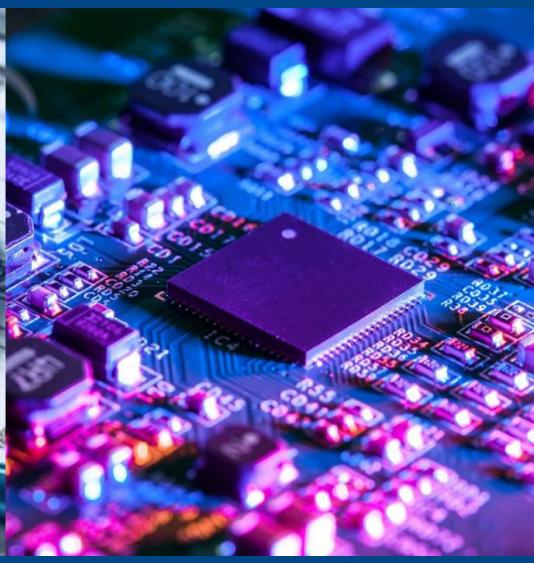
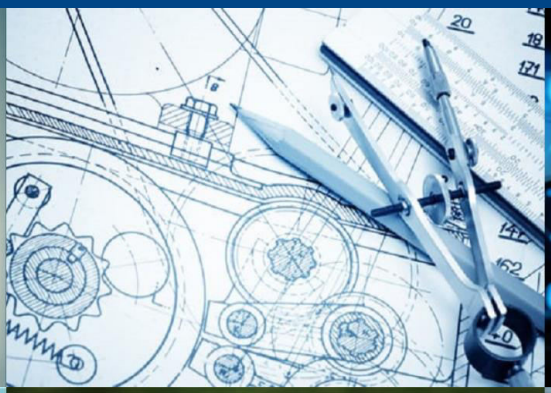
ISSN: 2582-7219

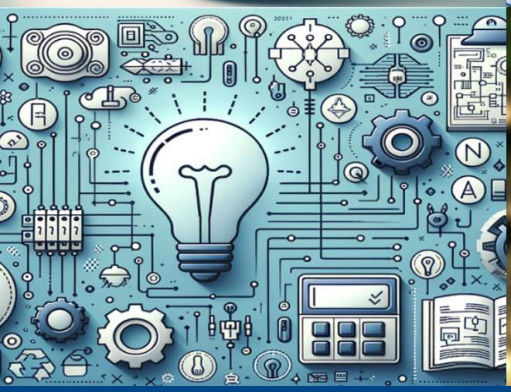




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805031

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Multi Cloud System to Avoid Server Failure using Wireless Sensor Network

Gayathri. K, N.Savitha

Department of CSE, AVS Engineering College, Salem, Tamil Nadu, India

Assistant Professor, Department of CSE, AVS Engineering College, Salem, Tamil Nadu, India

ABSTRACT: Wireless sensor network (WSNs) is based on new technology for the advanced wireless multi-hop architecture without prior setting of fixed infrastructure and the network node. Wireless sensor network (WSNs) autonomous operation can be mobile, multi-hop, it is the infrastructure-less wireless network. Security is one of the biggest challenges in advanced Mobile Ad hoc Network. Thus, the WSNs and security needs, there are two considerations must be, so that the second routing protocol in order to protect the secure packet transmission. In the routing and security that is an important aspect for in a WSNs, existing method routing protocol, however, is not enough to security requirements. The proposed Secure Packet Transmission Routing Algorithm (SPTRA) used designed to maximize the packet security, routing path, minimizing the impact of malicious attack activity over the spectrum, and select the best path. Many routing rule has proposed route in the wireless ad-hoc network that relies from its discovery source to the packet transmission of a given condition to the destination. The general terms advanced WSNs routing protocol, the security, and routing protocol. The proposed SPTRA algorithm improves the energy efficiency of the network and reduces the Packet loss rate of the node. The proposed method shows high performance than other existing evaluations of the most advanced state security and routing delay end-to-end Packet transfer rate, Packet loss.

KEYWORDS: wireless sensor network, Packet loss, Fault tolerance, Data transmission, back propagate.

I. INTRODUCTION

A sensor network, each small lightweight detection stations, the sensor includes a plurality of terminal is called. All sensor nodes switch, micro, and a transceiver and a power supply. In terms of physical effects and events are sensed by the transducer generates an electrical signal.A unit of packet binary data can be transmitted over a computer network. The part of the packet that needs to be pocket dropped or the node to compromise a transfer is dropped. Ad-hoc network is located on the existing base station and there is no network interconnection for the ad hoc for some special reasons.

Here the nodes are smart enough to pave the way and execute all the necessary tasks for sharing data from one node that is in the role of another node network. So, in order to make every node, and communication necessary, you need to provide the transceiver. Research activities related to the pledging of sensor network, security, creation of various developmental power barriers and re-power.

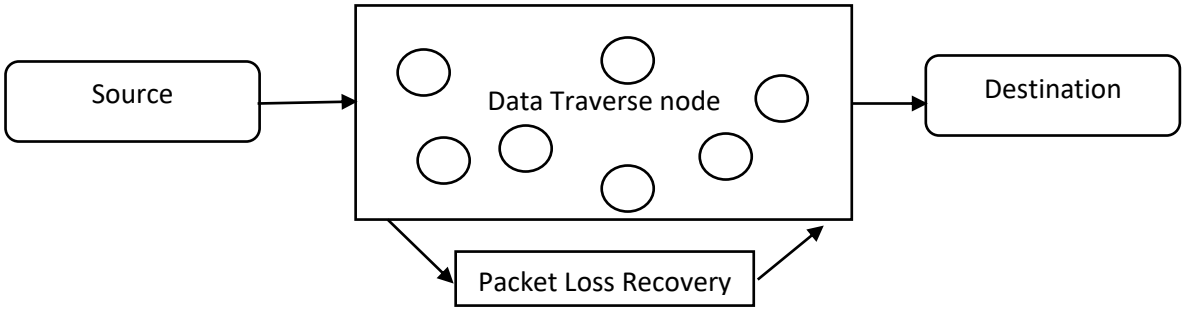


Figure 1 Device interconnected data traverse Networks

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 1 shows the number of these devices is a kind of interconnected networks with a small fraction of the individual hand. The contact range is about 10 meters. The network is made up of 30 units of the node, and the packet is created on all nodes. The sender and receiver are selected at 30 points. The sender sends the receiver packet using the shortest route method. Subsequently, the performance bandwidth will be examined for release or replacement. Tank node participate in this request broadcast. Then, the certificate will create a new node. Then, you can participate in the transmission of the new node.

Usually half of all nodes are routed at the same time leading to uninterrupted wireless nodes. Frequency diversity, but it can solve many of these problems (sun, etc.), broadband high energy noise source, you can prevent a completely wireless communication. Therefore, it is very important to classify the environment performance as the branch technology and RF interference for it. Our prototype WSN, Basic Requirements, Depending on a Single Mistake 1, imposed the routine of non-critical functions yet was critical to the overall success of the task.

1.1 Packet loss mechanism in WSN

Packet loss can reduce the packet arrival rate. The packet loss is obtained by causing a signal process the downgrade node of packet rateswhich filament to make the network several point of routes depends the WSN has all the possibilities. Therefore, it is easy to take actions that do not involve dropping .Identifying packets, and the fact that it is capable of capturing illegal behavior data and much needed transactions. There is no certificate can participate in any node transmission. The purpose of this paper is to detect non-invasive dropper or eligible packets using the location method. Until the new node, including WSN, receives a name certificate, you cannot participate in the broadcast process. After being certified from the tank's node, it can participate in the transmission

1.2 Fault tolerant representation

The design dropper pocket announced in this paper that you can enable the implementation of gifts as efficiently as necessary congestion. Drop Instruction Method Flow Cheating suggests switching to observation mode to combine a number and cross over the predefined threshold. He said the state would build on the need for droplet malfunction flow identification. The model is time-dependent of the low-throughput processor with data path accuracy.Then, the first identification of all previous methods of detection of the hypothetical link attack is presumably, only time, the solution to remove them from the network is a process of corrosive energy. How to choose a lower root and less expensive than the appropriate root, with the "avoid" option, the "identity" space is used for hypothetical attack.

II. RELATED WORK

The wrong path to the tolerance mechanism. The paper is efficiently distributed according to the most applicable capabilities of the sensor network advanced [1]. If a node fails, by applying this fault tolerance mechanism, the connection between the computing nodes, you can ensure maximum availability.

Prior to the source packet transmission attacks and unforeseen circumstances, some data packet and path identifier takes the recipient. Permanent malfunction is a feature that has a significant impact on the quality of the electrical service if it is interrupted [2]. In order to reduce the cost of effective testing that results in increased transmission, a more advanced algorithm has a greater need for reduced performance. Lower Pocket Propagation Rate Precise Fault Location Power System is a major issue [4]. Accordingly, significant research has been achieved in the field of low accuracy and methodology in the presence of a network-based functionality source.

In a multi-hop sensor network, the source of the data enables to track the transmission path of the PS source and the packets of the individual data. Although the source must be recorded for each packet [5], an important issue is the tight storage of the sensor terminal, due to shortcomings in energy and bandwidth. Therefore, there is a need to plan a lightweight look solution for low overhead [6]. In addition, the sensor is, in many cases, likely to receive an attacker operating in an environment that is not credible.

In contrast to existing studies using data and data in the source media [7], we both need a single channel. In addition, using traditional encryption and digital signature [8] solutions with traditional product areas security, they can lead to prohibitive costs and adopt a bitcoin-based data structure to store.The order of priority must be described behind the formula giving the node the highest priority so far: the radius of each node spreading around the radius of the radius is equal to its contact range in circular regions [9]. The local node density may be proportional to the number boundary

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

region of the bottom nodes of a single node [10]. The area is already equal to the number of new nodes covered by the transfer node that is subtracted to its boundary.

If the session specifies the reliability and security requirements of the user, it relates to the parameters of the adaptation protocol [11]. This relationship is of central importance for the ethical endeavor and how much the programs achieve credibility and security at the same time. In addition, by reducing the redundancy of the original data, using optimized encoding [12]. Finally, we moved in order to evaluate the algorithmic performance of large-scale simulation conversion network conditions.

Approval next-up channel can be adapted to similar hardware using busy tone. The wake-up channel [13] is being used. The protocol is implemented using off-the-shelf hardware. However, the protocol is not a fully distributed network and computer-centered access point or proxy centralized [14]. Another way to save energy on the sensor network is to allow a node in a sleep state when the traffic to the table is unable to receive their scheduled traffic. It has been suggested that such an approach may be the sensor networks often encountered [15], as compared to the more conventional an ad-hoc network, which is expected to be relatively stable topologies.

III. PROPOSED SOLUTION

Wireless sensor networks are grouped into a network of sensor nodes. They are located in different geographical locations, data can be easily collected. The main reason for the WSN is the need for physical infrastructure to accelerate growth, if there is a sensor node in the network that can be placed at the highest level environmental conditions. The main idea that the mobile ad-hoc network functions like a pillar again is to multi-hop the relay to find an alternative solution for messaging if you can indirectly reach the target.

The fault tolerance of the computational grid service system is configured with the idle computers in your organization. When adaptive fault detection mechanisms have been proposed to distinguish different fault, non closed, partial rollback mechanism based on communication domains and algorithms that checkpoint unblocked and low overhead, Fault Tolerance It has been proposed in order to reduce the overhead. They meet the requirements of such a system, there are some obvious advantages that have been shown in the experiment.

Working in a Shared Environment There is a special type of wireless sensor networks in an ad hoc network that transmits the neighboring data in the designated target switching frequency range to conclude the data at all points. The data network plays an important role in the decision-making process at large. Therefore, the maximum security of the data must be changed.Reduced to network wired network, wireless node, such as DOS, can easily lead to all packets and, as a result, there is little output of energy consumption in terms of packet arrival rate. Instead, the transceiver needs to be able to receive radio waves without being detected by analyzing the data via traffic analysis to determine if the attacker has been selected.

3.1 Rapid Packet Transmission Algorithm

Because of both low node and high node density, and partial loss to avoid pocket drop. Minimum Duplicate Packets there are multiple node receives, and then the range (RPTA) is chosen as soon as the boundary, distance from the nearest node to the packet transmission mechanisms is compared. To ensure location-specific and combination-time allocation, packet delivery has a lower end-to-end delay avoidance. This has led to a distant node that has a lower allocation rate. Due to the reduction of packet collision parcel drops, the fading channel has reduced the subsurface, thus increasing the success rate of its distribution as expected from the proposed scheme.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805031

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

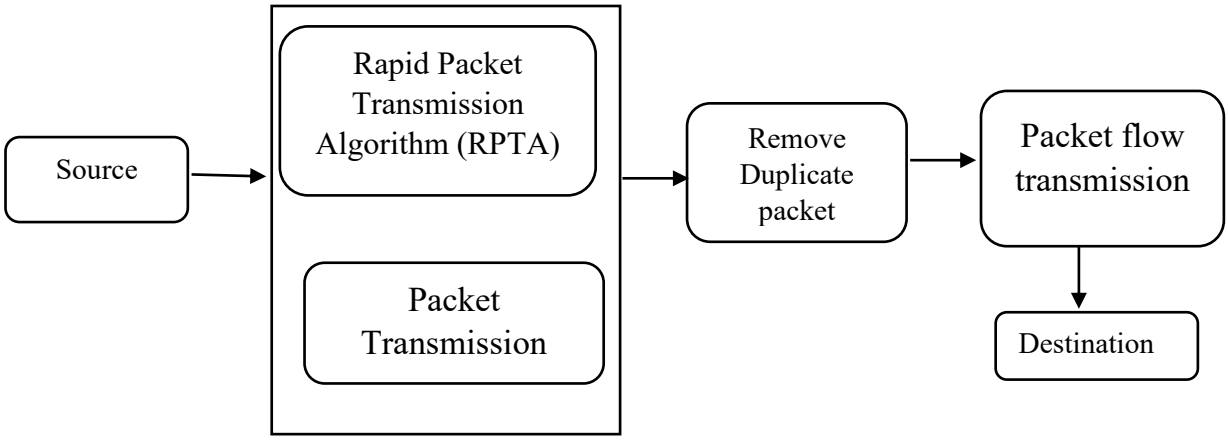


Figure2 Rapid Packet Transmission Algorithm

At the front end, a set of wireless nodes (routers) become a wireless web network. Figure 2 shows the Rapid Packet Transmission Algorithm. Both mobile and pixel are end users, fixed in place and connected to the network via these nodes. The selected set of these nodes, called a gateway, is connected to the optical components of a network. Typically, the gateway is installed on each ONU.

3.2.2 Packet Loss Avoid Algorithm

This rarely occurs in practice. However, in a scenario under large-scale disaster, it can be difficult to ensure network congestion, to standardize the impossible. Our goal is to develop a system that uses strict conditions of use. The algorithm, then known as the parameterized parameter in our study (PLAA), is the target bandage loss rate, which is around the bottom of the packet when it is packed, avoiding loss of bandage in almost every bottom frame taken by the network. There may be two possibilities for evaluating a signal for lost bundles, where the missing bundles hide.

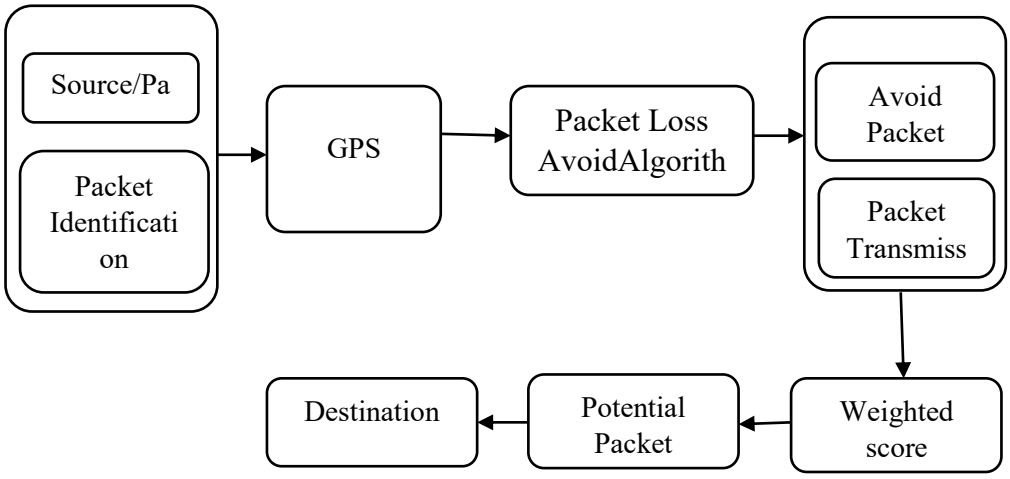


Figure 3Packet Loss Avoid Algorithm

A unique packet identifier target system, which combines the source address and identifier of these unique identifiers for reconfiguration data sets. Figure 3 shows Packet Loss Avoid Algorithm. The bit can be used to decrypt the packet, so that the router can know. The algorithm shown below

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Algorithm:
Input: Number of node with data transmission packets.
Output:Received lossless packets
Step 1: First, a new node n is added to the graph, connected by zero-weight edges to each of the other nodes.
Step 2: State =IDLE
Wireless node placed in the intermediate zone. Each node identifies its location relative to the sink.
Example: $n0 set X_ 0.0
Set using assigned the value

Step 3: To find Send address to receiver address
Step 4: Neighbor node allocate=0, to retrieve the value in Zero
Datapkt=0
Step 5: To send the energy in source to destination
Packet::free
Step 6: n2 node failure stage then remaining node send the energy in source to destination at a time
Step 7: To calculate the energy efficient, throughput, delivery ratio

The selection process comes as a component of the calibration process to process the packet at the point of observation or to print the arrival time and seal packet, a statement for each packet that is selected, and the contents of other possible information.

Packet Loss Avoid Algorithms

Failure to reach one or more data packets on a computer network can result in loss of bandwidth. Packet loss, usually a radio network, or network congestion, causes data transmission error. Depending on the packet loss, the spread packets, the percentage of lost packets will be measured. The Transmission Control Protocol (TCP) functions to ensure a reliable message to detect loss of ligament and reversibility. Pocket loss of TCP connections is therefore less deliberate and therefore less productive of the connection output, to avoid congestion.

Avoid Packet Loss

Pocket loss is the difference between received packet caused by contact. Packet loss is calculated using the awk script to generate the results, to process the trace file. The NS packet contains a header for the stack, and no data space. The simulator object, when it is created, is initialized depending on the general requirements of a packet header format, similarly, the log header is used for any object, IP header, TCP header, RTP header header (or optional if available) (UTP uses RTP header), trace headers defined, Each head in the stack All plots are recorded for the offset. What this means is that if the packet is allocated by a particular header agent and that all the log header stack is created, the network object, it uses te packet layer can be activated relative to the offset value to access any header.

Weighted score

Originally, it was designed to use a binary classification problem with a unique and numerical function. Relief, then applied to the standards, it is possible to select the scoring function over the feature selection, to calculate the activity score for each activity. Alternatively, the score is such that it can be used as a feature weights to guide downstream modeling.

IV. RESULT AND DISCUSSION

To analyze the performance of the proposed approach to overcome this section, the broadcast program provides the burden of flood data performance assurance on QoS parameters. The number of single packet replays, via a broadcast technology that is considered in the comparison parameters. Model, or terminal, means of approximating floods of approximate units sent by the network map performance in a uniform survey, and then, equal to the unit distance of the disk model diagram obtained by combining a small or terminal.

The use of this test is very important for a particular node traffic, and as a result, the movement of the network can be a realistic block chain from the very beginning. However, after a certain period of time, there is a possibility that the battery node starts emptying, the energy efficiency problem will be over. In such a situation, the utility, and thus the cost of reducing the resources allocated to this particular transport should extend the life of the network to reduce QoS.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This changes by dividing the number of nodes connected to the network density network. The high density of nodes and low traffic load are converted to different values. This proposed approach is due to the fact that the hue / s is in a network with density and velocity with a different network between 1 and 4 m. For each simulation, CSLA – Cross-Site Leaping Algorithm, SDP - Semi-Definite Optimization Problem, BLAC -Battery-Level Aware Clustering. Were formulated he number of random source and target connections is 10 and generates four data packets / sec.

Number of nodes	BLAC	SDP	RPT-PLLA
20	0	0	0
40	30.42	40.35	51.98
60	37.45	42.23	52.12
80	52.98	50.87	61.65
100	63.45	84.55	91.55

Table 1: Downgrade packet ratio

Table 1 gives a comparative study output of existing approaches and the proposed method. The packet arrival rate has been used to assess network quality. This is intended to define a ratio between the received packet and the source generated packet. This is a trace file and a script to generate the results you can get using downstream transfer rate. Wireless Sensor Networks (WSN), it is well known that energy consumption is one of the main concerns of most resource constraints network. In terms of the energy level of the cluster head terminal, the main reason for energy consumption is, for example, one of the terminals for which the node and the cluster head can randomize the long distance and the ad itself. Delivery Protocol in the Energy Sensing Environment As a research method for developing wireless sensor networks, the focus is on determining the low cost path in which the network is configured.

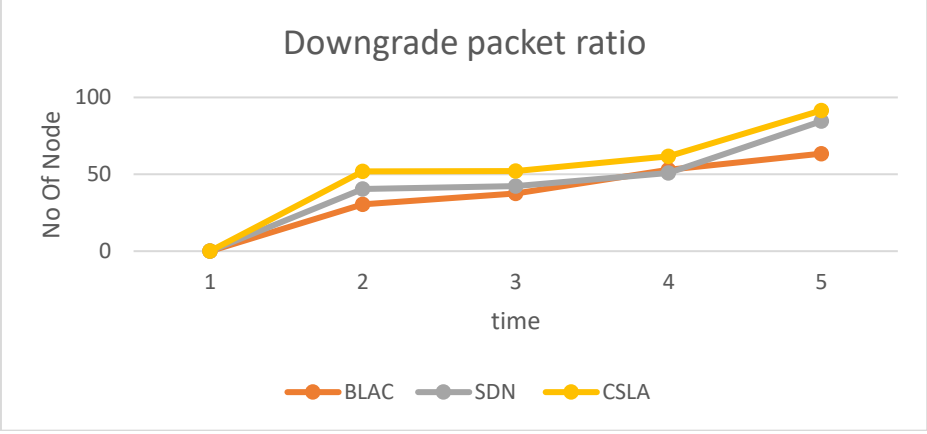


Figure 4 comparison of downgrade packet ratio

In the meantime, when the triggered error is acceptable, please avoid network swap. Our work is to predict the energy through the proximity of the node of the data transfer path to the target. Figure 4 shows the packet delivery ratio using the Rapid packet transmission network algorithm, and optimizing packet transmission. We are demonstrating the improvement in battery energy consumption through simulation decisions, without the transmission of data perceived as a minimum cost for communication speed costs.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

	BLAC	SDP	CSLA
10	0.54	0.58	1.18
20	5.2562	5.7271	6.7144
30	3.2545	4.2123	5.2124
40	8.4241	8.5956	8.7142
50	6.2412	8.1417	8.2450

Table 2: End to End Delay

The data exchange between the war's troops located at different location in the terrain causes a high end to end delay. The time which is taken by the source node to deliver the data successfully to the destination is called as end to end delay. It is the difference between the time at which packets generated by the sender and the time the packets received by the receiver and it can be obtained from the trace file.

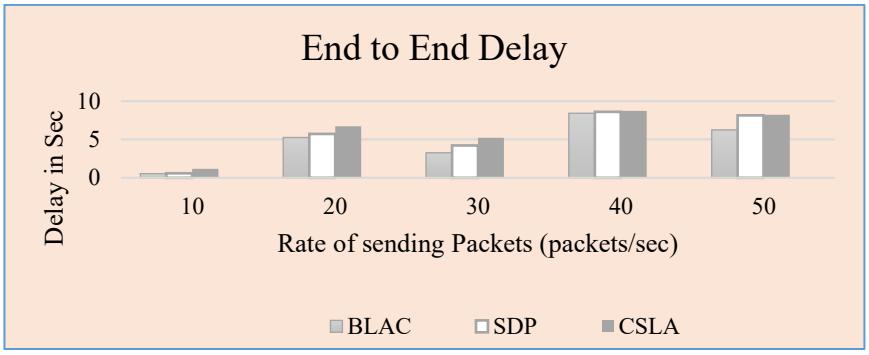


Figure 5 End to End Delay Ratios

Analysis of the Current System Decision Figure 5 and the proposed methodology should be used to conclude a project. The delay is calculated based on the rate of packet spreading in a given number of seconds. However, there are some differences. It allows only one packet / sec but only a delay of the proposed network of tracks. If the target is moved to close the source node, the delay is reduced. Otherwise, the delay will increase. The process fee data packet rate defines the number of packets generated by the source node for a specified period of time.

Acquired data function = downstream data* 8 / data transfer period

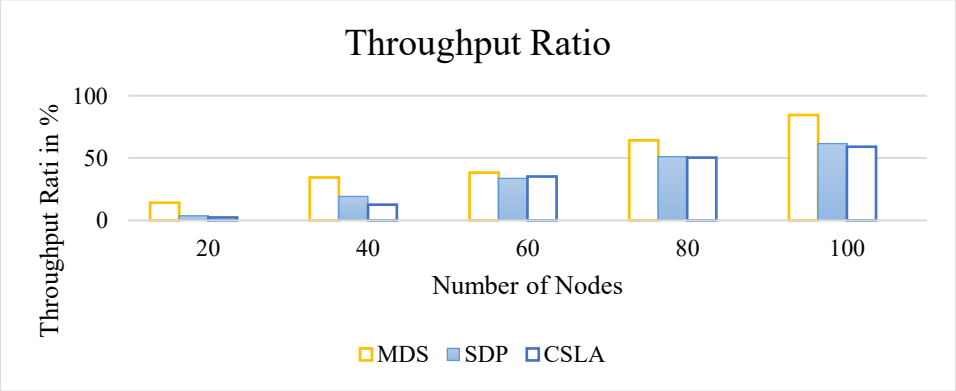


Figure 6: Throughput ratio analysis

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

From Analysis Output Rate and Image. Figure 6 shows the throughput analysis of the proposed scheme has clearly proven that CSLA can improve output by 34.5% as compared to existing systems. However, we believe that this is reasonable, even if the network is used in this situation and the CH node number is kept low. It is true of simulation, it is not a use case but it is less common in the nodes of these interactions.

	CH1	CH2	CH3
CSLA	93.82	90.27	91.04
BLAC	95.65	97.68	97.57

Table 3 Energy ratio comparison

After transmitting the data in the PS of CH, as shown in Table 3, we studied the remaining energy of the node, in this case. H1 is a profitable approach to establishing CSLA's main role in this approach. In contrast, other nodes have reduced their residual energy when using CSLA.

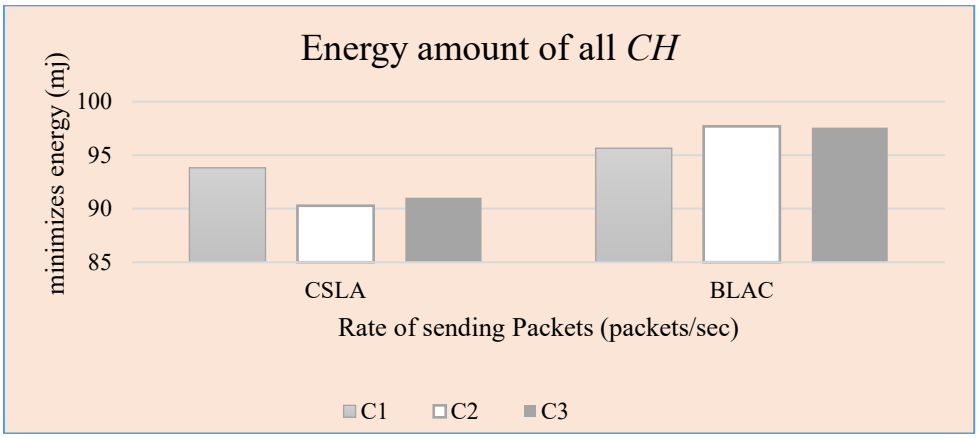


Figure 7: CH Energy ratio analysis

Pattern application method is based on a comparison of time complexity to try to change the original features and often the appropriate complexity time. The actual object of the method application feature bond is usually lost.

V. CONCLUSION

In this study, the analysis of the different packet loss system observations revealed that the main reason for the dropped packets is the lack of security when transmitting data to a wireless network. Using provenance to transmit data over a secure wireless network, avoid loss of bandwidth through protocols, and consider the necessary security measures to achieve total unobservability. Increased packet delivery rate and lower packet loss compared to other systems have been experimentally 95.6 % observed from the results. Accordingly, when sending data in conjunction with an increase in the packet delivery rate to ensure Output Advanced Data, the system can be predicted to be very effective, with little loss of bandwidth. In the future, with this scheme, the malicious packet discard detection technology, the work of the head of a minimum maintained over forming at the same time, it effectively in any environment Attack discarding a packet detector that you could be able to design, the packet loss of data at one time loss.

REFERENCES

[1] P. Kori and K. Cecil, "Secure Wireless Sensor Network Design Using a New Method of High-Speed Lightweight Encryption," *2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA*, Pune, India, 2022, pp. 1-8, doi: 10.1109/ICCUBEA54992.2022.10011005.

[2] B. Yuan et al., "Secure Data Transportation with Software-Defined Networking and k-n Secret Sharing for High-confidence IoT Services", *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7967-7981, Sept. 2020.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] C. Anitha, V. Praveena., V. SamuthiraPandi, S. Kumar, B. Shiva and A. Muniyappan, "Maximizing Cloud Security: Empirical Evaluation of an Efficient Identity oriented Signature Verification Scheme for Wireless Networks," *2024 2nd World Conference on Communication & Computing (WCONF)*, RAIPUR, India, 2024, pp. 1-6, doi: 10.1109/WCONF61366.2024.10692001.

[4] F. Tsvetanov and M. Pandurski, "Specific Security Issues in the Integration between Sensor Network and Cloud Structure," *2022 8th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE)*, Ruse, Bulgaria, 2022, pp. 1-4, doi: 10.1109/EEAE53789.2022.9831200.

[5] R. M. Manicka, K. S. Manoj and B. Kiruba, "A Novel Energy Efficient Sensor Data Encryption in Fog Based IoT Networks," *2023 International Conference on Next Generation Electronics (NEleX)*, Vellore, India, 2023, pp. 1-6, doi: 10.1109/NEleX59773.2023.10421411.

[6] Lili Wang and Xiaobei Wu "Distributed Prevention Mechanism for Network Partitioning in Wireless Sensor Networks" Journal of Communications and Networks, Vol. 16, No. 6, December 2014, Pg.No:667-676.

[7] Salvatore F. Pileggi,Carlos E. Palau,ManuelEsteve "Multimode WSN: Improving Robustness, Fault Tolerance and Performance of Randomly Deployed Wireless Sensor Network "2010 Second International Conference on Computational Intelligence, Communication Systems and Networks, Pg.No:112-117.

[8] KeerthanaS,Dr. J.C Miraclin Joyce Pamila"A Survey on Fault node Detection and Recovery Mechanisms in Wireless Sensor Network " 2015 International Conference on Advanced Computing and Communication Systems, Pg.No:1-5.

[9] Yongxuan Lai, Hong Chen "Energy-Efficient Fault-Tolerant Mechanism for Clustered Wireless Sensor Networks" IEEE 2007, Pg.No:272-277.

[10] Lin MA, Shuang JIA, Danyang QIN, Songxiang YANG "Research on Energy Sensing based Fault-tolerant Distributed Routing Mechanism for Wireless Sensor Network" IEEE 2016, Pg.No:1-12.

[11] ElhadiShakshuki, Xinyu Xing, Haiyi Zhang "Agent-based Fault Detection Mechanism in Wireless Sensor Networks" 2007 IEEE/WIC/ACM International Conference on Intelligent Agent Technology, Pg.No:31-34.

[12] Ines El Korbi, YacineGhamri-Doudane, RimelJaziand Leila AzouzSaidane "Coverage-Connectivity based Fault Tolerance Procedure in Wireless Sensor Networks" IEEE 2013, Pg.No:1540-1545.

[13] Nan Ya,XingweiWang,ShuangZhang,Min Huang "Multipath Fault-Tolerance Routing Mechanism in Data Center Network"2018 17th International Symposium on Distributed Computing and Applications for Business Engineering and Science,Pg.No:246-249.

[14] Liu Chen,Wei Zhou " "2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control,Pg.No:1255-1258.

[15] Mahdi Nasrullah Al-Ameen" A Clustered Response Approach for Wireless Sensor Networks with an Application to Fault Tolerance Mechanism"IEEE 2010, Pg.No:1-9.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com