IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 9, September 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

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

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109013 |

Design and Implementation of Energy Efficient Device -To-Device Communication System Based on MANET and Secured Communication Using AODV Protocol

Mr.M.Kumar M.E (PhD) [1*], Chaitra.T [2]**

Assistant Professor, Department of Electronics and Communication Engineering, Er. Perumal Manimekalai College of Engineering College, Hosur, India[1*]

P.G Student, Department of Electronics and Communication Engineering, Er. Perumal Manimekalai College of Engineering College, Hosur, India[2**]

ABSTRACT: The Device-to-Device (D2D) communication presents a new paradigm in mobile networking to facilitate data. D2D development is driven by mobile operators using short-distance communications to improve network performance. In this project, we investigate two fundamental and interrelated aspects of D2D communication, security and privacy, which are essential for the adoption and deployment of D2D communication. Mobile Ad-hoc Networks (MANETs) features such as open medium, dynamic topology, lack of centralized management and lack of infrastructure expose them to a number of security attacks and MANET framework allows to user to access and deliver data through their connected devices on the base station. This project as presents the device-to-device communication based on MANET network and analyses the performance of AODV when attacked by black hole, by varying the mobility of the nodes in the network. A MANET is a type of wireless network that self-organizes and automatically interconnects in a decentralized approach. Each node in the MANET is free to move from one location to another in any direction within the MANET. This analysis is carried out by simulating scenarios of AODV based MANET using Network Simulator 2 (NS-2). The performance metrics that are used to do the analysis are throughput, packet delivery ratio and end-to-end delay and plotted as a graph in graph The throughput and packet delivery rate will decrease when the network is attacked by a black hole because the malicious node will swallow or drop some packets. End-to-end delay is also reduced in the presence of a black hole attack because a malicious node pretends to have a valid base station to anther device routing tables and therefore shortens the route discovery process. Black hole attack is one type of attack that is more common in MANET reactive routing protocols such as Ad-hoc On-demand Distance Vector (AODV). So, in this system we use a encrypted key for sending the information securely. It then redirects all packets going to the destination node to itself and drops them instead of forwarding them.

I. INTRODUCTION

Device-to-Device (D2D) communication represents a promising technique to modify devices to speak directly with the interaction of access points or base stations. the essential construct of D2D is to knowledge exchange between nodes. many studies analyzed the construct of exploitation D2D in cellular networks. However, a standard cellular system doesn't permit devices to directly communicate with one another, instead all communications turn up through the bottom stations. This study may be a move forward over the Manet numerous systems. The authors explained the device-to-device communication below the cellular networks. The Device-to-Device (D2D) communication among phone networks is delineated as communication directly among 2 smartphone users while not making an attempt to cross the bottom station. The system study can be wont to improve and expand current Manet communication. Its outcomes square measure to form a brand new structure for secure communication among sensible devices. Therefore, we'd like communication technologies that may scale network capability and modify knowledge exchange on-demand over the proper network connections. a tool with a wireless property will act as a hotspot to that knowledge is offloaded/cached from the baccalaureate and from that alternative devices might transfer the information exploitation D2D links. UEs having less process power or low energy budgets may offload computation-heavy tasks to near additional capable UEs exploitation D2D links. goodish analysis has gone into style of offloading techniques.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109013 |

exploitation D2D communication, an outsized quantity of information will be transferred quickly between mobile devices in brief vary.

II. LITERATURE SURVEY

[1] Device-to-device (D2D) communication has been given during this paper, together with the and points it offers; the key open problems related to it like peer discovery, resource allocation etc, difficult special attention of the analysis community; a number of its integrant technologies like mm wave D2D (mmWave), immoderate dense networks (UDNs), psychological feature D2D, relinquishing procedure in D2D and its varied use cases. design is usually recommended attending to fulfill all the subscriber demands in Associate in Nursing optimum manner. The Appendix mentions some current standardization activities and analysis comes of D2D communication.[2]This projected work explains the mitigation methodology by mistreatment node isolation methodology in order that once the malicious node is detected, it'll be removed from the cluster and thence the packet call the network because of self-seeking Node attack may be reduced. Also, during this projected work performance analysis of ad-hoc distance vector (AODV), Adhoc On-demand Multipath Distance Vector(AOMDV), Destination Sequenced Distance Vector(DSDV) Routing protocols has been analyzed supported output and Packet delivery magnitude relation parameters mistreatment the NS2 machine.
[3]To avoid this issue, projected a brand new approach known as good attack discover ion (SAD) approach that is employed to detect the sort of denial of service attack in wireless unplanned network. This unhappy approach consists of 4 varieties of attacks detection is feasible. In general, police work the categories of malicious attacks is most vital than police work malicious node. By victimization this approach, will discover the sort of malicious attack and once will build the perfect answer in future. unhappy approach has detects the botnet attack, part attack, worm hole attack and sink hole attacks. Botnet attack can occur once the overflow occur to the actual node. Blackhole attack can occur once any of the intermediate node can block the info transmission to the destination. hole attack can occur once any of the wrongdoer node disturbs the close nodes. swallow hole attack can occur once any of the wrongdoer node disturbs the neighbor node unceasingly. In simulation, by victimization the network machine version a pair of.35 performance of the wireless unplanned network was analyzed.[4] The purpose of this study is to investigate the comparison of blackhole attack and flooding attack against energy-efficient AODV on VANET. This analysis uses simulation strategies and several other supporting programs like OpenStreetMap, SUMO, NS2, NAM, and AWK to check the AODV routing protocol. Quality of service (QOS) parameters employed in this study ar turnout, packet loss, and finish to finish delay. Energy parameters are wont to examine the energy potency used. This study uses the amount of variations of nodes consisting of twenty nodes, 40 nodes, 60 nodes, and totally different network conditions, specifically traditional network conditions, network conditions with part attacks, and network conditions with flooding attacks. The results obtained may be all over that the very best price of turnout once network conditions ar traditional, the best price of packet loss once there's a part attack, the very best finish to finish delay price and also the largest remaining energy once there's a flooding attack.

III. PROPOSED SYSTEM

In planned system fifteen nodes, Omni-directional antenna, TCP/FTP link layer were used. AODV protocol is employed as a routing protocol. Common attacks during this system square measure part attack and collision attack. Data packets are not allowed to reach its sink node by blackhole attacker node. So here a method is being proposed for blackhole attack detection and prevention. In this method the blackhole is detected before it attacks the node and reprogram its data and prevents from data loss. 2 devices communicate directly with one another, with management links provided by the bottom station. although direct, the communication is entirely managed by the bottom station. A central dominant entity, i.e. the bottom station (BS) is gift, interference management is feasible. The technique used for isolation is encrypted 16-digit key identity. before transmission mechanism of data between the devices, these oughts to notice one another. Device discovery are often attainable by a periodic broadcasting of the device identity. Distance constraint is mostly thought-about, for D2D pair creation. Energy Consumption is low. Simulating space is giant i.e., a thousand * a thousand.The results additionally show that output decreases slightly once quality of the nodes is inflated within the network. the rise within the speed of the nodes decreases each end-to-end delay and packet delivery quantitative relation. The analyzed throughput, delay time and packet delivery ratio (PDR) values can be plotted in graph by using Xgraph.

ADVANTAGES

- The status of the node can be detected like dead and alive

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109013 |

- MANET increase the efficiency of the network

IV. FLOW CHART

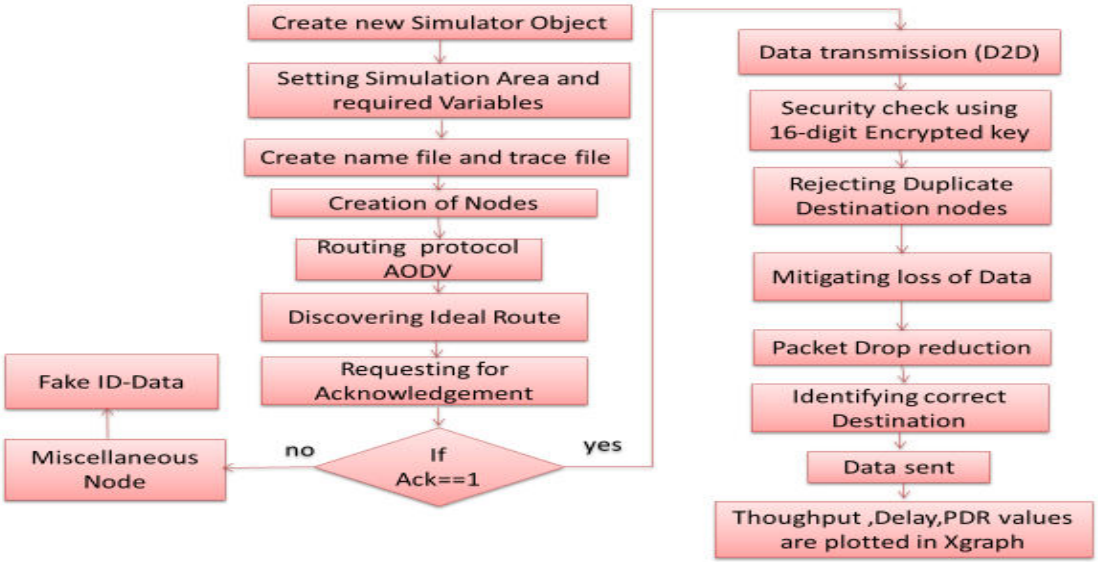


Fig.no: 1 Flow chart

Parameters	Existing system	Proposed system
Algorithm	DSR (Dynamic Source Routing Protocol)	AODV (Ad Hoc On – Demand Distance Vector)
Packet delivery ratio (PDR)	Increased	Decreased (95.000)
End-to-end delay	Decreased	Decreased (17.000)
Throughput	Slightly Increased	Very large increase (83.000)

Table no 1:Comparison table

IMPLEMENTATION DETAILS:

In this paper we implemented a energy efficient device-to-device communication system based on MANET and secured communication using AODV protocol. The network simulator object is created and 15 nodes will be created and assigned initial position as well as the destination at each point in the simulation. Also the size of each node is defined. The required variables will be set and assigned with respective values. The source node will request for the acknowledgement and based on the received acknowledgement, it will determine the correct destination and avoid all the other malicious nodes as they sent an inappropriate acknowledgement. The term AODV stands for Ad-hoc On-

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109013 |

demand Distance Vector. This protocol will determine the appropriate route for the construction of path for the purpose of data transmission from device to device communication. Then the condition of the node will be checked as whether it is in active state or inactive state. If it is in active state, data will be transferred using TCP (Transmission Control Protocol). Otherwise, Node will be isolated. In the middle of the data transmission, the malicious nodes in the network will try to connect in the transmission which may leads to data loss. In order to avoid such Black hole attack, the source node will generate encrypted key and the Destination node will accept the generated encryption key for the purpose of security aspects. The Simulated circuit will be displayed in the Network Animator (NAM) which is the end result of the simulation of the proposed circuit I.e., device to device communication MANET (Mobile Ad-hoc Network).The results also show that the throughput decreases slightly as the mobility of the nodes in the network increases .Increasing the speed of nodes reduces both the end-to-end delay and the packet delivery ratio. The analyzed throughput, delay time and packet delivery ratio (PDR) values can be plotted in graph by using X graph..

V. WIRELESS NETWORK DESIGN

PARAMETERS	VALUES
Area of Simulation	(1000 X 1000)m
Nodes number	15
Types of Routing protocol	AODV
Internet protocol type	TCP
Antenna Model	Omnidirectional
Max package	50
Type of the MAC	802.11
Transmission speed	1.2 Mbps
Bandwidth	20MHz

AODV PROTOCOL

AODV referred as Ad Hoc On-Demand Distance Vector. Ad-hoc On-demand Distance Vector (AODV) is a combination of on-demand and distance vector i.e. hop-to-hop routing methodology

Steps involved in AODV routing protocol:

- Path discovery
- Reverse path setup
- Forward path setup
- Rout table management
- Path maintenance
- Local connectivity management

Advantages of NS2 Simulation Code for AODV:

- Scalable to large population of nodes.
- Broadcast is minimized.
- Reduces memory requirements and needless duplications.

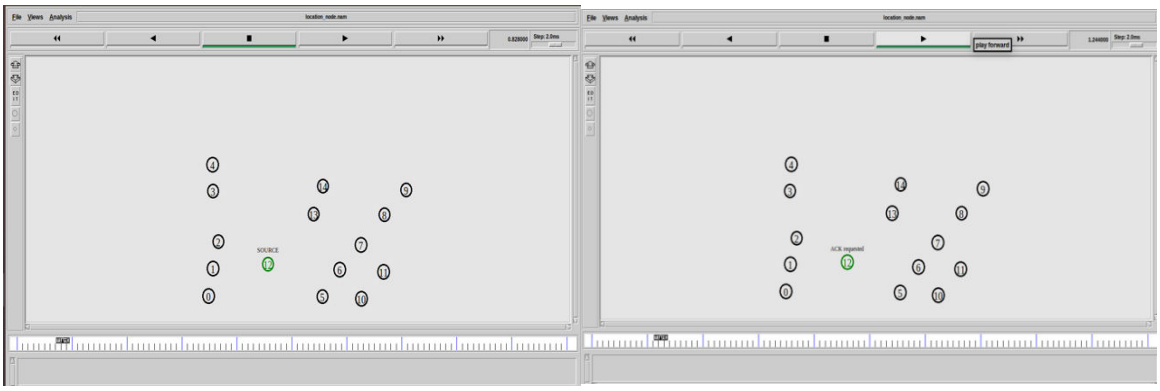
VI. RESULTS

In this project, we had developed the model for the blackhole attack detection in wireless device to device (d2d) communication, in this we developed 15 nodes was successfully designed. we completed the project with detection of miscellaneous nodes. The wireless nodes will be developed in the ns2 simulator and finding the miscellaneous nodes based on the encrypted16-digit key and find the block hole attack .The reduced delay time,PDR and throughput values are plotted in Xgraph. The output screenshots are given below.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

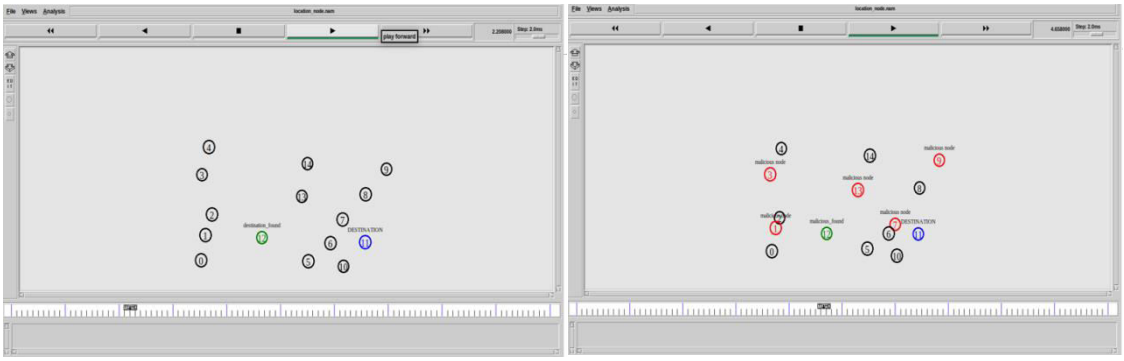
||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109013 |



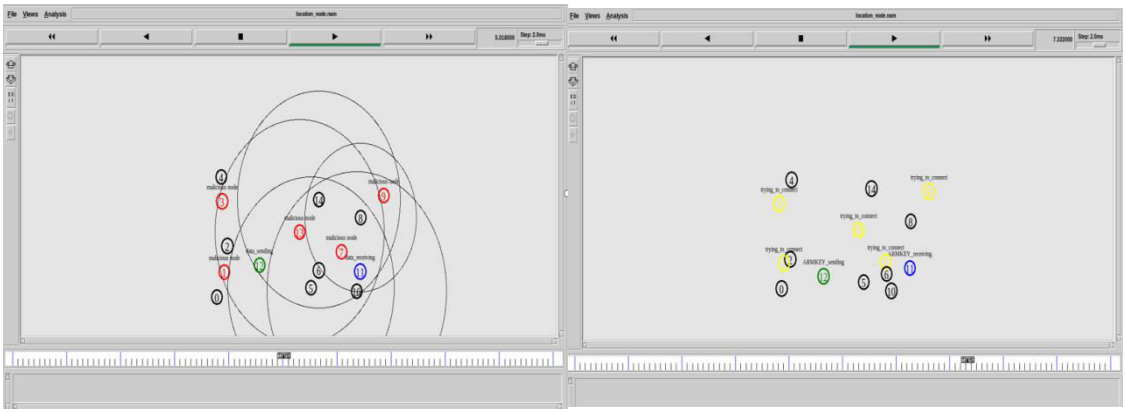
(a)4 Nodes in the source(b)5 Source node send ack request

(a)The above screenshot represents the nodes are created in the NS2 simulator.In That the soure node will be send acknowledgement request for destination.
(b) The source node send the acknowledgement request to destination for data communicating device to device.



(c)6 Source node find the destination node **(d) 7 Miscellaneous nodes were found**

(c)In the nam window the source node find the destination node among the 15 nodes.
(d)The source node will request for the acknowledgement and based on the received acknowledgement, it will determine the correct destination and the malicious nodes can be found.



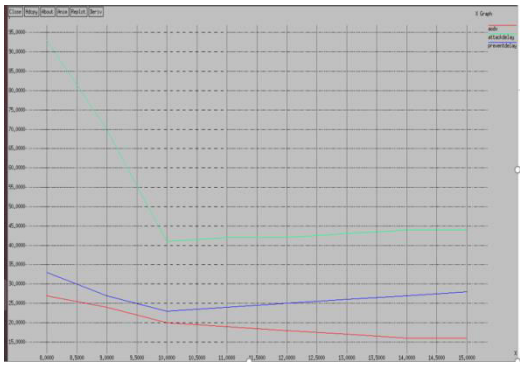
(e) 8 Data sending in source to destination(f)9 Trying to connect nodes and ARM keys

(e)The sorce node sending the data to destination node.
(f) In the middle of the data transmission, the malicious nodes in the network will try to connect in the transmission which may leads to data loss. In order to avoid such Black hole attack, the source node will generate encrypted key and the Destination node will accept the generated encryption key for the purpose of security aspects.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

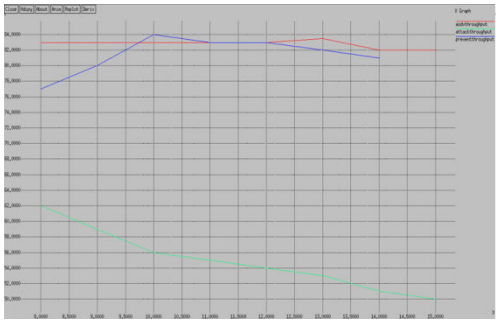
| DOI:10.15680/IJIRSET.2022.1109013 |



PARAMETER	VALUE
Reduced delay value	17.000
Attack delay value	45.000
Prevent delay value	26.000

(g)10 Delay

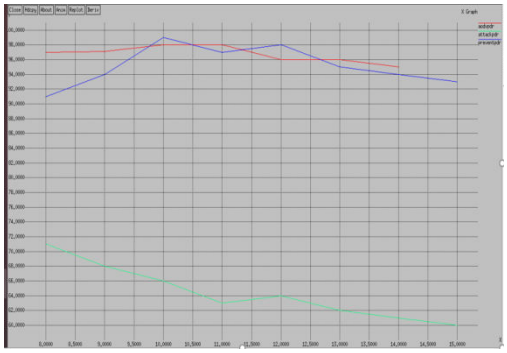
(g)X-axis =number of nodes, Y-axis = AODV delay , Attack delay ,Prevent delay



PARAMETER	VALUE
Increased throughput value	83.000
Attack throughput value	52.000
Prevent throughput value	82.000

(h)11 Throughput

(h)X-axis =number of nodes, Y-axis = AODV throughput, Attack throughput, Prevent throughput



PARAMETER	VALUE
Reduced PDR value	95.000
Attack PDR value	60.000
Prevent PDR value	93.000

(i): 12 Packet Delivery Ratio (PDR)

(i)X-axis =number of nodes, Y-axis = AODV PDR , Attack PDR ,Prevent PDR

VII. CONCLUSION

The state-of-the-art solutions to tackle security and privacy challenges in Device-to-Device (D2D) communication. The reviewed approaches span across a variety of D2D prospects, such as network communication and location privacy. In addition to the conventional review on security, we also provide a detailed discussion on D2D privacy. In this Project, we have presented a new technique to detect black hole attacks in wireless device to device communication. Our proposed system implements AODV protocol as routing protocol. It does not require additional hardware, node location or send any information to base station. No extra communication is used for the purpose of detecting and isolating black hole attacks. AODV protocol is more efficient routing protocol generally as it establishes ideal routes that can be enhanced for d2d communication purpose. Further, this methodology ensures the security in the data

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109013 |

transmission procedure and plotted the xgraph for reduced values of delay packet delivery ratio and Throughput . Proposed technique is also applicable when black hole nodes advertise high quality link, strong transmitted power etc. In such cases also, our system manages to detect and isolate the such attacks in wireless communication.

REFERENCES

[1] PimmyGandotra, Rakesh Kumar Jha "Device-to-Device Communication in Cellular Networks: A Survey"
[2] Karthik Pai B. H., Nagesh H. R, Niranjan N. Chiplunkar, "Mitigation and performance evaluation Mechanism for Selfish Node Attack in MANETs"
[3] vijithaananthi, vengatesan "detection of various attacks in wireless adhoc networks and its performance analysis"
[4] Andrew Fiade, AfieYudhaTriadi, Ahmad Sulhi, Siti UmmiMasruroh,VeliaHandayani and Hendra BayuSuseno "Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network)"
[5] Poornima B, Kalpana P S "Clustering Technique to Secure MANETs From Black Hole Attack"
[6] I. Krontiris, T. Giannetsos, T. Dimitriou, "'Launching a sinkhole attack in wireless communication; the intruder side"ARPN Journal of Engineering and Applied Sciences 13(10), 3378-3387.
[7] TanweerAlam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 3, Issue 5, pp.450-456, May-June.2018 [8] Alam, Tanweer, and Mohammed Aljohani.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details