Network Security:Optimistic Link Selection for Security – QoS Measures in Relaying Network

Dr. G Umarani Srikanth
Prof.Dept of CSE St. Peter's College of Engineering and technology Chennai, India

S. ChenchuLakshmi, Dept of CSE St. Peter's College of Engineering and technology Chennai, India

B. Gayathiri, Dept of CSE St. Peter's College of Engineering and technology Chennai, India

Abstract—*This paper identifies the best route for the data transfer from the source node to the destination node in any network. Initially source node will send dummy packets to analyze the best available route that connect the destination node. It goes through the following parameters like capacity, cost, throughput, battery level to transfer the packets to the destination. Based on the nodes dynamic behavior Self Routing system is implemented. In real time data will be send from source to destination by secured way.*

Keywords— Quality of Service, Network Security, Multi-relay, Cryptographic, Physical layer security, Wireless Sensor Network, Network Construction, Dynamic Routing.

I. INTRODUCTION

Information is made sure about by applying the key-based enciphering (cryptographic) strategies in the upper layers of the system convention stack. In spite of the fact that these cryptographic techniques have indicated their adequacy in wired systems, the inborn trouble of mystery key conveyance/the executives without unified control and complex encryption calculations included may altogether constrain their applications in decentralized remote systems. This spurs the presentation of physical layer security (PLS) innovation as of late as the corresponding way to deal with further improving the security in remote interchanges. The way of thinking behind PLS is to abuse the common haphazardness of commotion and the physical attributes of remote channels (like blurring) to give data hypothetical security, which has been viewed as the most grounded type of security regardless of the registering capacities of busybodies. Therefore, PLS procedures are profoundly encouraging to ensure never-ending secure correspondence for remote systems. In the original work, wynerpresented the wiretap channel model as a fundamental structure for the investigation of PLS dependent on the Shannon's idea of flawless mystery. Thusly, many exploration exercises have been dedicated to investigating the PLS under other channel models, for example, non-corrupt channel, Gaussian channel, multi-radio wire channel and transfer channel. Spurred by these early investigations, different methodologies for improving PLS have been proposed in writing, which principally incorporate channel precoding/beamforming, agreeable sticking, channel coding and connection/transfer choice. This undertaking centers around the connection/transfer determination for making sure about the correspondence in remote helpful systems. The principle preferred position of connection/hand-off choice is its usage effortlessness, as the refined transmission strategies or express synchronization process isn't required.

The protected correspondence in a two-bounce agreeable remote system, where a cradle supported transfer advances information from the source to goal, and a detached spy endeavors to block information transmission from both the source and relay Limitations of leaving framework are Less security and Congestion happening.

Server will powerfully course the way with the goal that the parcels are moved to the goal progressively. The favorable circumstances are more security, cost is viable, effectively recognize the best course.

II. OBJECTIVE OF THE PROJECT

The aim of the project is to provide route from source to destination by finding energy, battery level, cost and throughput of the node.

III. LITERATURE SURVEY

This paper [1]- The mystery blackout execution of support helped multirole different info numerous yield agreeable frameworks within the sight of a latent meddler. Because of the inaccessibility of the channel state data of busybody's channel, a cradle supported joint transmit radio wire and transfer determination plot dependent on the fundamental channel is proposed to improve the mystery execution. In particular, they model of the advancement of the transfer cushions as a Markov chain and infer new definite and asymptotic shut structure articulations for the mystery blackout likelihood, which gives a productive method to evaluate the impact of framework parameters on the mystery blackout likelihood. In addition, basic asymptotic outcomes are additionally misused under two extraordinary situations.

This paper [2]- They propose two agreeable secure transmission plans to ensure a two-jump support helped arrange helped by a vitality collecting hand-off. In the main plan, they accept that the information on the vitality reaping

and blurring directs states is known in a non-causal way (disconnected). In the subsequent plan, they expect that this information is known in a causal way (on the web). For the two plans, they first structure a viable connection choice arrangement by assessing the transmission effectiveness and data security prerequisites. At that point they ideally designate the reaped force at the hand-off hub. For the disconnected plan, they boost the normal mystery rate under the steadiness limitations of the information line and the vitality line as indicated by the proposed connection determination approach, and structure a two-arrange iterative calculation to choose the transmission interface and dispense hand-off's transmit power. In the online plan, the first model the normal mystery rate most extreme issue as a Markov choice procedure, and afterward use the causal information to choose the best transmission connect and ideally apportion hand-off's transmit power. Likewise, the specific and asymptotic shut structure articulations are determined for the ergodic mystery rate. Numerical outcomes are introduced to approve the investigation and exhibit that the proposed plans beat the other cradled helped secure transmission plans helped by the vitality collecting transfer regarding normal mystery rate.

This paper [3]- A busybody which can catch the information transmission from both the source and transfer hubs is considered to undermine the security of transmission. Limited size information supports are thought to be accessible at each hand-off so as to abstain from choosing simultaneously the best source-to-hand-off and transfer to-goal joins. The proposed max-proportion transfer determination plot is appeared to beat one dependent on a maximum min-proportion hand-off plan.

This paper [4]- This paper explores the security-postpone exchange off of the cradle supported hand-off choice plan in a two-jump remote framework, which comprises of a source-goal pair, one spy, and numerous transfers each having a limited cushion. To assess the security and defer exhibitions of the framework, the infer logical articulations for the start to finish (E2E) secure transmission likelihood (STP) and the normal E2E delay under both great and halfway meddler channel state data (CSI) cases. These scientific articulations help us to investigate the natural exchange off between the security and postpone exhibitions of the concerned framework. Specifically, the outcomes right now that: 1) the greatest E2E STP increments as the requirement on the normal E2E delay turns out to be less severe, and such pattern is increasingly delicate to the variety of the quantity of transfers than that of the hand-off support size; 2) then again, the base expected E2E defer will in general decline when a less exacting imperative on E2E STP is forced, and this pattern is progressively touchy to the variety of the hand-off cushion size than that of the quantity of transfers.

This paper [5]-They proposed general-request transmit radio wire determination to upgrade the mystery execution of numerous information different yield multi- eavesdropper channels with obsolete channel state data (CSI) at the transmitter. What's more, likewise infer the likelihood of nonzero mystery limit and the ε-blackout mystery limit, individually. Straightforward asymptotic articulations for the mystery blackout likelihood uncover that the mystery decent variety request is decreased when the CSI is obsolete at the transmitter, and it is autonomous of the quantity of receiving wires at every busybody NE, the blurring parameter of the spy's channel ME, and the quantity of spies M. For Scenario II, they make a thorough investigation of the normal mystery limit acquired by the framework. In particular, new shut structure articulations for the specific and asymptotic normal mystery limit are determined, which are substantial for general frameworks with a subjective number of receiving wires, number of busybodies, and blurring seriousness parameters. Falling back on these outcomes, they additionally decide a high sign to-commotion proportion power counterbalance to unequivocally measure the effect of the fundamental channel and the meddler's channel on the normal mystery limit.

This paper [6]- The mystery execution of full-duplex hand-off (FDR) systems. The subsequent investigation shows that FDR systems have preferred mystery execution over half duplex transfer systems, if the self-impedance can be all around stifled. They additionally propose a full duplex sticking hand-off system, in which the transfer hub transmits sticking signs while accepting the information from the source. While the full duplex sticking plan has similar information rate as the half duplex plan, the mystery execution can be altogether improved, making it an alluring plan when the system mystery is an essential concern. A mathematic model is created to dissect mystery blackout probabilities for the half duplex, the full duplex and full duplex sticking plans, and the reproduction results are additionally exhibited to confirm the examination

This paper [7]- Due to the communicate idea of radio engendering, the remote air interface is open and available to both approved and ill-conceived clients. This totally varies from a wired system, where conveying gadgets are truly associated through links and a hub without direct affiliation can't get to the system for unlawful exercises. The open correspondences condition makes remote transmissions more helpless than wired interchanges to malignant assaults, including both the uninvolved listening stealthily for information capture and the dynamic sticking for upsetting authentic transmissions. Subsequently, this paper is propelled to look at the security vulnerabilities and dangers forced by the inborn open nature of remote correspondences and to devise effective resistance systems for improving the remote system security. They initially outline the security necessities of remote systems, including their valid, classification, uprightness, and accessibility issues. Next, a far-reaching outline of security assaults experienced in remote systems is exhibited in perspective on the system convention engineering, where the potential security dangers are examined at every convention layer. Likewise give an overview of the current security conventions and calculations that are embraced in the current remote system principles, for example, the Bluetooth, Wi-Fi, WiMAX, and the long-haul advancement (LTE) frameworks. At that point, they examine the best in class in physical-layer security, which is a rising procedure of verifying the open interchanges condition against listening in assaults at the physical layer. A few physical-layer security methods are audited and thought about, including data theoretic security, fake commotion supported

security, security-arranged beamforming, decent variety helped security, and physical-layer key age draws near. Since a jammer radiating radio signs can promptly meddle with the genuine remote clients, they additionally present the group of different sticking assaults and their countermeasures, including the steady jammer, discontinuous jammer, receptive jammer, versatile jammer, and insightful jammer. Also, they talk about the joining of physical-layer security into existing validation and cryptography systems for additional verifying remote systems. At last, some specialized difficulties which stay uncertain at the hour of composing are outlined and the future patterns in remote security are examined.

This paper [8]- Cooperative transferring is a compelling technique for expanding the range and unwavering quality of remote systems, and a few handing-off procedures have been received in significant remote principles. As of late, helpful transferring has likewise been considered with regards to PHY security, which is another security worldview to enhance customary cryptographic plans that generally handle security at the upper layers. In remote PHY security, hand-off hubs can be utilized to abuse the physical layer properties of remote diverts so as to help a tied down transmission from a source to a goal within the sight of at least one busybody. While a few leaps forward have been made right now zone, until this point in time, the issue of how to adequately receive progressed handing-off conventions to upgrade PHY security is still a long way from being completely comprehended. Right now, present a thorough rundown of current condition of-threat PHY security ideas in remote transfer systems. A contextual investigation is then given to evaluate the advantages of intensity designation and transfer area for upgraded security. They at last framework significant future research headings in handing-off topologies, full-duplex handing-off, and cross-layer plan that can touch off new interests and thoughts on the point.

This paper [9]- The fifth era (5G) system will fill in as a key empowering influence in fulfilling the persistently expanding needs for future remote applications, including an ultra-high information rate, a ultrawide radio inclusion, an ultra-huge number of gadgets, and an ultra-low inertness. This article looks at security, a significant issue in the 5G organize where remote transmissions are intrinsically powerless against security ruptures. In particular, they centre around physical layer security, which shields information classification by misusing the characteristic irregularity of the correspondences medium and receiving the rewards offered by the troublesome innovations to 5G. Among different advances, the three most encouraging ones are examined: heterogenous systems, enormous various info numerous yields, and milli-meter wave. Based on the key standards of every innovation, they recognize the rich chances and the extraordinary difficulties that security creators must handle. Such a distinguishing proof is relied upon to unequivocally propel the comprehension of future physical layer security.

This paper [10]- This paper gives a far-reaching review on different various receiving wire strategies in numerous radio wire hubs. In particular, they give a nitty gritty examination on different receiving wire strategies for ensuring secure interchanges in highlight point frameworks, double jump handing-off frameworks, multiuser frameworks, and heterogeneous systems. At long last, future research bearings and difficulties are distinguished.

This paper [11]- Physical layer security (PLS) has been broadly investigated as an option in contrast to ordinary cryptographic plans for verifying remote connections. Numerous examinations have demonstrated that the collaboration between the authentic hubs of a system can essentially upgrade their mystery correspondences execution, comparative with the noncooperative case. Spurred by the significance of this class of PLS frameworks, this paper gives an extensive overview of the ongoing deals with helpful transferring and sticking methods for verifying remote transmissions against spying hubs, which endeavour to catch the transmissions. In the first place, it gives an inside and out diagram of different secure transferring methodologies and plans. Next, an audit of as of late proposed answers for helpful sticking methods is furnished with an accentuation on power assignment and beamforming procedures. At that point, the most recent improvements in half and half procedures, which utilize both agreeable handing-off and sticking, are explained. At long last, a few key difficulties in the space of agreeable security are exhibited alongside a broad conversation on the utilizations of helpful security in key empowering agents for 5G interchanges, for example, nonorthogonal numerous entrances, gadget to-gadget correspondences, and gigantic different information various yield frameworks.

This paper [12]-They consider a square blurring underlay intellectual radio system where the essential system (PN) comprises of a source and a goal, and the auxiliary system (SN) has three hubs, in particular a source, a half-duplex interprets and-forward transfer, and a goal. They propose a novel connection choice convention for the SN with the end goal that the throughput of the SN is augmented while the normal or immediate obstruction to the essential goal is kept underneath a specific limit. Specifically, in the proposed convention, the auxiliary hand-off (SR) chooses ideally when to transmit information, get information, and be quiet. To this end, the SR is outfitted with a support for the capacity of data. In the proposed strategy, the obstruction from the PN to the SN is additionally considered and dropped by a crafty impedance cancelation plot. Their reproduction results show that for a given obstruction limit, the proposed connection choice convention beats the current transferring approaches revealed in the writing as far as these secondary throughputs.

This paper [13]- While mystery in correspondence frameworks have truly been acquired through cryptographic methods in the upper layers, late research endeavours have concentrated on the physical layer and have uncovered plentiful open doors for security structure. Specifically, the mix of sign preparing methods with channel coding for mystery has been key to the advancement of physical-layer security endeavour. Albeit verifiable coding methods for mystery have been known since the 1970s, express code developments have just been found inside the most recent decade. The motivation behind this article is to give an outline of the best in class in coding for mystery. They examine the general standards of coding, and they delineate

them with a few models. Specifically, they examine the significance of a settled code structure and stochastic encoding, which take into consideration the two-information unwavering quality and security.

This paper [14]- They explored the blackout execution of an intensify and-forward (AF) transfer framework that endeavours cushion helped max-connect hand-off choice. Both deviated and symmetric source-to-hand-off and transfer to-goal channel setups are considered. They determined the shut structure articulations for the blackout likelihood and investigate the normal bundle delays. They demonstrate that the assorted variety request is among N and 2N (where N is the transfer number), comparing to a hand-off support size among 1 and ∞, separately. In additional scientifically show the coding gain. Numerical outcomes are given to confirm the hypothetical examinations.

This paper [15]- It was based on two-hop communication link source send information to destination with 'trusted half duplex relay node' beware of eavesdropper 'between the source and destination there is no direct link'. Using ON/OFF power control it was proposed that maximum secrecy throughput, with the help of two-hop communication system, the results are demonstrated as numerical values.

This paper [16]-The ad-hoc network system was admired by the application of physical layer. It was mainly focused on a single hop and two-hop networks. It maintains high QOS and enhance the mounting and performance of the multi-hop network. Initially connection outage probability (COP) and then secrecy outage probability (SOP) will takes place. The final result hasbeen updated in the form of security QOS trade-off and to maintain the system performance effectively.

This paper [17]- This 'point-to-point secure communication over flat fading channels under an outage constraint'. All the more explicitly, they broaden the meaning of blackout ability to represent the mystery requirement and get sharp portrayals of the comparing key points of confinement under two unique presumptions on the transmitter channel state data (CSI). To start with, they discover the blackout mystery limit expecting that the transmitter has ideal information on the authentic and spy channel gains.

TABLE 1.

APPROCHES FOR AUTHOR/OBJECTIVE ANALYSIS

SI .NO	AUTHOR	OBJECTIVE
1	X. Tang	The productive method to evaluate the impact of framework parameters on the mystery blackout likelihood.
2	D. Wang	Two agreeable secure transmission plans to ensure a two-jump support helped arrange helped by a vitality collecting hand-off.
3	G. Chen	The security of transmission in cushion helped disentangle and-forward agreeable remote systems.
4	Y. Huang	To upgrade the mystery execution of numerous information different yield multi-eavesdropper channels with obsolete (CSI) at the transmitter.
5	G. Chen	The FDR systems have preferred mystery execution over half duplex transfer systems, if the self-impedance can be all around stifled.
6	Y. Huang	Double jump enhances

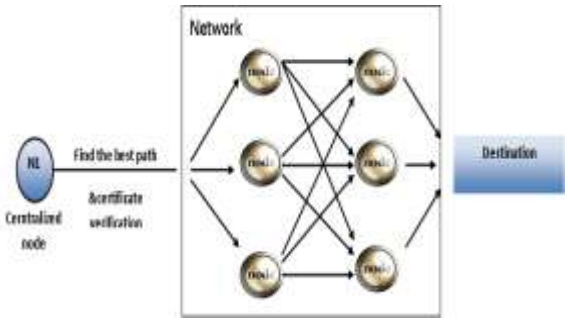
This paper [18]- 'They consider a secrecy relaying communication scenario where all nodes are equipped with multiple antennae. 'An eavesdropper has the access to the global channel state information (CSI)', and 'all the other nodes only know the CSI not associated with the eavesdropper'. Another mystery transmission convention is proposed, where the idea of obstruction arrangement is joined with helpful sticking to guarantee that counterfeit clamour from transmitters can be adjusted at the goal, yet not at the busybody because of the haphazardness of remote channels. Explanatory outcomes, for example, ergodic mystery rate and blackout likelihood, are created, from which increasingly astute comprehension of the proposed convention, for example, multiplexing and assorted variety gains, can be acquired. A couple of extraordinary cases, where blackout likelihood can't be diminished to zero paying little mind to SNR, are additionally talked about. Re-enactment results are given to exhibit the presentation of the proposed mystery transmission convention.

This paper [19] It was proposed that link selection policy for fastened communication over a 'buffer aided and two hop communication links. It was supposition to lend information to the destination with the aid of a trusted half duplex relay node beware of spy. At first, ordinary transferring conventions were equivalent parcel of the idea opportunity for the gathering and the transmission of the handoff is considered. In this manner a low unpredictability and asymptotically ideal connection determination on/off force control was proposed. Numerical output decides that the buffer aided two hop communication system is good in high throughput and improved in significance.

This paper [20]- They considered the safe transmission of data over an ergodic blurring direct within the sight of a everybody. It can be seen as the remote partner of wyner's wiretapper. The mystery limit of such a framework and is portrayed under the supposition of asymptotically long soundness interims. CSI case increases the real collector and the madder. Using SNR to goes to vastness, and curiously is appeared to accomplish the mystery limit under the full CSI presumption is secured correspondence over moderate blurring channel.

		and-forward multi-reception apparatus transferring frameworks over Rayleigh blurring channels, about the immediate connection between the source and the goal.
7	Y. Zou	The remote air interface is open and available to both approved and ill-conceived clients.
8	M. Agirwal	The vision of cutting edge 5G remote correspondences lies in giving exceptionally high information rates, amazingly low dormancy, and critical improvement in clients' apparent nature of administration (QoS)
9	L.J. Rodr´ıguez,	Compelling technique for expanding the range and unwavering quality of remote systems, and a few handing-off procedures have been received in significant remote principles.
10	N.J. Yang,	(5G) system will fill in as a key empowering influence in fulfilling the persistently expanding needs for future remote applications, including an ultra-high information rate, and an ultra-low inertness.
11	F. Jameel	Physical layer security (PLS) has been broadly investigated as an option in contrast to ordinary cryptographic plans for verifying remote connections.
12	A. Mukherjee	Physical layer security is to empower the trading of classified messages over a remote medium within the sight of unapproved busybodies, without depending on higher-layer encryption.
13	W.K. Harrison	The mix of sign preparing methods with channel coding for mystery has been key to the advancement of physical-layer security endeavour.
14	N. Zlatanov,	A system comprising of a source, a half-duplex deciphers and-forward hand-off with a support, and a goal. They accept that the immediate source-goal connect isn't accessible and all connections experience blurring.
15	Z. Tian	The shut structure articulations for the blackout likelihood and investigate the normal bundle delays. They demonstrate that the assorted variety request is among N and 2N
16	Y. Xu	It maintains high QOS and enhance the mounting and performance of the multi-hop network.
17	O. G¨ung	Point-to-point secure communication over flat fading channels under an outage constraint
19	X. Zhou	They are keen on the subject of how a lot of throughput should be yieldedforaccomplishinga specificdegreeof security.
19	Z. Ding	The counterfeit clamour from transmitters can be adjusted at the goal, yet not at the busybody because of the haphazardness of remote channels.
20	P. K. Gopala	They considered the safe transmission of data over an ergodic blurring direct within the sight.

IV. ARCHITECTURE DIAGRAM



V. PROPOSED SYSTEM:

In the Proposed System, this system depends on a multi-root binary-tree organize geography whose roots fill in as centres. It is demonstrated that this system can be worked utilizing a basic self-directing circuit exchanging calculation dependent on bit-deciphering. With pipelining, it offers to create parcel stream rates up to the most extreme physical limit of its connections as the directing time adds up to unravelling the slightest bit at each switch along a way between two centres

VI. MODIFICATION:

Change is our Implementation; we break down optimal Route for information move into the goal in any system. Source node needs to sends sham bundles to examine the best accessible course that interface the goal. We are executing this venture in Wireless Sensor arrange, so the courses would progressively in portability design. So, our framework needs to break down each hub's Capacity, Cost, throughput, Battery level to move the bundles to the goal. After the investigation, server will powerfully course the way with the goal that the parcels are moved to the goal progressively. In view of the hubs dynamic conduct Self Routing framework is actualized.

VII. MODULE DESCRIPTION

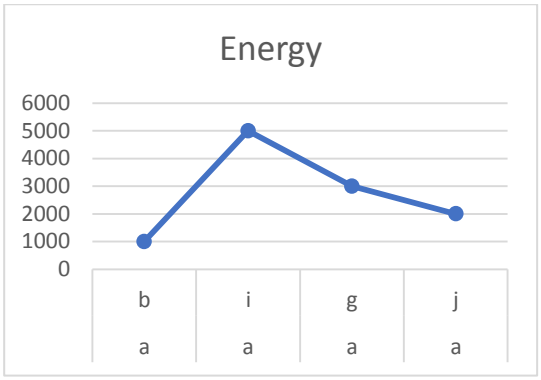
NETWORK CONSTRUCTION:

We create network topology to avoid security problem. Network has many numbers of node details. It maintains the connection details also. Nodes are interconnected and exchange data with other nodes. Nodes are connecting with other nodes in the network. All node should pass a dummy packet to know the battery level, capacity, throughput and cost of node.

BATTERY ANALYSIS:

In this module analyse capacity of battery and its lifetime according to the set of tasks executed by the nodes. After knowing it the data should transferred from one node to another. Every node has to know the battery level of predecessor node. After that only data will transfer.

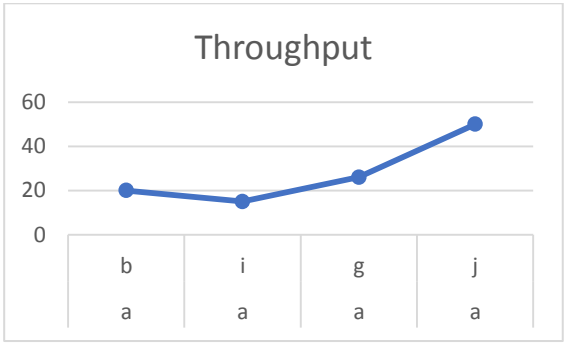
Source	Path	Energy
a	b	1000
a	I	5000
a	g	3000
a	J	2000



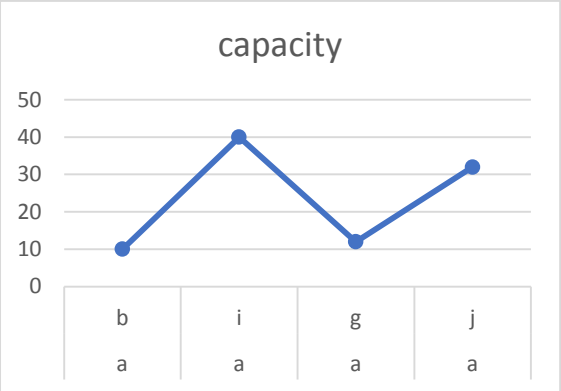
CAPACITY AND THROUGHPUT:

A common strategy for playing out an estimation is to move an 'enormous' record from one. The throughput is then determined by separating the document size when to get. The Reasons for estimating throughput in systems. Individuals are frequently worried about estimating the greatest information throughput in bits every second of an interchanges connection or system get to. A regular technique for playing out an estimation is to move an 'enormous' document starting with one framework then onto the next framework and measure the time required to finish the exchange or duplicate of the record. The throughput is then determined by separating the record size when to get the throughput in megabits, kilobits, or bits every second.

Source	Path	Throughput
A	B	20
A	I	15
A	G	26
A	J	50



Source	Path	Capacity
A	B	10
A	I	40
A	G	12
A	J	32



COST ANALYCIS:

In this module the network will determine the flexible path to transfer the data from the source node to the destination node. There will be many paths will be available from source node to the destination node. So that the data will be transferring via the path which has the highest connectivity so that the data will reach the destination node in reliable manner. so, for every node has their energy and cost of that node is calculated so that based on the cost we can send the data and it choose the shortest path. Will lead to no packet loss in the network.

Source	Path	Cost
A	B	200
A	I	400
A	G	100
A	J	300

DYNAMIC ROUTING:

Dynamic routing is a networking technique that provides optimal data routing. If any node is busy in decided route automatically it will take dynamic route to send the information.

BEST ROUTE BASED ROUTING:

The modification that we are doing in this project is Capacity Calculation. If the Source hub needs to send the information to the goal hub by means of adaptable ways and there are numerous adaptable ways are accessible to send the information to the goal hub. As of now we are figuring the limit of the accessible ways. So which way is having the most elevated limit, with the goal that the information will be sends to by means of that way to the goal hub?

VIII. CONCLUSION

Through this project we send information from source to destination in secured way. The data should be sent through node by identifying its battery capacity, cost and throughput. So, data will not be hacked by anyone.

IX. REFERENCE

[1] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," 2018 (to appear). https://ieeexplore.ieee.org/document/8437135

[2] D. Wang, P. Ren, and J. Cheng, "Cooperative secure communication in two-hop buffer-aided networks,",Nov.2018.https://ieeexplore.ieee.org/document/8116649

[3] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," Jun.2014.https://ieeexplore.ieee.org/document/6746659

[4] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," 2008. https://ieeexplore.ieee.org/document/4626059

[5] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," Aug.2015.https://ieeexplore.ieee.org/document/7118654

[6] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," Mar.2015.https://ieeexplore.ieee.org/document/7004893

[7] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," 2016. https://ieeexplore.ieee.org/document/7514758

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trend2016. https://ieeexplore.ieee.org/document/7467419

[9] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," IEEE Commun. Surveys Tuts., vol. 18, no.3, pp.1617–1655, Feb.2016. https://ieeexplore.ieee.org/document/7414384

[10] Jing Wan, Deli Qiao, hui-Ming Wang "Power control land link selection" https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=7693