Enhancing Video Quality of Service by using Zone Routing Protocol in Wireless Networks

A.Vijayaraj[1] , P.Gururama Senthilvel[2] , Vasanth Raj P.T[2], P.Ramadoss[3], K.Mariappan[3]

[1]Associate Professor, Department of IT, Vignan's Foundation for Science, Technology and Research, Guntur, AP, India.

[2]Associate Professor, Department of CSE, Meenakshi College of Engineering , Chennai,Tamil Nadu, India.

[2]Center for System Design Chennai Institute of Technology , Chennai, Tamil Nadu, India.

[3]Assistant Professor, Department of IT, Vignan's Foundation for Science, Technology and Research, Guntur, AP, India.

[3]Assistant Professor, Department of IT , Vels Institute of Science Technology & Advanced Studies, Chennai, Tamil Nadu, India.

satturvijay@gmail.com, gurupandian.cse@gmail.com, vasanth14191@gmail.com, vp.ramadoss@gmail.com, mari.tvtg@gmail.com

Abstract: The usefulness of wireless mesh networks has improved progressively over time due to their flexibility. A wireless mesh network, as its name implies, it is a network of interconnected wireless routers connected in a mesh topology, where data is transported via multiple transmission paths. An important component of an effective video security system is the implementation of the RSA algorithm to encrypt and decrypt the video. The ViLBaS concept is an existing concept, which detects all of the network's nodes and confirms which of the network's nodes is most impacted by the congestion. This concept is concerned with the OLSR protocol and how it is used to transport packets from the sender to the receiver. The system incorporates the ZRP protocol instead of the OLSR protocol in the proposed system. A similar idea can be implemented by utilizing a zone routing protocol. There are two protocols used in zone routing: the proactive protocol and the reactive protocol. We use "Proactive" techniques in which we send the packet directly to the receiver if both the sender and receiver are in the area defined. Reactive protocols will send the packet to the receiver if it is outside the reactive area. All quality-of-service parameters were assessed at the end.

Keywords: Routers, Mesh topology, MPEG video, Congestion, Zone routing, Proactive, Reactive

1. Introduction

A critical requirement in setting up a wireless mesh network is for all the routers in the network topology to be in communication with each other. They must then communicate the data stream in a multi-hop fashion. It is lightweight and has very high maneuverability. This paper improves the Quality of Service, which can be defined as things like output, delay, etc. ViLBaS is a type of load balancing that especially optimizes the distribution of video content. Also, it increases the overall efficiency of wireless mesh networks. To help relieve congestion and avoid data drops, the ViLBaS observer's traffic flow looks for the node that causes the most arrogance among congestion and then routes video streams away from the node. The actual stream of video being sent from a sender node to a receiver node in a wireless mesh network topology is what we consider to be the true state of video delivery. Wireless mesh networks can support multiple users simultaneously, and these networks are vulnerable to congestion because congestion issues frequently require a node to be redirected via flow selection. The node activity detector was used to detect the congested node. The Node Activity sensor (i.e.) the detection of the congested node when the queue occupancy level increases. No one except the user can change the occupancy level of the queue. If the level gets to that point, congestion will happen. When the network becomes congested, the sender can identify the congested node and select a new flow that utilizes the least risky transmission method. Identifying the less loaded node allowed the new flow to be selected, and a new path was selected so that the packet could be sent through the identified less loaded node. To use the new path if the previous path is congested, it must monitor for determining whether or not the previous path is affected by congestion. It must be concluded that the new route has also been impacted by congestion and, therefore, it should be chosen. Implementing the new routing would mean that the packet will be sent directly to a recipient. Security Analysis uses batch testing as a way of ensuring a batch is complete. The Batch verification technique is used to check the validity of all the nodes in the network. The legitimate and invalid data can be classified with the aid of the key-value and node ID. To sum up, all authentication should be performed and the data should be transferred from the sender to a destination point by using Relay nodes. A relay node is generated

automatically to represent the relative energy efficiency of the node. The new path is designed to help the path determination process run more smoothly. It is to make sure that if the previous path becomes clogged, the new path is not affected. Congestion should be observed, and then a new direction should be chosen. This latest routing implementation would result in the packet being sent directly to a recipient. When one of the less loaded nodes in the network was found, the news flow was chosen. The new flow has been chosen, and so the packet will be sent along the new route. To aid in the transfer of data from one location to another, two relay nodes will be established. the packet will be sent directly to a receiver with the introduction of the current routing Identifying the least loaded node in the flow of traffic led to identifying the new route, and by identifying the new path, the packet was then sent down the newly discovered path. Two relay nodes will be set up to carry out the transfer of data from one location to another. The recipient of the encrypted message will decrypt it after arriving at the destination. To sum up, all authentication should be performed and the data should be transferred from the sender to a destination point by using Relay nodes. To maximize efficiency, the new path will keep an eye out for deciding whether the previous path is impacted by congestion or not, and if the previous path is impacted by congestion, the new path should be chosen. A new path will be set up, which will enable the packet to be sent directly to the receiver. This latest routing implementation would result in the packet being sent directly to a recipient.

2. Related Works

This is how Wireless Mesh Networks (WMN) are applied in video surveillance: they provide a wonderful opportunity for placement in a wide-ranging community, for which consistency and efficiency are the two most important difficulties for delivering video to the public at high speeds [1]. While, present routing protocols do not give rise to a positive result when attempting to balance the workload for video communication necessities, such as distributing traffic for important facts and providing delay requirements. In the case of a proposed application of Field-based AnyCast Routing (FAR) protocol [1], which collects corrupted routing information, the said route will consume debauched forces. Mobile Ad hoc networks will describe the optimized link-state routing protocol in [3][4]. One of the main concepts used in the multi-point relays is the wireless LAN. Additionally, it distributes all of the mass messages during the overflow phase. The protocol has been tailored to the needs of a mobile wireless LAN by optimizing the link state algorithm while taking into consideration the requirements of mobility. One of the most important concepts used in the protocol is that of Multi Point Relays (MPRs). Nodes that act as MPRs participate in the flooding process and do so by forwarding broadcast messages [3] and [7]. Use of the OLSR protocol to constrict the overflow results in the opposite of the video flowing. In the long run, data loss and the additional transfer of data packets would make the data packets sent from sender to receiver travel at a reduced pace. The video transmission stream includes the sending and receiving locations' routing information, which is used to move the data from one location to another. At the same time, the intermediate node will gather all the information about the receiver side (referred to as the receiver's endpoint) [13] and [14]. With the optimization technique, we will generate a simulation of the result as if it were derived from assumptions. The simulation-based technique that details the random flow of data. A Vijayaraj, P DineshKumar[15], expressed the census management with PDA demonstrated that carefully enumerating and presenting census data is simple and painless. In such a large country as India,

The RSA count proposed by Rivest, Shamir and Adleman as an open key cryptosystem is used as a piece of different correspondence frameworks to ensure data mystery. A variety of issues were defined about this estimate, and in that way, several issues for consideration can be produced. Extending this computation was made feasible in this paper since it produced a greater amount of money and allowed people to take a longer time to sign up. An enhanced encryption strategy that can be connected with the RSA key time framework. The suggested procedure relies on a quick and dirty examination of the logarithmic restricted fields. The upgraded count can be executed on new time frameworks (second-period frameworks and so forth) and applies to remote frameworks with Bluetooth contraptions which require extended security by the development of the utilization area. Meanwhile, we have used an impressive lengthy encryption key, which improves speed and security, and the multidimensional nature of the calculation. This results in an enhanced calculation rate while retaining the processor's capabilities.

Propelled mark has been giving security organizations to secure electronic trade over the web. The RSA computation was most for the most part used to give a security system. Now we have balanced the RSA count to update its level of security. This paper provides a rationale between RSA and Revised RSA computation in a timeframe that's close to real-time and significantly increases security by allowing users to do encryption and unscrambling when working with varying sizes of data. It was recognized that the estimated financial performance of these predictions took into consideration recent key interest and security levels. A combination of RSA and balanced

RSA computations was used to code and decode various sizes of compositions. In terms of security, two levels better than unmodified RSA, the diversion result shows that in modified RSA, calculating the key period is quicker, and as a result, it increases security. RSA figuring is speedier than Modified RSA to the extent of encryption and disentangling speed. An important concept to grasp in the multipoint exchanges is the remote LAN. Using the surge technique, the show sends messages to users. In other words, the tradition is the change of the settings associated with a system that was redone to have a convenient remote LAN. For example, one important thought that people have included in their tradition is that of MultiPoint Relays (MPRs). Data loss and passing on of additional data is accomplished relatively as all the data from the sender gets sent to the beneficiary. the video movement stream contains the purpose of being energetic and upbeat to support the table's move to send data, starting at one location and proceeding to the next. To hand over all of the bits of knowledge from the source to the destination, the transitional center will acquire all of the data on the beneficiary side [13] and [14]. Instead of producing one story based on only one assumption, the strategy will yield entertainment-based conclusions. The diversion-based framework describes the flood of data using non-verifiable concepts. Yuhua Lin et. al [16] proposed a strategy for discovering supernodes by taking into account the credibility of the information provided. Because of the previously mentioned evidence, we firmly believe in employing a receiver-driven encoding rate adaptation strategy to monitor these two variables and guarantee the quality of service, provided that different games have different degrees of latency tolerance and packet loss tolerance. H. Facchini et. al [17] determined the actions and effect of video traffic on WAN networks, a quantitative analysis is carried out through experimentation. We suggest a fourth sub-scenario WAN testbed that enables unicast or multicast video traffic compressed with multiple codecs to be inserted. We found some important performance and QoE metrics from the capture of video traffic, such as unicast and multicast throughput, delay, jitter, and Pareto propagation. Abubakr O, et al [19] proposed an edge-cache-aided CDN-based over-the-top multicast video streaming method, where the video material is partly cached on distributed cache servers and the edge-cache makes use of an access-dependent online edge caching solution. Besides, by using two-stage probabilistic scheduling for the options of servers and the concurrent streams between the server and the edge router, we are also able to ensure excellent throughput efficiency. This paper optimizes the weighted stall period tail risk. M Sanjay Ram, A. Vijayaraj[22], suggested a method for creating a trusted computing framework for cloud computing systems by incorporating a trusted computing platform into the system and paying close attention to the security requirements in the cloud computing environment.

Michael Seufert and et. al[20] described the boost turnover and avoid attrition, and in doing so, they have the goal of providing their clients with the best service. Reactive traffic control also functions as a part of QoE in the network operators' responses to changes in their traffic patterns. Furthermore, the ability to deliver an excellent user experience frequently results in the desire to implement specifications regarding user activity and operation. Irena Orsolic et al [21] described the steady and, up until now, a growing increase in global network traffic. Much of this traffic is coming from the large number of online video streaming platforms, which causes network operators to have to manage their resources effectively while also fulfilling customer requirements and demands. If one wishes to maintain video quality and efficiency for the end-user, it is important to perform application-level monitoring and analysis of key Performance Indicators (KPIs) such as the End-User Performance Indicators (EUPIs) that precisely gauge end-user QoE. R Srinivasan, A Vijayaraj [18], suggested new approaches for designing optimised FSO network structures based on mixed integer programming formulations to increase connection availability and high data rate, while also taking into account the allocation of restricted bandwidth. Our findings point us in the right direction for designing a high-efficiency reconfigurable FSO network.

3. Architecture Overview

To help relieve congestion and avoid data drops, the ViLBaS observer's traffic flow looks for the node that causes the most arrogance among congestion and then routes video streams away from the node. A streamed video transmission that originated from a sender node in a wireless mesh network. Wireless mesh networks such as the one created in our office have a single point of failure which frequently leads to congestion. To counteract this, traffic rerouting takes place via flow selection. Recognized by using a node activity detector, the congested node was referred to as "overburdened." To detect, the Node Activity sensor identifies (i.e.) that the node is congested due to queue occupancy level. No one except the user can change the occupancy level of the queue. If the level crosses the congestion threshold, the condition will occur. Once the congested node has been detected, a new flow will be chosen to deliver the packet to the destination. Possible flows identified, from the one with the least loaded node, lead to the selection of a new path and consequent route to the packet. If the new path encounters congestion, it should

automatically determine whether the earlier path is affected by blocking or not. If the earlier path is affected by blocking, the new route should be selected. It is designed to ensure that the packet is delivered straight to the receiver.

A. Architecture Description

Mesh networking typically relies on random packet sampling or some kind of hand-off between source and destination network to avoid having lags in data delivery. This load balancing service can virtually eliminate any packet loss that might occur on the distribution path between these two networks. ViLBaS is used to find the node on the network with the highest amount of snootiness, where the traffic becomes congested, and moves the network video streams away from that node to avoid network data drops. The congested node was discovered through the use of a node activity detector. In other words, the Node Activity sensor will be able to identify whether or not the node is complete. No one except the user can change the occupancy level of the queue. If the level reaches congestion, the system will become overloaded. Once a single-arriving packet can be found to be in critical condition, the best alternative course of action is to choose is selecting another flow that has not already busied the packet forwarding device and enqueuing it. To determine if the new path should be chosen, it will keep an eye out for finding that the path isn't slowed down or not, it looks for whether the previous path is affected by congestion. When congestion is detected, a new alternative should be searched. By implementing the original routing, the packet will be sent straight to a receiver. To find the less loaded node, the news flow was used to identify the node, and through the node, the packet will be sent along the original path. To avoid having to make the initial calculation over and over again, the new path should attempt to determine if the earlier route is disturbed by congestion. The new path should be picked if the previous path has been impacted by congestion. This improves overall performance as the packet is directly forwarded to the recipient. Automatically a relay node is installed to match the node's performance. To verify whether the new path is affected by congestion, the path tracing framework shall monitor the previous path for that status and take appropriate action if the previous path has been impacted by congestion. By implementing the new routing, the packet will be sent straight to a receiver.

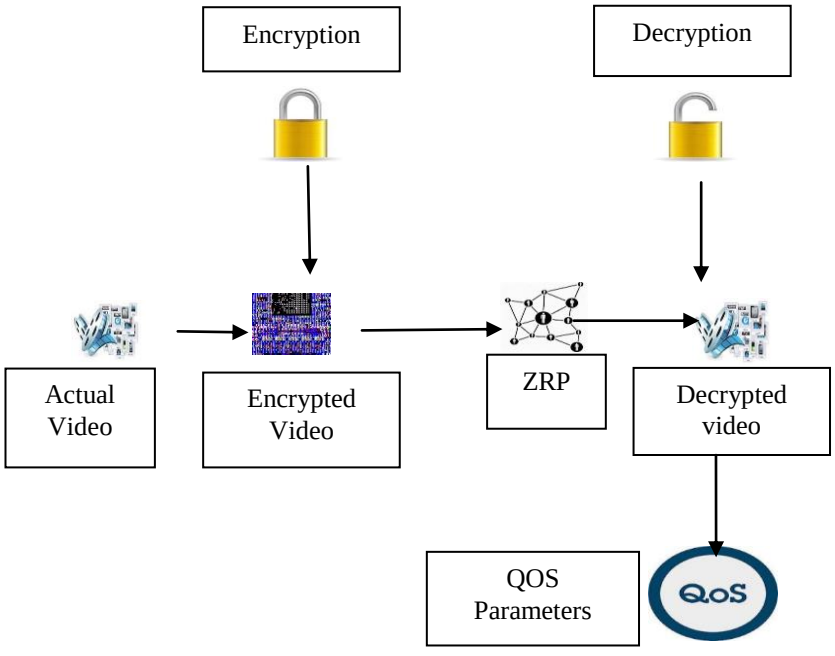

Figure1. Architecture Diagram

B. MPEG Video Security

It was carried out on a 30-node network. Nodes are formed for data packets to be sent and received. Decryption is performed by RSA Algorithm for encryption. For each node, it is possible to create node ID and key-

value automatically. For cryptography on the sender side, the public key is used, and on the destination side, the private key is used. The batch check approach is used in Security Analysis. Using the batch test approach, valid and invalid nodes are identified in the network. With the help of key-value and node ID, valid and invalid can be found. All checks should be carried out, and the data should be transmitted from the sender via Relay nodes to the destination point. Depending on the effectiveness of the node the relay node is built automatically. If the new path can be chosen, then it is monitored to detect whether or not congestion affects the previous path. A new route should be chosen if congestion is encountered. The packet is directly forwarded to a recipient by applying the new routing. To identify the less loaded node, the new flow is selected by designating a path with a lesser amount of data load. Once a path is determined to have a lower data load, packets are sent on that path. Two relay nodes will be established to send data from one location to another. The receiver will decrypt the message once they reach the destination point. When considering if a new path is to be picked, it will monitor whether or not congestion affects the earlier path. A new route should be picked if congestion is detected. With the new path, the packet is forwarded to the receiver directly.

Node Model

- It was carried out on a 30-node network
- Nodes are formed for data packets to be sent and received

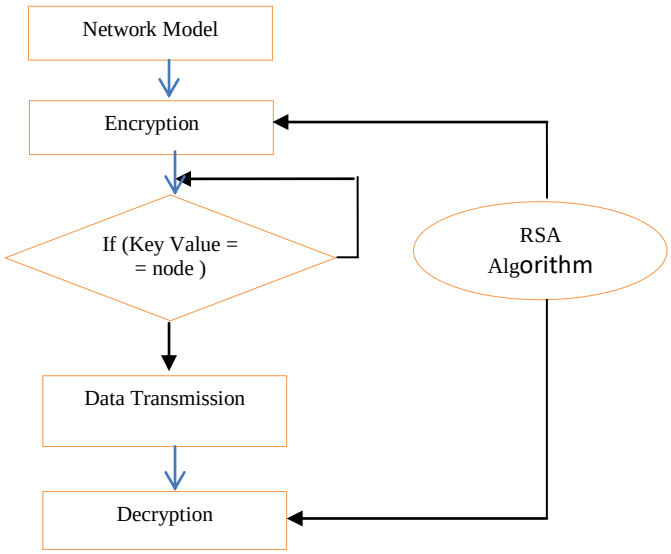

Figure 2. MPEG Video Security

C. RSA Algorithm

One of the main practical public-key cryptosystems is RSA and is widely used for the secure transmission of information. The encryption key is open in such a cryptosystem and contrasts with the decryption key that is kept a mystery. This asymmetry in RSA depends on the common-sense problem of factoring the factoring problem out of two large prime numbers. Ron Rivest, Adi Shamir and Leonard Adleman make up the RSA algorithm. Given two large prime numbers, alongside an assistant quality, an RSA customer makes and then distributes an open key. It is necessary to keep the prime numbers mysterious. Anyone can use the general society key to scramble a message, but with distributed techniques right now, if individuals are sufficiently substantial in general key, only someone can disentangle the message with the learning of the prime numbers. Breaking RSA encryption is referred to as the RSA problem; an open inquiry remains whether it is as difficult as the problem under consideration. RSA is a moderately moderate calculation, and it is less commonly used to scramble customer data directly because of this. More often, for symmetric-key cryptography, RSA passes encoded shared keys that can therefore perform mass encryption-decoding operations at a much higher speed.

D. Batch Verification

- The batch check approach is used in Security Analysis.
- Using the batch test approach, valid and invalid nodes are identified in the network.
- With the help of key-value and node ID, valid and invalid can be found. Transfer of data
- All checks should be carried out, and the data should be transmitted from the sender via Relay nodes to the destination point.
- Depending on the effectiveness of the node the relay node is built automatically.
- To transmit data from one place to another, 2 relay nodes will be established.
- The message will be decrypted by reaching the destination point.

4. Zone Routing Protocol

The Zone Routing Protocol(ZRP) is a protocol that prevents packet loss by providing an effective method of sending the packet from the sender to the destination. ZRP is a process that uses two protocols, a proactive protocol and a reactive protocol to send the packet from one place to another. The zone contains an area in which all nodes belong to a specific zone with numerous nodes. The ZRP divides or splits the region where the packet is sent from one place to another. With the help of a hop-count, the zone can be split or divided. The overhead problem should be reduced by the hop-count. This area routing protocol can mitigate the loss of packets, improve service quality such as throughput, simulation delay, bit rate, etc. Quality of service parameters such as performance, simulation delay, increase in bit rate. The Zone Routing Protocol is used to speed up the process of senders to the target point. The Zone routing protocol shall store all details on the transmitters and destinations for an efficient data flow. The neighbor node sends the packet to the following hop for all nodes that have neighbor node specifics. Proactive is a protocol that can be used within the same area for the sending of the protocol. Send packets from the same area directly. Reactive is a protocol to deliver a packet outside the area. If the target is not located within the same zone, the packet will be sent from sender to recipient by the reactive protocol. The ZRP should be IARP and IERP. The IARP should deliver the packet to the same area and classify or disconnect the number of hop counts by country. The user number of trips should split a zone. The sender and recipient will send the packet directly from the recipient to the receiver within the number of trips or the IERP will send the packet that identifies the route previously determined by inspecting the congestion node. If not, that means you can pick a route and forward the packet to the recipient.

A. Node Activity Detector

The Node Activity Detector detects which node has more data and monitors its queue level. The queue level to be determined by the user only. It results in acceptance if the occupancy level of the queue exceeds. The congested node is monitored by the activity sensor of the node. When the queue is tracked, the congested node is regulated. Every path should communicate with each other when one node is affected by congestion; the route together with the node should affect congestion. More data to bring the route than another path node. The detector of node activity The detector should identify the node receiving more data, which should be identified using the activity node detector.

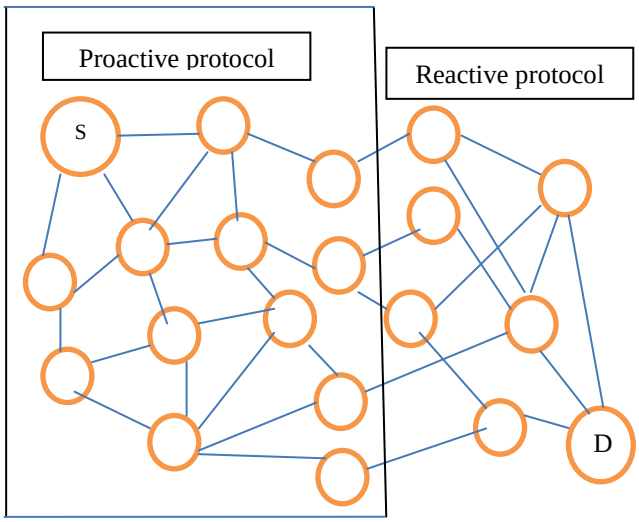

Figure 3. Zone Routing Protocol Diagram

B. Flow Selection

The flow selection monitors, when a blocked node is detected, what node holds fewer packet numbers and which route is appropriate for safe forwarding of the packet to the recipient. The safest route should be established using the flow selector. The flow selector chooses the flow to transmit the transmitting data to the receiver without interruption or loss of data. It examines which node and which path contains additional data, which path is suitable for transmitting data to the sender-receiver. The route should choose which flow contains more than the queue occupancy to be recognized and which finds a new flow for selection using a flow selector. During the re-routing process, the Routing Table and the Intermediate Node will update sender and recipient data. The data should be sent from one location to another by many senders and receivers in the wireless mesh node.

C. Previous Node Identifier

It checks whether or not congestion affects the last node. Another flow is searched by submitting a packet when it gets affected by congestion. A routing algorithm is the area routing protocol used in this ViLBaS notion. A protocol is a proactive and reactive protocol for zone routing. With the proactive protocol, the sender and receiver send the packet straight to the receiver within the same vicinity. The sender and recipient send the packet outside the reactive protocol zone from one zone to another. The ZRP should be IARP and IERP. The IARP should deliver the packet to the same area and classify or disconnect the number of hop counts by country. The user number of trips should split a zone. The sender and recipient will send the packet directly from the recipient to the receiver within the number of trips or the IERP will send the packet that identifies the route previously determined by inspecting the congestion node. If not, this means a path can be selected and the packet can be sent to the receiver.

D. New Route Selector

The packet to send data in various flows will be selected. The packet certainly can't reach the receiver section if the chosen route is affected by congestion. The New Route Selector will help you choose a new route by inspecting uncontrolled routes. The new route selects an uncongested node from the sender to the receiver to transfer the video. The new path to the congested node should be selected while the data is transferred from one sender to the receiver. You should select the most secure path to send a packet without dropping the packet.

E. Quality of service analysis Parameters

The whole system's achievement is known as the quality of service. Only consumers can monitor the complete performance of a system. To measure the quality of service levels such as transfer delay, bit rate, video quality, availability of video streams, performance, etc. Some parameters should be measured in the video quality level, which can improve both software and video quality. The photographs or photographs may be blurred, gentle, and collated with other video stream images, etc. The video stream should be measured according to quality of service parameters.

Zone Routing Protocol Algorithm

Data Types: Video packs, wireless mesh nodes

Result: Achieving video traffic load balance

Step 1: Start

Step 2: start node = n;

Step 3: Initialise node-level = nl;

Step 4: Initialise q = 0;

Step 5: Mark high loaded node with hl;

Step 6: Mark the loaded node with ll less;

Step 7: if (q>nl) hl; other ll;

Step 8: Data encryption

Step 9: Check for data transmission.

Step 10: Decrypt recipient data

Step 11: Finish

Table I

Simulation Set-up

Factors	Values
Emulator	Network Simulator 2
Node	100 m
Queue Size	75
Routing Protocol	ZRP
Data Type	MPEG 4
Onset Percentage	70%
Video MBR	150 kbps

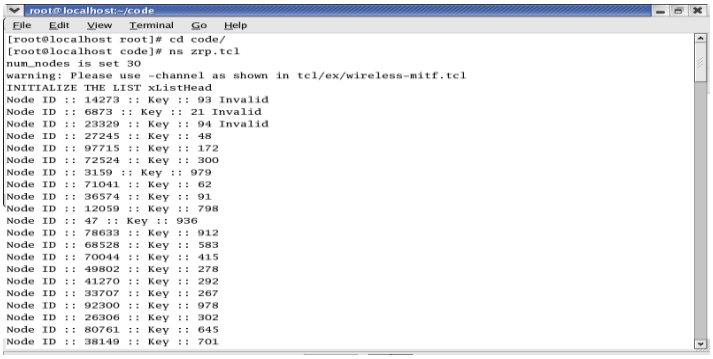

Figure 4. Valid and Invalid Identification

The batch check approach is used in Security Analysis. Using the batch test approach, valid and invalid nodes are identified in the network. With the help of key-value and node ID, valid and invalid can be found.

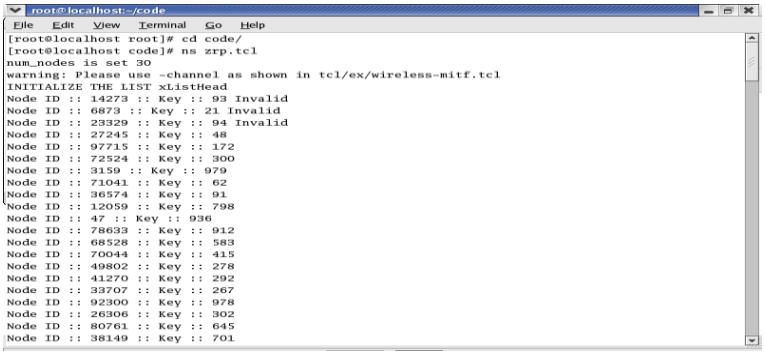

Figure 5. Key-value and Node ID generation

In the 30 nodes are created and node 0 acts as a sender and node 18 as the recipient. To transfer the data from the sender side to the receiver side, the relay node should be chosen. Depending on the distance between the transmitter and the receiver, the relay node must be developed. The data can be transferred from sender to destination by using relay nodes using Zone Routing Protocol. Depending on the distance between sender and destination, relay nodes should be built.

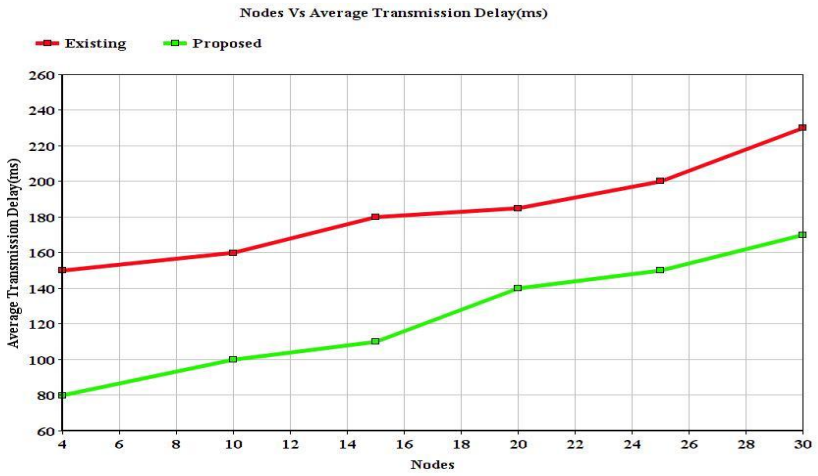

Figure 6. Nodes Vs Transmission Delay

The current system often automatically increases the number of nodes, and in this system, the transmission delay is shorter than in the current system.

Figure 7. Simulation Time Vs PDR

In the current system, the number of nodes automatically adjusts the packet delay Ratio, but the packet delay ratio for the proposed system is lower than the existing system.

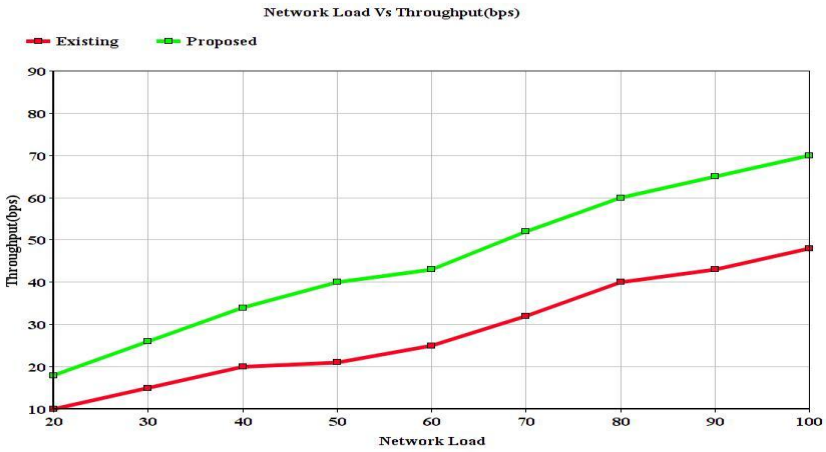

Figure 8. Network Load Vs Throughput

The current system automatically adjusts the node load level and reduces the throughput level, so the current system is lower than the current system.

5. Conclusion And Future Enhancement

A node through congestion is found most pretentious by the system traffic flow of the ViLBaS observer and data drops are avoided by redirecting the video stream near the overfilled node. The current stream of the video circulation from a sender node to a receiver node in a telecommunications network topology. All people are transferring a packet to the Wireless Mesh network recipient to re-route the packet node by flow selection, in many situations the congestion happens. By using the node activity detector, the congested node is identified. The new road will be tracked to ascertain whether or not the previous path is influenced by congestion and if it is affected by congestion, the new path should be chosen. The packet is delivered directly via the new path to the recipient. The overhead will be reduced by using the Zone routing protocol. The ViLBaS principle in conjunction with the Future Enhancement Zone Routing Protocol ensures security during the transmission of the packet from sender to receiver. No packets would be sent and received at the same time in the Wireless Mesh Network 'n' Data can be lost at that

time or some other node can hack it. Improving the level of quality of experience is the future improvement of this project (QoE). The packet cannot be compromised by hackers or any other nodes by providing security.

References

[1]. Bahr.M. (2006), 'Proposed routing for IEEE 802.11sWLAN mesh networks, 'in Proc. 2nd Annu. Int. Workshop Wireless Internet (WICON). Boston, MA, USA, Art. ID 5.

[2]. Clausen.T and Jacquet.P. (2003),'Optimized Link State Routing Protocol (OLSR)',IETF Standard RFC 3626 (Experimental).

[3]. De Couto.D.S, Douglas.S.J, Aguayo.D, Bicket.J, and Morris.R. (2005),'A high-Throughput path metric for multi-hop wireless routing,' Wireless Networks, vol. 11, no. 4, pp. 419–434, 2005.

[4]. Draves.R, Padhye.J, and Zill.B. (2004),'Routing in multi-radio, multi-hop wireless meshnetworks,' in Proc. 10th Annu. Int. Conf. Mobile Comput.Netw. (MobiCom), Philadelphia, PA, USA,pp. 114–128.

[5]. Hava.A, Muntean.G.M, Ghamri-Doudane.Y, and Murphy.J. (2013), 'A new load balancing mechanism for improved video delivery over wireless mesh networks,' in Proc. IEEE 14th Int. Conf. High Perform. Switch. Routing (HPSR), Taipei, Taiwan, pp. 136–141.

[6]. Johnson.D, Hu.Y, and Maltz.D.(2007), 'The Dynamic Sender Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4', IETF Standard RFC 4728 (Experimental),[Online]. Available: http://www.ietf.org/rfc/rfc4728.txt

[7]. Perkins.C, Belding-Royer.E, and Das.S.(2003),' Ad Hoc On-Demand Distance Vector (AODV) Routing', IETF Standard RFC 3561 (Experimental).

[8]. Wang.Zand Crowcroft.J.(1996), 'Quality-of-service routing for supporting multimedia applications,' IEEE J. Sel. Areas Commun., vol. 14, no. 7, pp. 1228–1234.

[9]. Yang.Y, Wang.J, and Kravets.R, (2005),'Designing routing metrics for mesh networks,' in Proc. IEEE Workshop Wireless Mesh Netw. (WiMesh), Santa Clara, CA, USA.

[10]. Frank H. P. Fitzek, Technical University Berlin Martin Reisslein, Arizona State University(2001)"MPEG-4 and H.263 Video Traces for Network Performance Evaluation".

[11]. Ricardo Matos, Nun Coutinho(2012) proposed "Quality of Experience-based Routing in Multi-Service Wireless Mesh Networks."

[12]. Mulaz Kserawi, Sangsu Jung (2014), proposed "Multipath Video Real Time Streaming by field-Based Anycast Routing".

[13]. Peter Orosz, Tamas Skopko, (2014) proposed "A Case Study on Correlating Video QoS and QoE".

[14]. Yanjiao Chen (2015), proposed "From QoS to QoE: A Tutorial on video Quality Assessment".

[15]. A Vijayaraj, P DineshKumar "Design and implementation of census data collection system using PDA" , International Journal of Computer Applications, Volume 9 , Issue 9 Pp 28-32 , 2010.

[16]. Yuhua Lin, Member, and Haiying Shen, 'Cloud Fog: Leveraging Fog to Extend Cloud Gaming for Thin-Client MMOG with High Quality of Service', IEEE Transactions On Parallel And Distributed Systems, Vol. 28, No. 2, Pp.431 445, February 2017.

[17]. H. Facchini, S. Pérez, L. Marrone and F. Hidalgo, 'Experimental Study of Multicast and Unicast Video Traffic in WAN Links' , IEEE Latin America Transactions, Vol. 15, No. 10, Pp. 1847 1855, October 2017.

[18] R Srinivasan, A Vijayaraj , Mobile communication implementation techniques to improve last mile high speed FSO communication" , Trends in Network and Communications, Springer, Berlin, Heidelberg, Pp: 55-63, 2011.

[19]. Abubakr O. Al-Abbasi , Vaneet Aggarwal , and Moo-Ryong Ra , 'Multi-Tier Caching Analysis in CDN-Based Over-the-Top Video Streaming Systems' , IEEE/Acm Transactions On Networking, Vol. 27, No. 2, Pp. 835 847 April 2019.

[20]. Michael Seufert , Sarah Wassermann , and Pedro Casas, 'Considering User Behavior in the Quality of Experience Cycle: Towards Proactive QoE-Aware Traffic Management' , IEEE Communications Letters, Vol. 23, No. 7 , Pp 1145 1148, July 2019.

[21]. Irena Orsolic , And Lea Skorin-Kapov , 'A Framework for In-Network QoE Monitoring of Encrypted Video Streaming' , *Digital Object Identifier 10.1109/ACCESS.2020.2988735,* Volume 8, Pp 74691 74706, 2020.

[22]. M Sanjay Ram, A. Vijayaraj, " Analysis of the characteristics and trusted security of cloud computing", International Journal on Cloud Computing, Volume 1 Pages, 61-69, 2011.