# Enhancing the Communication of IoT Using African Buffalo Delay Tolerant and Risk Packet Jump Approach

[1]SHRIDHAR SANSHI, [2]PRAMODH KRISHNA D., [3]RAMESH VATAMBETI*
[1]Department of CSE, National Institute of Technology Puducherry, Karaikal, INDIA
[2]Department of CSE, Narayana Engineering College, Guduru, INDIA
[3]School of Computer Science and Engineering, VIT - AP University, Amaravati, Andhra Pradesh, INDIA.

Abstract- The Internet of Things is used in many sectors for different applications in an efficient way. However, sharing huge data to distant destinations is a difficult task such as sending large data from remote area for healthcare application. So that the Delay Tolerant Network is used but, in some cases, the presence of selfish nodes in Delay Tolerant Network may drop all the packets. To overcome this problem the current research affords a novel African Buffalo Delay Tolerant Network with Risk Packet Jump (ABDTN –RPJ) mechanism to improve the communication channel by predicting the selfish and misbehavior node in an earlier stage. Besides, RPJ is introduced to split the huge data to the other neighboring nodes to reduce packet load on the node if the load is greater than the capacity of the node. Finally, the ABDTN –RPJ is implemented and evaluated using the NS2 simulator. The comparison results proved the efficiency of the proposed model by reducing the delay and drop rate.

Keywords: IoT, communication, DTN, African Buffalo optimization, Risk transfer

Received: May 8, 2021. Revised: July 21, 2022. Accepted: August 16, 2022. Published: September 15, 2022.

## 1. Introduction

The Internet of Things (IoT) accompanied by sensor technology [1] is a trending topic in today's network world [2]. Especially in the healthcare industry is attained more benefits from this technology [3]. Without sensor technology, one could not imagine an appliance [4] because sensor technology plays a significant role in all fields. Moreover, the IoT is more adaptable in the health care system, to collect the specified body condition in which the sensor is inserted. The assimilation of the IoT strategy in the clinical industry [5] has reverted many researchers around the world to develop smart appliances [6] such as mobile healthcare [7], intelligent model, health-aware suggestions [8], and so on. IoT is the clustered communication system, with a huge number of host functions at a time for the specified work [9]. Besides, IoT devices are consist of sensors and storage space to store the sensed or gathered information [10]. Thus, the IoT is utilized in various sectors and processed in different operations to achieve the desired task [11]. The information gathered by sensors is important for any application to perform the desired task. Therefore, it becomes critical not to lose any data during the communication. In an IoT Delay-tolerant environment, service establishment is a difficult task because each host in the entire network has a huge burden of loads to carry on [12]. Satisfying the customer needs with a limited resource becomes more critical [13]. Using the Delay Tolerant Network (DTN) in the IoT environment can enhance communication by controlling devices more efficiently. The DTN is used in many applications including military, space communication, vehicular communication, communication in remote areas, tracking and monitoring of wild animals, and many more. The link in DTN is eager to maintain end-to-end connectivity of the network. To achieve this, the DTN is processed with a store-carry-forward mechanism to transfer the message to a particular location that is challenging to reach [14]. If a node aims to broadcast the data to the target node, then the intermediate nodes should be within the range of contact, if not a node waits for the intermediate nodes to arise for communication opportunity.

In today's digital world, communications in the IoT network are embedded with the Internet or any other cloud server [15]. The IoT devices (non-mobile) are worked through the internet by doing the task like control, monitor, etc. further IoT devices effectively include automated data collection. The sensors attached to the IoT devices sense the information of particular events that are critical for the application and send data to the root (base station) node. However, the time taken by the IoT devices to transfer the information in the DTN framework is not enough because of the short contact time to transfer the information. The heavy load on the IoT devices may cause link failure. Further, the problem becomes more challenging in presence of selfish/malicious nodes. The selfish nodes take the opportunity of forwarding their information by utilizing the resource of their neighbor nodes while not providing its resource for neighbors to forward their information. These may cause link failure as there will not be a communication path established in presence of selfish nodes. To overcome such problems many researchers developed some novel

approaches like adaptive spray [16], Fuzzy based approach [17], intrusion detection [18], and so on. However, the problem persists because of the DTN flexibility and IoT broad usage. Therefore, in this paper, a hybrid routing and risk migration model has been designed to reduce the risk factor in the DTN-IoT communication channel. The proposed idea can be applied to the healthcare applications that requires large medical data to be transmitted from remote area. The key contribution of this current research is summarized as follows:

- Initially construct the African Buffalo Delay Tolerant Network (ABDTN) by the use of the network simulator.
- Before transferring the data, monitor all the IoT nodes for the malicious and any selfish activities.
- Consequently, the message is transferred and then checks the communication or packet load and nodes capacity.
- If the packet load is more than the capacity of the node then the Risk Packet Jump (RPJ) model is initiated to transfer the packet to other free nodes.
- Finally, evaluate the data transmission rate.

The remainder of this research article is itemized as follows, section 2 describes recent literature related to IoT and DTN, section 3 defines problem statement, section 4 deals with the proposed methodology, section 5 enumerate the result and discussion, and section 6 concludes the paper.

## 2. Related Work

*Some of the recent literature's related to the detection of a malicious node, distribution of load, and delay tolerant described as follows:*

The author Tuan Le [19] proposed a routing strategy to route large data by dividing it into smaller chunks. The smaller chunks were further forwarded to the destination based on several successive nodes. The paper also proposed a delivery model by considering crucial parameters like contact time, data size, contact frequency and build a contact graph for delivery. The proposed model was evaluated using simulations by collecting real-world mobility traces. Results of simulation showed a 53% improved delivery rate compared to other works.

The authors in [20] have proposed a new hybrid protocol for IoT DTN by taking the advantages of DTN routing strategies namely flooding strategy and forwarding strategy. The modified Prophet metrics were used in the new protocol to improve the delivery rate. Also, the protocol uses replication bundles to maintain the quality of service in IoT. The simulation results conducted on the ONE simulator showed an 18% improvement in the delivery rate.

The authors Yosra Zguira et al [21] have proposed a lightweight protocol for bike-sharing applications in urban areas and called it Internet of Bikes for DTN (IoB-DTN). In the IoB-DTN protocol, three buffer management policies were discussed so that which packet to be discarded when the buffer is full. The simulation results were conducted on the Omnet++ simulator and the results showed the impact of redundancy packets on the overall efficiency.

In the wireless medium, identifying the estimated location is a significant task for process distribution and resource usage. So AhmadAlZubi et al [22] proposed a location-assisted service to reduce the transmission delay and to maximize resource utilization. Finally, the projected technique minimized the request broadcasting delay. Also, the comparison analysis proved the efficiency of the proposed model.

The crowdsourcing paradigm is a trending field in the IoT environment, especially in the online job allocation model. Chongyu Zhou et al [23] proposed an online scheme auction to allocate the late tolerant job. Besides, the system utility also increased by categorizing the trustful user in the network channel.

The essential part of IoT is WSN, which can perform both sensing and message broadcasting processes. But the severe threat against IoT technology is denial attacks which consume and collapses a large amount of data in a hybrid manner. To overcome this Zubair A. Baiget et al [24] proposed a hybrid intelligent denial attack detection model to protect the IoT device. The proposed model is tested with different kinds of attacks also achieved better results compared with other work.

The authors Solmaz et al [25] have proposed a hybrid protocol for detecting selfish nodes by combining the methods of reputation-based method and game theory-based method. The hybrid protocol has three phases to monitor the behavior of neighboring nodes. If the activity of the neighbor node was found to be malicious then a penalty was assigned to the node as a punishment. The simulation results of the proposed protocol showed an improvement of 12% for detecting the selfish nodes compared to other works.

Sybil attacker makes and controls more than one characteristic on any system. These illegal characteristics of the Sybil attacker cause several malicious exercises without the dread of being distinguished and hence responsible for submitted malign activities. To overcome this problem, Sohail Abbas [26] projected a recognition system that notices both intended and unintended Sybil characteristics using one-time positioning devoid of causing time positioning information overhead.

The DTN enables efficient communication through all wireless communication channels but securing the communication medium is difficult. To overcome this problem Naveed Ahma et al [27] proposed a pseudonyms approach to secure the DTN. When comparing this strategy with security protocols the pseudonyms mechanism attained a better security rate by protecting the DTN communication channel against malicious activities.

## 3. Problem Statement

DTN is more suitable for IoT environments as it allows the information to reach the destination through successive nodes. In the DTN network if the nodes are IoT sensors then it carries much more gathered and sensed information and that has to be transferred to a certain base station where the processing and decision will take place. However, in such DTN, transferring the huge gathered information is challenging. Further, it

complicates in presence of malicious and selfish nodes. Hence to resolve the huge burden on IoT nodes and to increase the transmission facilities in presence of selfish nodes, some of the mitigation strategies should be followed.

The problem in the DTN IoT network is shown in fig. 1. In fig. 1, the source node 1 forwarding its gathered information to the destination node 11 via nodes 8, 9, and 10. If any disruption in the link then the information is stored in the previous node's buffer and wait for the connection establishment. A malicious node joins the network to establish a connection. During that period a malicious or selfish node can get the information or purposely drop the packets.

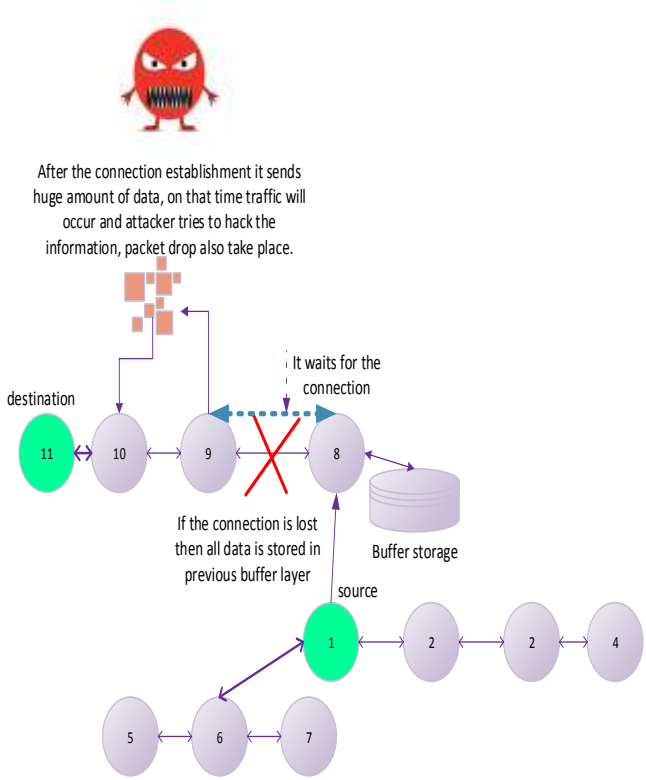


Figure 1. Problem model

# 4. Proposed Model: ABDTN-RPJ

Considering the conventional network system DTN has as many facilities because it tolerates the link failure by delaying the packets. Therefore, it is utilized in several communication applications. To improve the performance of such applications a new ABDTN is designed. Initially, the ABDTN is developed for the communication process, and then the fitness function of the African buffalo is used to predict the malicious and selfish node in an earlier stage. To forward more packets in the IoT environment a novel risk transfer mechanism is developed. Simultaneously, the RPJ model is also developed to maintain path stability.

The proposed approach is diagrammatically shown in fig.2.

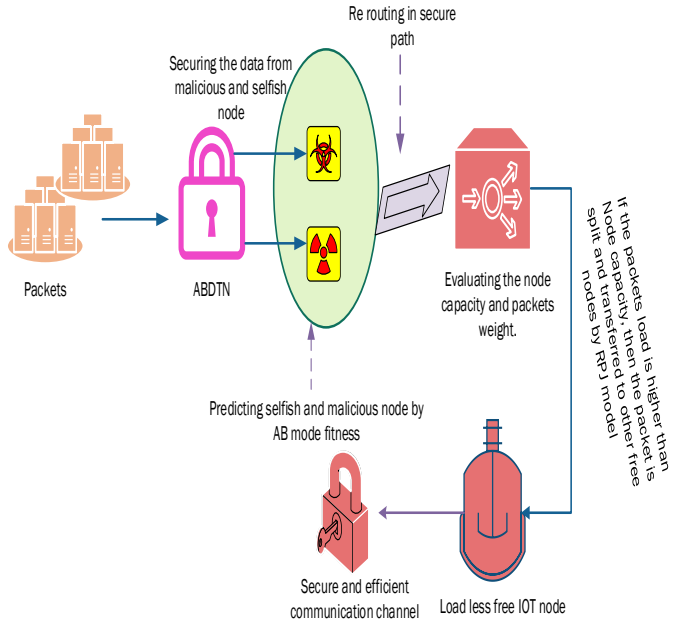


Figure 2. Proposed model

## 4.1 African Buffalo Waiting Network

The ABDTN model is designed for providing a tolerant mechanism to the network paradigm. It is an improvement over the DTN which supports the transfer of information to a distant destination. ABDTN has many advantages over the conventional network which does not have the ability for detecting and preventing malicious activities.

African buffalo is a heuristic mechanism; here it is utilized to predict and remove the selfish and malicious node by its fitness function. Here all the nodes are considered as IoT nodes thus the IoT nodes have more sensitive information that is kept very secret so the prevention and detection of attack are quite important. In the ABDTN model, every group has an elective member that is the head of the group which is represented as $\lambda$ .Here, the head of the buffalo is considered to be a monitoring node. The working of the proposed network is elaborated in algorithm. 1. The head buffalo monitors all the buffalos in the group by monitoring the fitness function of each buffalo. The Algorithm 1 uses eqn. 1 for estimating the radio frequency of entire node links and eqn. 2 for searching malicious node.

**Algorithm.1 ABDTN**

int ***node*** $Y^* = 1,2,3...n$ *//$Y^*$ is the set of node present in network channel*

***Begin:*** *searching for less energy nodes (malicious and selfish node)*

*Estimate the radio frequency of entire node links*

$$f_{\mu+1} = f_{\mu} + l_1 x_1 (r_{g\max.\mu} - m_{\mu}) + l_2 x_2 (r_{p\max.\mu} - m_{\mu}) \quad (1)$$

*Where* $f_\mu$ *and* $m_\mu$ *represents the link and node frequency, respectively.* $\mu$ *is frequency evaluating factor of each node* $(\mu = 1,2,.....N)$ *,* $l_1$ *and* $l_2$ *are the learning factors;* $x_1$ *and* $x_2$ *are* ***random node selection to calculate its frequency*** *between [0,1];* $r_{g\max.\mu}$ *is the* ***maximum radio range*** *and* $r_{p\max.\mu}$ *represents the maximum frequency of link rate to transfer the information.*

***Search*** *the selfish and malicious node* $\mu$ *in relation to* ($r_{p\max.\mu}$ *and* $r_{g\max.\mu}$) *using Eqn. (2) [37]*

$$f_{\mu+1} = \frac{(m_\mu + f_\mu)}{\pm 0.5} \quad (2)$$

***Is*** $r_{g\max.\mu}$ *updating. Yes go to step 6. No go to step 2*

*If the stopping criteria isn't met, return to eqn. (1) [37], else stop the process*

***Output:*** *medium frequency value for embedding*

The significant parameters of ABDTN is

- Earlier prediction of malicious and selfish node
- Frequently monitoring the IoT node for any fault

These both important function of the newly developed network model is utilized to carry on the communication channel in the better way.

## 4.2 Risk packet jump (RPJ)

If one node overloaded with more number of packets than its capacity then packet drop may occur. To avoid that risk transfer model is adopted. The working of RPJ is to split the huge data to the other nodes.

**Algorithm.2 RPJ**

*int packets*

**fetch** ($packets$)

calculate the available packets in the network medium

**if** $(p \geq k^*)$

// **here** $p$ **is the packet size and** $k^*$ **is the bit rate**

$packet \rightarrow C$ // $C$ **is the other free node**

// **packet is forward to the other free nodes**

**if** $(Y^* \leq k^*) \rightarrow C$

$c = gained\ packets$

else (search for other free hubs)

Stop

If the IoT is utilized in different sectors such as military or space applications then there is a huge amount of data, so distributing the data is a difficult task in DTN. For that, the risk transfer model is proposed to reduce the burden of the node. When the load is minimized or shared equally to the entire nodes then the packet drop will be reduced.

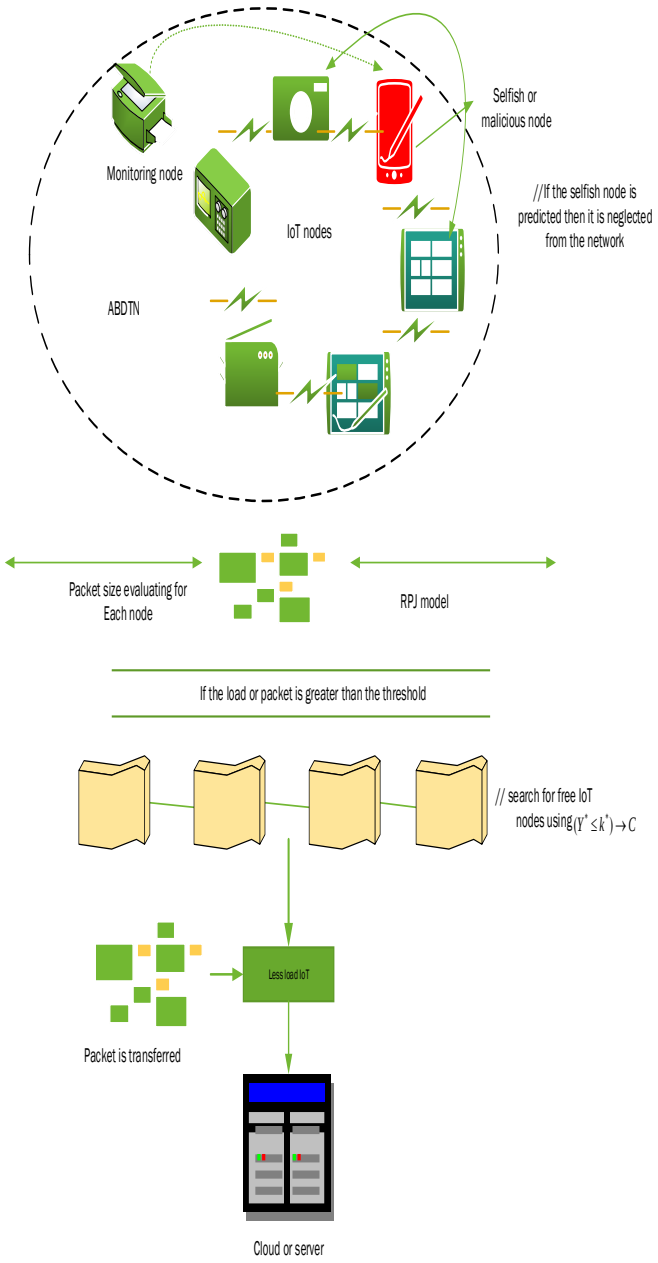


Figure 3. Proposed work flow model

The entire process of the projected strategy is elaborated in fig. 3. In the beginning stage itself, the monitoring process is initialized by the AB fitness function. The RPJ is activated to detect the load on each of the nodes. If the load is greater than the threshold then searches for the node whose value is less than the threshold. If a node is found then the load is transferred or else it will wait for other nodes.

# 5. Results and Discussion

The proposed approach is implemented in NS2 and running on the Windows 7 platform. Ns2 is the simulator tool that is

popularly used to simulate the network model. The comparison of the proposed strategy is compared with recent existing approaches to determine the efficiency of the proposed work. This research work aims to enhance the transmission channel for IoT communication so that the DTN model is adopted. Here the ABDTN network is constructed with 30 IoT nodes, before message broadcasting, the energy of the node should be determined otherwise cause's huge data loss.

## 5.1 Case study

Nowadays, IoT application is advanced in many fields to evaluate the successful measure of the proposed model the case study is processed.

Let us consider, there are IoT nodes that contain set of sensed medical information and medical records. It would be transferred to the server, thus the server is located in far distances. So before forwarding the packets the present nodes in network should be analyzed and monitored, whether it is good condition to receive the packets or not. Here, 5 is the total number of nodes, 0.2 is the link frequency, 0.1 is the node frequency. While substituting these values in eqn. (1) eqn. (3) is obtained

$$f_{\mu+1} = 0.2 + 1(0.5 - 0.1) + 1(0.5 - 0.1) = 1 \quad (3)$$

Now the 1 is above 0.5 then it is good nodes if the node energy is below the range of 0.5 then its go the next eqn. (2) to check wheather it is malicious or not. The gathered infromation from the patient with the help of IoT is detailed in tabular form.

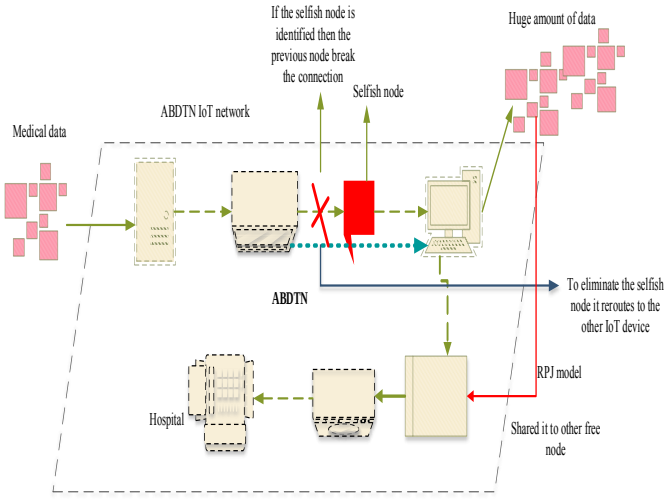


Figure 4. Interior work flow of the proposed approach

The interior work flow of the proposed approach is detailed in fig.4. In the other model the high weight packet is distributed to the other node which is in the Free State condition by the method of Risk packet jump. For that one of the node is initiated and monitor all the node in RPJ method it sets the maximum threshold of 2000 bits for an each node. Then the evaluate is processed by eqn.(4).

$$(p \geq k^*) = (3000 \geq 2000) \quad (4)$$

Let us consider 3000 is the bits of packet size which is handled by a single node and 2000 is the maximum threshold range. If the packet size is higher than the maximum threshold then it forward to the other node.

## 5.2 Performance metrics

To evaluate the effeteness of the proposed strategy some of the key metrics should be validated in standard way such as routing overhead, packet delivery ratio, delay, packet drop ratio and node life time. For that some of the recent existing works are adopted such as precedence and Reliability base Routing in Delay Tolerant model (PRiDE) [25], Online auction scheduling (OAS) [21], locality assisted delay service detection (LADS) [20].

*Routing overhead*

Routing overhead is calculated in terms of packet size divided by node capacity, it is well evaluated by calculating the traffic analysis in the network link. Each node has own buffer to store the data when the connection is interrupted.

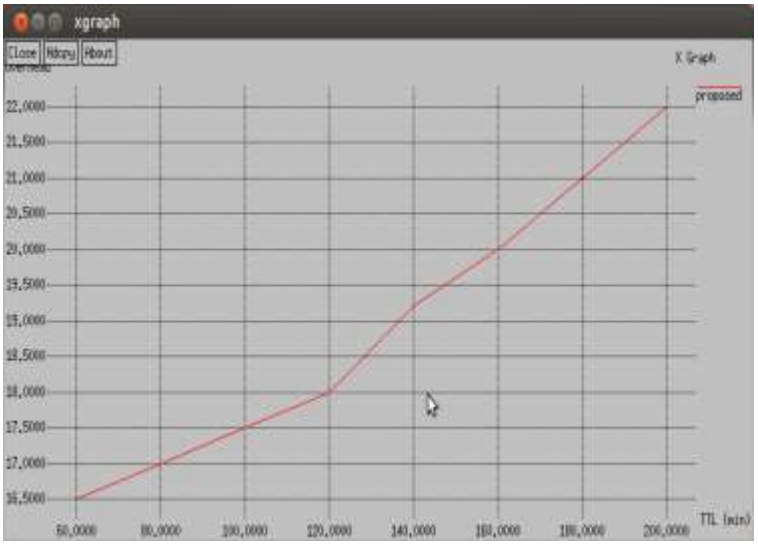


Figure 5. Routing overhead

Here the routing overhead is validated under the TTL condition; the metrics time to alive of nodes is defined as the remaining energy of the IoT node after transferring the message. The attained routing overhead by the NS2 is shown in fig.5 and its comparison result is validated in figh.6.

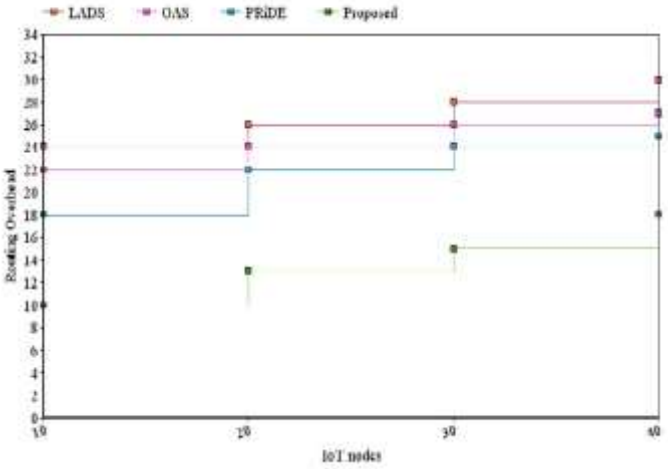


Figure 6. Routing overhead comparison

Table 1. Routing overhead comparison

| | Routing overhead comparison | | | |
|---|---|---|---|---|
| **IoT nodes** | **LADS** | **OAS** | **PRiDE** | **Proposed** |
| 10 | 24 | 22 | 18 | 10 |
| 20 | 27 | 23 | 20 | 12 |
| 30 | 29 | 24 | 22 | 14 |
| 40 | 30 | 27 | 24 | 18 |

*Packet delivery ratio*

It is validated by calculating the number of packets which delivered in limited interval of time. In DTN the packet delivery ratio is improved by developing the high routing protocols. The packet broadcasting is defined as the amount of packets delivered by source and the amount of data received by the target node in eqn.(5).

$$\text{Packet delivery ratio} = \frac{amount\ of\ delivered\ packets}{amount\ of\ received\ packets} \quad (5)$$

The obtained packet delivery ratio by the network simulator is shown in fig.7 and its comparison is elaborated in fig.8 and table.2.

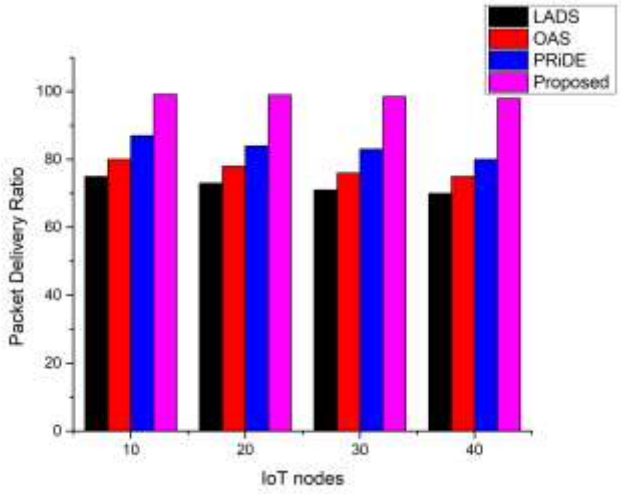


Figure 8. Packet Delivery Ratio Vs IoT nodes

Table 2. Packet delivery ratio comparison

| | packet delivery ratio | | | |
|---|---|---|---|---|
| **IoT nodes** | **LADS** | **OAS** | **PRiDE** | **Proposed** |
| 10 | 75 | 80 | 87 | 99.2 |
| 20 | 73 | 78 | 84 | 99 |
| 30 | 71 | 76 | 83 | 98.5 |
| 40 | 70 | 75 | 80 | 98 |

*Delay*

While broadcasting the packet, the approximation of receiving time is noted. The delay is validated as the extra time taken to complete the process. The obtained delay rate is mentioned in fig.9 and its comparison is evaluated in fig.10 and table.3. As shown in fig.10 the proposed idea showed better delay as compared to other techniques especially in high density of node. In the proposed technique, intermediate nodes are selected immediately and forwarded as compared to others techniques.

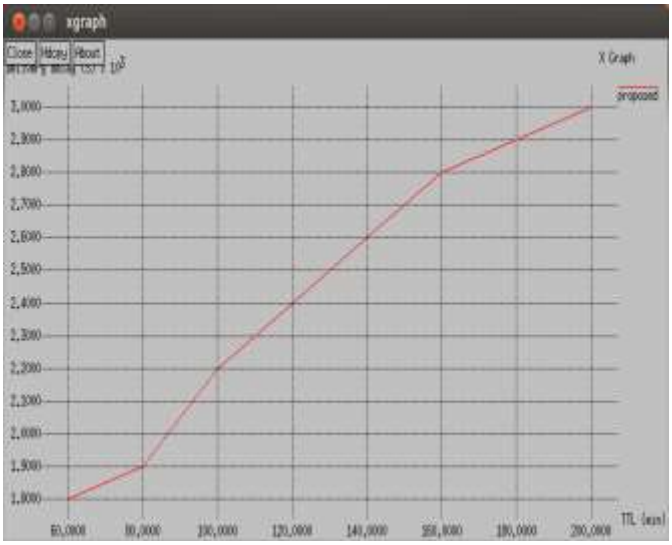


Figure 9. Delay rate

The proposed mode shows the delay rate as 3 ms for 40 IoT nodes, while comparing it with the recent existing approached it proved the efficency by attaing very less delay rate.

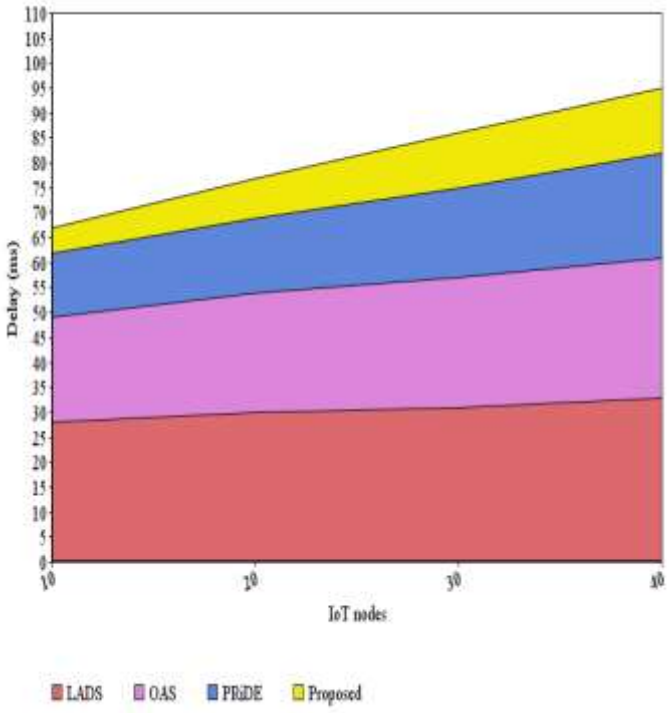


Figure 10. Delay comparison

The statics of the delay comparison with exing approach is drawn in table.3, also here the delay is calculated as milli second.

Table 3. Delay comparison

| | Delay (ms) comparison | | | |
|---|---|---|---|---|
| **IoT nodes** | **LADS** | **OAS** | **PRiDE** | **Proposed** |
| 10 | 33 | 28 | 20 | 7 |
| 20 | 37 | 32 | 24 | 10 |
| 30 | 43 | 35 | 26 | 15 |
| 40 | 50 | 40 | 28 | 18 |

## 5.3 Node life time

In wireless communication medium the awareness of node is more important before transfering the data or information. So the life time of the node is estinated by evaluating the energy of nodes. The comaparison of node life time is detailed in fig.11 and in table.4.


Figure 11. Node life time

After the each data transmission the life time of the node should be evaluated for the better communication channel. Without the awareness of node life time the efficient transmmision in wireless medium is impossible.

Table 4. Node life time

| **Methods** | **Node life time (s)** |
|---|---|
| LADS | **10** |
| OAS | **15** |
| PRiDE | **20** |
| Proposed | **55** |

## 5.4 Packet drop

Packet drop is validated by taking the difference between the amount of received packet by the total number of original packet in eqn.(6).

$$packet \quad drop = \frac{received \quad packets}{Total \quad packets} \tag{6}$$

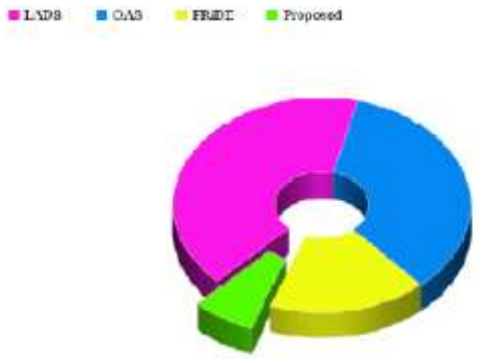


Figure 12. Packet drop ratio comparison

The comparison of packet drop ratio with existing approach is validated in fig. 12 and its statistics is drawn in Table 5

Table 5. Packet drop ratio

| Methods | Packet drop ratio |
|---|---|
| LADS | **10** |
| OAS | **8** |
| PRiDE | **6** |
| Proposed | **3** |

### 5.5 Discussion

From all the comparison validation results, the proposed approach proved its efficiency and which is applicable in all DTN wireless environment without much complexity. Aslo it assured the security communication in the wireless channel.

## 6. Conclusion

To afford the network channel for an IoT device is some more a critical issue, so that the present research work proposed a novel strategy which is ABDTN to construct an efficient network channel. The fitness ofn function of african buffalo is utilized here to predict the malicious and selfish node in earlier stage. Then a novel RPJ mechanism is introduced to tranfer the high load packet to the other noder duirin g the distribution process. Thus thecommunication channel of IoT is enhanced and spport to foprward the huge data to the far distances. Finnally, the proposed model is compared with existing approached and gained better resut by attaining the high packet delivey ratio as 99% and reduced packet drop ratio as 3%.

### *References*

[1] Gautam, P.K., Johari, R., Yadav, A.K., Dahiya, R., Kaur, I., Bhatia, R., Chaudhary, S.: Pride: Priority and reliability-based routing in delay tolerant network. Proceedings of ICETIT 2019, pp. 1016-1027. Springer International Publishing, Cham (2020).

[2] Reddy, M.P., Kumar, A., Kuchi, K.: Joint control and shared channel scheduling for downlink in 3gpp narrowband-iot. In: 2020 International Conference on COMmunication Systems NETworkS (COMSNETS), pp. 476-483 (2020). DOI 10.1109/COMSNETS48256.2020.9027476

[3] Redhu, S., Hegde, R.M.: Optimal relay node selection in time-varying iot networks using apriori contact pattern information. Ad Hoc Networks 98, 102065 (2020). DOI https://doi.org/10.1016/j.adhoc.2019.102065.

[4] Mao, Y., Zhou, C., Ling, Y., Lloret, J.: An optimized probabilistic delay tolerant network (dtn) routing protocol based on scheduling mechanism for internet of things (iot). Sensors 19(2) (2019). DOI 10.3390/s19020243.

[5] Gao, W., Liang, H., Nguyen, J., Liang, F., Yu, W., Lu, C., Orpilla, M.: Emulation-Based Performance Evaluation of the Delay Tolerant Networking (DTN) in Dynamic Network Topologies, pp. 23-41. Springer International Publishing, Cham (2020). DOI 10.1007/978-3-030-24344-9 2.

[6] Benhamida, F.Z., Bouabdellah, A., Challal, Y.: Using delay tolerant network for the internet of things: Opportunities and challenges. In: 2017 8th International Conference on Information and Communication Systems (ICICS), pp. 252-257 (2017). DOI 10.1109/IACS.2017.7921980

[7] Chekired, D.A., Khoukhi, L.: Multi-tier fog architecture: A new delay tolerant network for iot data processing. In: 2018 IEEE International Conference on Communications (ICC), pp. 1-6 (2018). DOI 10.1109/ICC.2018.8422170

[8] Kim, S.H., Han, S.J.: Delay-tolerant sensing data delivery for iot network by using signal strength information. Peer-to-Peer Networking and Applications 11(1), 181-197 (2018)

[9] Madamori, O., Max-Onakpoya, E., Grant, C., Baker, C.: Using delay tolerant networks as a backbone for low-cost smart cities. In: 2019 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 468-471 (2019). DOI 10.1109/SMARTCOMP.2019.00090

[10] Yao, Y., Sun, Y., Phillips, C., Cao, Y.: Movement-aware relay selection for delay-tolerant information dissemination in wildlife tracking and monitoring applications. IEEE Internet of Things Journal 5(4), 3079-3090 (2018). DOI 10.1109/JIOT.2018.2831439

[11] Chai, W.T., Ooi, B.Y., Liew, S.Y., Shirmohammadi, S.: Taxi-sharing: A wireless iot-gateway selection scheme for delay-tolerant data. In: 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), pp. 1-6 (2018). DOI 10.1109/I2MTC.2018.8409812

[12] Kim, S., Kim, D.Y.: Efficient data-forwarding method in delay-tolerant p2p networking for iot services. Peer-to-Peer Networking and Applications 11(6), 1176-1185 (2018)

[13] Mozny, R., Masek, P., Stusek, M., Zeman, K., Ometov, A., Hosek, J.: On the performance of narrow-band internet of things (nb-iot) for delay tolerant services. In: 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), pp. 637-642 (2019). DOI 10.1109/TSP.2019.8768871

[14] Kocherla, R., Vatambeti, R. An Efficient Routing Strategy for Energy Management in Wireless Sensor Network Using Hybrid Routing Protocols. *Wireless Pers Commun* **124,** 49–73 (2022). https://doi.org/10.1007/s11277-021-09318-x

[15] Liang, H., Gao, W., Nguyen, J.H., Orpilla, M.F., Yu, W.: Internet of things data collection using unmanned aerial vehicles in infrastructure free environments. IEEE Access 8, 3932-3944 (2020). DOI 10.1109/ACCESS.2019.2962323

[16] Cui, Jianqun, et al. "An adaptive spray and wait routing algorithm based on quality of node in delay tolerant network." *IEEE Access* 7 (2019): 35274-35286.

[17] Cuka, Miralda, et al. "Implementation and performance evaluation of two fuzzy-based systems for selection of IoT devices in opportunistic networks." *Journal of Ambient Intelligence and Humanized Computing* 10.2 (2019): 519-529

[18] Khalid, Waqar, et al. "Frid: Flood attack mitigation using resources efficient intrusion detection techniques in delay tolerant networks." *IEEE Access* 7 (2019): 83740-83760.

[19] Le, T.: Multi-hop routing under short contact in delay tolerant networks. Computer Communications 165, 1-8 (2021). DOI https://doi.org/10.1016/j.comcom.2020.10.018.

[20] Abdellaoui Alaoui, E.A., Zekkori, H., Agoujil, S.: Hybrid delay tolerant network routing protocol for heterogeneous networks. Journal of Network and Computer Applications 148, 102456 (2019).
DOI https://doi.org/10.1016/j.jnca.2019.102456.

[21] Zguira, Y., Rivano, H., Meddeb, A.: Iob-dtn: A lightweight dtn protocol for mobile IoT applications to smart bike sharing systems. In: 2018 Wireless Days (WD), pp. 131-136 (2018). DOI 10.1109/WD.2018.8361708

[22] AlZubi, Ahmad, et al. "Location assisted delay-less service discovery method for IoT environments." Computer Communications 150 (2020): 405-412.

[23] Zhou, Chongyu, Chen-KhongTham, and MehulMotani. "Online auction for scheduling concurrent delay tolerant tasks in crowdsourcing systems." Computer Networks 169 (2020): 107045

[24] Baig, Zubair A., et al. "Averaged dependence estimators for DoS attack detection in IoT networks." Future Generation Computer Systems 102 (2020): 198

[25] Nobahary, S., Garakani, H.G., Khademzadeh, A., Rahmani, A.M.: Selfish node detection based on hierarchical game theory in iot. EURASIP Journal on Wireless Communications and Networking 2019(1), 1-19 (2019)

[26] Abbas, S.: An efficient Sybil attack detection for the internet of things. In: A. Rocha, H. Adeli, L.P. Reis, S. Costanzo (eds.) New Knowledge in Information Systems and Technologies, pp. 339-349. Springer International Publishing, Cham (2019)

[27] Ahmad, N., Cruickshank, H., Cao, Y., Khan, F.A., Asif, M., Ahmad, A., Jeon, G.: Privacy by architecture pseudonym framework for delay tolerant network. Future Generation Computer Systems 93, 979-992 (2019). DOI https://doi.org/10.1016/j.future.2017.11.017.

**Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)**

Shridhar Sanshi – Proposed Algorithm, Coding and simulation of proposed approach.
Pramodh Krishna – Literature review and identification of related approaches for comparison.
Ramesh Vatambeti – Results and discussion