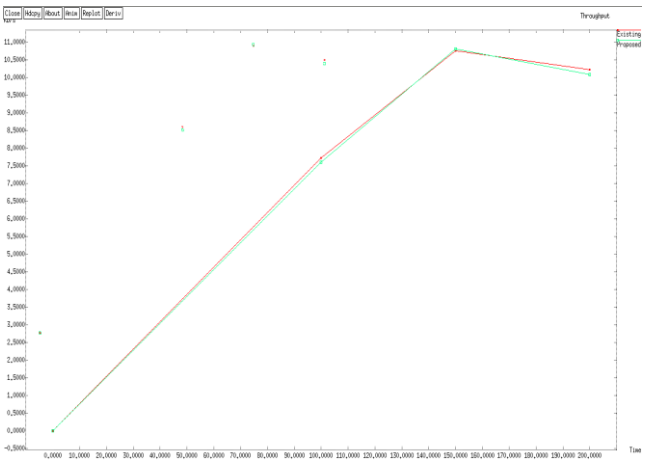

Fig.7.Throughput graph

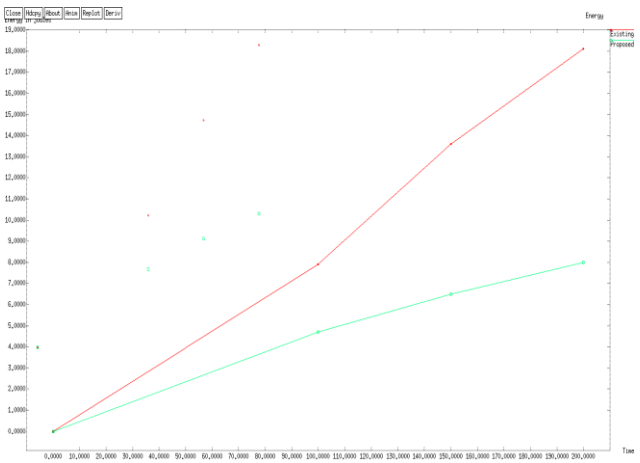

Fig.8.Energy graph

VI. CONCLUSION

The protocol resolved the malicious node vulnerability in which we used chaotic map characteristics to avoid multiple malicious nodes. We secure attacks by placing a node anywhere in anetwork. Simulation results have shown that the pr otocol is more efficient and reliable in terms of protection.Because of its adaptable nature, remote Ad-Hoc arranges are effectively sent independent of geological limitations. These systems are presented to both outer and inside assaults as there isn't incorporated security instrument. Most examination is done here, still need. The consequences of the Black Hole and Gray Hole assault on MANETs utilizing AODV conventions have been found and investigated. In various MANET conventions, for example, DSR, TORA and GRP with the Black Hole and Gray Hole Attack different types of assault, for example, wormholes, jellyfish and sybil, must be contemplated.

REFERENCES

[1] L. Tamilselvan and V. Sankaranarayanan, ‘‘Prevention of co-operative black hole attack in MANET,’’ *J. Netw.*, vol. 3, no. 5, pp. 13–20, 2008.
[2] N. Jaisankar, N. Saravanan, and K. D. Swamy, “A Novel Security Approach for Detecting Black Hole Attack in MANET”, Proc. Business Administration and Information Processing Heidelberg, pp. 217-223, 2010.
[3]K. S. Chavda, and A. V. Nimavat, “Removal of Black Hole Attack in AODV Routing Protocol of Manet”, Proc. IEEE conference on computer networks, Tiruchengode, India, pp. 207-212, 2013.
[4]W. Wang, G. Zeng, J. Yao, W. Hanli, and T. Daizhong, “Towards Reliable Self-Clustering Mobile Ad hoc Networks” International Journal on Computer and Electronics Engineering, Vol. 38, No. 1, pp. 551- 562, 2012.
[5]N. Kalia, and K. Munjal, “Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol” International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, No. 3, pp. 529-533, 2013.
[6]S. Abid, and S. Khan, “Improving Performance of Routing Protocols Using MRP Framework” International Journal of Ambient Systems and Applications (IJASA), Vol. 2, No. 1, pp. 1-8, 2014.
[7] A. K. Jain and A. Choorasiya, ‘‘Security enhancement of AODV routing protocol in mobile ad hoc network,’’ in Proc. 2nd Int. Conf. Commun. Electron. Syst. (ICCES), Coimbatore, India, Oct. 2017, pp. 958–964.
[8] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, “ An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network”,24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.
[9] M. Patel and S. Sharma, "Detection of malicious attack in MANET a behavioral approach," 2013 3rd IEEE International Advance Computing Conference (IACC), 2013.
[10]S.Sharma, Rajshree, R.P.Pandey, V.Shukla, “Bluff-Probe Based Black Hole Node Detection and Prevention”, IEEE International Advance Computing Conference (IACC 2009), pp. 458-462, March, 2009.
[11] Z.Wang, Y. Chen, and C. Li, ``PSR: A lightweight proactive source routing protocol for mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 63,no. 2, pp. 859_868, Feb. 2014.
[12] J. Sen, M. G. Chandra, S. G. Harihara, H. Reddy and P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks," 2007 6th International Conference on Information, Communications & Signal Processing, 2007.
[13] J. Cai, P. Yi, J. Chen, Z. Wang and N. Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," 2010.
[14] Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., & Ma, M. (2019). Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics. IEEE Access, 7, 158481-158491.
[15] D. Ravilla, V. Sumalatha, and C. Putta, ``Hybrid routing protocols for adhoc wireless networks," Int. J. Ad hoc, Sensor Ubiquitous Comput., vol. 2,no. 4, pp. 79_96, 2011.
[16] T. Issariyakul and E. Hossain, Introduction to Network Simulator NS2. Boston, MA, USA: Springer, 2009.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details