International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 14, No.1 (Sep-2023)

http://dx.doi.org/10.12785/ijcds/140166

Spider Monkey Algorithm for Enhancing Security in Delay Tolerant Network

Pradosh Kumar Gantayat[1] **and Raj Gaurang Tiwari**[2]

[1]*Faculty of Science and Technology, ICFAI Foundation for Higher Education, Hyderabad, India*
[2]*Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*

Received 06 Dec. 2022, Revised 13 Jul. 2023, Accepted 10 Aug. 2023, Published 01 Sep. 2023

Abstract: Delay tolerant networks (DTNs) have recently emerged as the preferred method of transmitting data to the destination node(DN). Furthermore, communications are sent through intermediary nodes, which impacts network security. The difficulty arises also due to selfish nodes and malicious nodes. To improve the efficiency of the network's transmission and reduce the number of dropped packets, Spider-Monkey-based Node Identity Confirmation (SMbNIC) architecture has been proposed in this paper. More than a hundred nodes are first set up in the DTN ecosystem. Each node's energy value is determined, and fitness is used in the DTN ecosystem to detect and eliminate selfish nodes and malicious nodes. When the proposed method's performance is compared to that of existing methods, it is clear that the proposed method is vastly superior in terms of reduced energy consumption, increased throughput, decreased delay in routing packets from source to destination, reduced packet loss, and increased packet transmission rate. Using these values, one may better construct a resilient and long-lasting network.

Keywords: Delay Tolerant Network, Energy Level, Selfish Node, Malicious Node, Forward Message, Attacks, Node Identity.

1. INTRODUCTION

Due to the impossibility of constant connection between every node in a contemporary Wireless Network (WN), information is sent through intermediary nodes[1]. When this happens, data transmission fails due of packet loss and latency in the connection[2]. In addition, DTN is crucial for the effective transmission of messages or data[3]. Each node in a DTN has a limited buffer memory to temporarily hold messages until they are sent to the next node in the chain of relays[4]. For the purpose of transmitting groups of messages over the network, DTN provides options such epidemic routing, Spray, direct delivery, PRoPHET(Probability Routing Protocol using History of Encounters and Transitivity), and wait for transferring bundles of messages in the network[5]. High error rates, intermittent connection, variable or extended latency, asymmetric data rates, confusing mobility patterns, and data loss are the most problematic occurrences during data transmission over a DTN[6]. The most common way to describe a DTN now is as a collection of disparate nodes[7]. It has highly mobile nodes with abundant resources that only broadcast a little amount of data[8]. The nodes of DTN are used to carry store and forward information to the destination node[9]. During the transmission process, messages are transferred over intermediate nodes which affects security problems in the network because of some selfish node[10]. Because of the limited resource such as storage capacity and energy it may drop messages[11]. It consists of three layers Bundle Layer (BL), Link Layer (LL), and application layer which are shown in figure 1 [12].

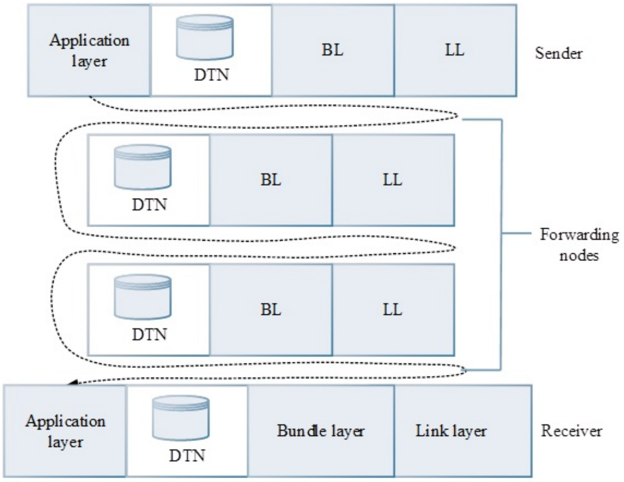

Figure 1. Layered architecture of DTN

Subsequently, the bundle layer is used for transferring the message to the intermediate nodes and the application node is used for providing user connectivity with other layers[13]. Over unreliable wireless links, DTN is categorized through frequent disconnection, high end-to-end latency, and opportunistic communication[14]. Moreover, DTN is comprised of mobile nodes which are suffering opportunistic communication, regularly changing network topology because of the absence of end-to-end connectivity, and sparse connection[15]. As well, DTN contains two uncooperative nodes such as a malicious node and a selfish node[16]. Consequently, the selfish node is reluctant for forwarding packets to the destination using other nodes[17]. Also, the malicious node can attack the system by interrupting the operation of the network[18]. As well, the identification of malicious and selfish nodes is the most challenging task in DTN[19]. The network performance is based on routing protocol, and the identification of security breakage and the presence of malware is the most difficult task[20]. So,there is a need to create a model for optimising safe routes in the DTN that can identify selfish and malicious nodes. The following is an exhaustive summary of the proposed model's primary contributions.

- Initially, the required number of nodes is created with a few selfish and malicious nodes in the DTN environment.
- Hereafter, novel SMbNIC framework is designed with a suitable parameter for monitoring the DTN.
- Accordingly, fitness is updated in the DT environment to check and identify the selfish or malicious nodes.
- During the identity verification process, if the node energy level is not matched to the normal node energy, selfish or malicious node is detected.
- At last, the achieved results of the proposed model are compared with existing techniques with respect to throughput, delay, energy consumption, packet loss, and packet delivery.

The rest of this paper is structured as follows: In Section 2, we discuss previous efforts in the same general area. Methods are described in further depth in Section 3. The findings are discussed in Section 4, and comparisons to other methods and the proposed model are made in Section 5. The study is then wrapped up in Section 6.

2. RELATED WORK

The following are descriptions of a few current literature reviews based on DTN security:

A bitcoin-based, secure incentive mechanism for cooperative vehicular DTN services was predicted by Youngho Park et al.[21]. Moreover, bitcoin is widely recognised as a leading global cryptocurrency and digital payment system. During implementation, the cryptographic technique is making the possibility of developing a credit-based incentive system at a low cost. But the attack rate is high when comparing other existing techniques.

The nodes of DTN carry, store and forward the information or data to the destination node. During the transmission, security issues take place due to some selfish nodes. Atul Sharma et al.[3] developed a backtracking algorithm based on DTN for contrasting selfish nodes. The developed algorithm helps distribute partially mannered nodes. The performance of the established results is compared with existing techniques. However, the packet drop ratio is found high.

DTN is one of the kinds of recurrently connected networks featured over intermittent connectivity, long delay, and asymmetric data. L. Wu et al.[22] offered a spray approach based on the social crisis for improving the routing algorithm. Based on the social crisis, the developed technique selects the next hop which enhances the performance. Multiple pieces of spray message are sent during the waiting period, delivering the redundant message over a secure route with a high error rate.

To improve the stable delivery service of the variable network in outlying areas, Yining Hu et al.[23] recommended using digital payments based on the blockchain. The developed model's primary function is to facilitate data transmission inside the base station by providing stable access to the regional network. However, the packet delivery rate is less compared to other techniques.

Sujoy Saha et al.[24] developed time efficient and lightweight routing system to detect the attacks present in the routing protocol. Moreover, a new trusted node is utilized to transfer all information through a long range of connectivity. Additionally, simulation is achieved with an improved ONE simulator that reveals the enabled connection between trusted nodes. But the main problem in the developed model is slow detection and high overhead which causes the less packet delivery rate.

3. PROPOSED METHODOLOGY

Spider monkeys communicate their thoughts and feelings via body language, including sexually receptive and aggressive stances. When travelling together, they use a unique cry that sounds like a horse's whinny to communicate across great distances. Each member of the group has a unique call that can be readily recognized by everyone else. Spider monkeys are able to avoid danger, band together, and chat across vast distances because to this kind of communication. Members of the group often rely on both verbal and acoustic means of interaction. In this research we are motivated to create a socially-aware stochastic optimization method by the foraging habits of spider monkeys. Based on their foraging habits, spider monkeys are classified as having a fission-fusion social structure (FFSS). The suggested method, which is inspired by the actions of spider monkeys when foraging, is best described in terms of FFSS.

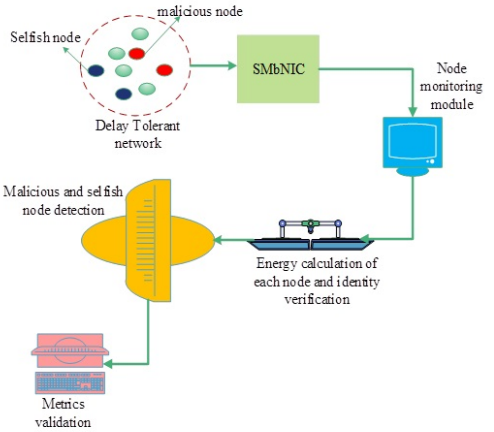

Figure 2. SMbNIC Architecture

This method breaks down spider monkey foraging behaviour into four phases. After foraging, the group evaluates their position in reference to food sources. In the second step, group members reassess their food source distance and posture. In step three, the local leader updates its best position within the group, and if it is not updated for a particular number of times, the group disperses and searches for food separately. In the fourth stage, the global leader improves its position and splits the group into smaller subgroups if necessary. The four stages are continued endlessly until the desired outcome is achieved.

The proposed algorithm uses a spider monkey algorithm to find the presence of selfish and malicious nodes in a wireless environment as they degrade the whole structure through hacking the user details or data and increasing the packet drop rate.

In this paper, a new Spider Monkey-based Node Identity Confirmation (SMbNIC) scheme has been proposed. The spider monkey fitness function is utilized in DT routing for identifying and detecting selfish nodes and malicious nodes during message transmission. Also, the power of the node has been checked frequently to reduce the packet drop. It contains nodes for forwarding a message from source node (SN) to destination node (DN). Finally, the performance metrics are validated with other states of the art techniques. The designed model is detailed in figure 2.

Selfish node and malicious node increase the packet drop ratio, dropped messages, and unsent messages. With the help of the SMbNIC, We quickly identify the selfish node and malicious node in the network.

A. Selfish and malicious node

Generally, the selfish node is one of the types of the node that drop every incoming message from SN and deny the forward messages to the other relay node for saving the energy and resource of the network. Those nodes are generating selfish behavior by degrading the delivery ratio of the network by aggregating the rate of packet drop. Furthermore, the main reason for the selfishness of the nodes in DTN establishment methods and limited network resources leads to an increase the attacks in network transmission. Furthermore, a malicious and selfish node in the network is shown in figure 3.

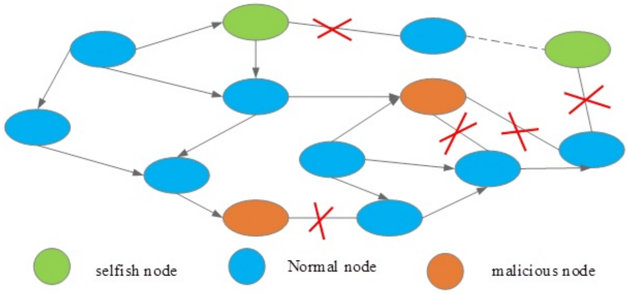

Figure 3. Selfish and malicious node

The selfish behavior is identified using computation requests from the service of the nodes. Thus the selfish nodes are identified using the energy level of each node. Moreover, a malicious node is a node which denies the service transmission to the other nodes in the network. It leads to attaining communication breakage and attacks.

B. Spider Monkey-based Node Identity Confirmation (SMbNIC)

The SMbNIC is the algorithm for detecting malicious and selfish nodes in the DTN and the model attains high efficiency and robustness in implementation. It has the essence of a few control parameters to identify and detect malicious and selfish nodes. Additionally, the time interval is required for investigating travel time and energy value. The various dimensional search spaces are useful to identify every node's energy value. Consequently, malicious and selfish node position is recognized using some variables in the DTN environment. Thus, the designed model involves three phases: node monitoring, energy level measurement, and selfish and malicious node detection. Moreover, distinguishing the node's position in DTN and node monitoring process are identified using Equation 1 and 2.

In the Equation 1, node position is identified before actual transmission occurs, here P_0 is called node position which can be calculated based on number of communication paths (C_0) available with respect to the destination node, and node movement with respect to the position (q*(s)). Here, q(s) is termed as SN and DN position.

$$P_0 = \left|C_0.q^*\left(s\right) - q\left(s\right)\right| \tag{1}$$

In the Equation 2, node travelling time has been calculated which is based on node movement with respect to the position ($q^*(s)$) and travelled node distance (D_t)

$$q\Big(s+1\Big)= q^{*}\Big(s\Big)-U_d.D_t \tag{2}$$

SN distributed information (U_d) is delineated in Equation 3.

$$U_d = 2u_d.r - u_d \tag{3}$$

The number of communication paths available with respect to the destination node has been calculated in Equation 4.

$$C_0 = 2.r \tag{4}$$

Where s is called as node time travelling time, r is denoted as a transmission path of equally transmitted nodes. The energy of each node is determined using Equation 5, and the nodes' classification as "normal," "selfish," or "malicious" is deduced from this information.

$$\vec{B}(T+1) = \begin{cases} q*(s) - U_d D_t, if e \geq 0.5 \\ D_t.e^{el}cos(2\pi l) + q^{*}(s), if e \leq 0.5 \end{cases} \tag{5}$$

Where D_t is called as every node travelled information with distance from SN to DN. Moreover, e is considered as nodes' continuous energy value. Furthermore, normal, selfish, and malicious nodes are separated using the calculated energy value also identify and detect the selfish and malicious nodes.

After determining the typical node's energy rate and node type, the following step may be taken. Using Equation 6 and 7, the selfish and malicious nodes are identified.

$$D_t = |U_d.s(n).m(n) - S(m)| \tag{6}$$

$$Q(s+1) = s(n).m(n) - S_m D_t \tag{7}$$

After identifying the node energy rate and normal node, the next step is to detect the selfish and malicious node by using Equation 6 and 7 where, s(n) is denoted as detection of selfish nodes present in DTN and m(n) is represented as malicious nodes detection. Likewise, S_m is denoted as the spider monkey fitness function, which examines the information of the presented node based on data packets and finally identifies the malicious and selfish nodes based on the energy level calculation of each node. The gained fitness function of the designed model is calculated using Equation 7. Thus, the proposed replica attains high performance for detecting selfish and malicious nodes and less computation time.

Algorithm 1 SMbNIC [Selfish and Malicious Node Identification and Characterization]

```
Initialize $n$ number of nodes as input
Update to SMbNIC
Start monitoring process    ▷ it will monitor the node position and movements
while $s$ ¡ $MaximumMovementOfNode$ do
    Update $U_d$, $D_t$, $C_0$, and $e$
end while
Send the analyzed information to the next stage
Energy level calculation based on the behavior of the nodes
        NodeMonitoringModule → EnergyCalculation
Update the position of the node
if $U_d < 1$ then
    The energy level of moving node value measured
else if $U_d \geq 1$ then
    Identify the moving node energy value using Equation 5
end if
Detection phase    ▷ identify and detect the selfish and malicious node
if $e \geq 0.5$ then
    Detect the selfish node
else if $e < 0.5$ then
    Detect the malicious node
else
    Detect the Normal node
end if
Measure the fitness function using Equation 7
```

4. RESULTS AND DISCUSSION

In order to identify malicious and selfish nodes in DTN, a unique SMbNIC approach was developed. The DTN environment begins with a MATLAB-generated 500 nodes. Each DTN node has its own unique energy value. A selfish node and a malicious node are distinguished by their respective energy values. In order to identify the selfish and malicious nodes, the developed model employs three procedures. Finally, the created model's performance metrics—with regards to energy consumption, packet delivery rate, throughput, packet transmission rate are verified using established methods.

A. *Performance Evaluation*

The implementation work of the developed SMbNIC is done by the MATLAB tool and the parameters like throughput, energy consumption, delay packet loss, and packet transmission are calculated. Moreover, the developed approach is validated using existing methods like Performance Optimization in DTN using Backtracking Algorithm (POBA)[3], Adaptive Multiple Spray and Wait for Routing system (AMSWR)[22], DT Payment Technique using Ethereum Blockchain (EB)[23], and Efficient Lightweight Technique in DTN routing (ELT)[24].

1) *Energy Consumption*

During the process of communication, nodes spend some amount of energy for interacting SN to DN through packet transmission of relay nodes. Moreover, the required total amount of energy for communicating packets is called energy consumption. Thus, the measurement of energy consumption is obtained by Equation 8.

$$E_c = (R_s S_n) + E_t \tag{8}$$

Where R_s stands for the energy that was received, E_t for the energy that was sent, S_n for the source node. In addition, each node's average guess is used to determine its energy usage. In this case, the best solution is supplied to nodes with the lowest energy use. Table I provides a breakdown of the energy use comparisons.

Table I shows that energy consumption in the network of 100 nodes for POBA, AMSWR, EB, and ELT methods are 19.423J, 56.12J, 14.64J and 33.42J respectively. But, the energy consumption for proposed SMbNIC method is only 8.23J in the same network. Thus the less energy consumption enhances the lifetime of the node.

2) *Throughput*

The network capacity of the proposed framework is optimal with respect to the total number of packets transported successfully between the SN and DN. Moreover, throughput is calculated using Equation 9.

$$T_p = \frac{PR}{PS} \tag{9}$$

Where PR stands for the total number of packets received at the destination and PS stands for the total number of packets transmitted from the origin. Table II provides an in-depth analysis of the differences in throughput.

The developed SMbNIC technique gained a large rate of throughput as 1000kbps in the network of 100 nodes. Moreover, POBA, AMSWR, EB and ELT methods attained 712.44kbps, 271.7kbps, 628.93kbps and 351.9kbps respectively. Thus, the large rate of throughput shows the reliability of the network.

3) *Delay*

It is the sum total of everything that happens as a packet travels from SN to DN. In other words, the delay is the entire transmission rate of packet size divided by the ratio of distance and speed evaluation. As a result, Equation 10 includes a discussion of how to determine the delay.

$$delay = \sum_{i=1}^{n} \frac{P_i}{P_r} \tag{10}$$

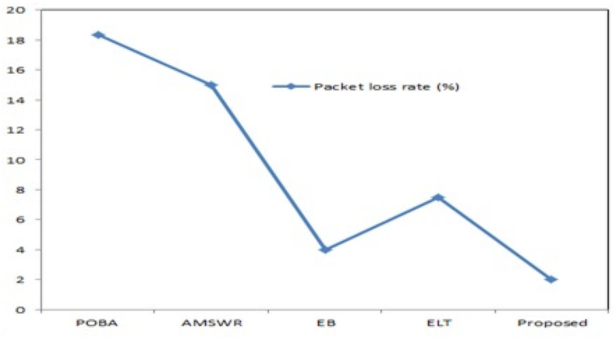

Figure 4. Comparison of packet loss rate

The time it takes for data packets to travel from the sender's location to the DN is denoted by P_i , while the number of packets successfully received at the destination is denoted by P_r . The table III provides a comparison of the time delays associated with several existing approaches.

Table III shows that in the network of 100 nodes POBA, AMSWR, EB and ELT techniques attained delay rates 3.76s, 9.68s, 5.34s and 12.3s respectively while the proposed SMbNIC method gained delay rate 1.5s. While comparing to proposed method with other techniques in the network of higher nodes, proposed method attains least delay rate in every case. Thus, the proposed framework enhances the performance of the transmission path.

4) *Packet Loss*

The quantity of package or data is not received in the DN or last point at a given specific quantity of time and it is calculated using Equation 11.

$$P_{drop} = \frac{amountofpacketdrop}{timeperiod} \tag{11}$$

High rates of dropped packets may render a whole network useless. In figure 4, we see a comparison of packet losses.

Figure 4 shows that POBA, AMSWR, ELT and EB attained packet loss rates 18.34%, 15%, 7.5%, and 4% respectively. But the proposed SMbNIC method attained 2% packet loss rate which is very less compared to other existing approaches.

5) *Packet Transmission*

Data broadcast over the whole network may be calculated by looking at the packet transfer rate. Additionally, packet transmission is the ratio of packets sent to packets received, and may be calculated mathematically using Equation 12.

$$P_t = \frac{Tp}{Rp} \tag{12}$$

Where T_p is the total number of packets sent and R_p is the total number of packets received. Table IV provides a

TABLE I. Validation of energy consumption (in Joule)

No. of Nodes	POBA	AMSWR	EB	ELT	Proposed
100	19.423	56.12	14.64	33.42	8.23
200	41.508	60.03	21.43	39.03	11.78
300	44.865	61.11	25.23	42.13	13.67
400	53.112	67.12	32.43	45.7	15.03
500	55.993	68.98	36.65	51.2	18.45

TABLE II. Validation of Throughput(in kbps)

No. of Nodes	POBA	AMSWR	EB	ELT	Proposed
100	712.44	271.7	628.93	351.9	1000
200	537.71	271.9	661.31	366.32	880
300	481.74	284.5	596.90	370	745
400	327.65	284.3	495.76	375.67	700
500	237.90	320.3	496.35	380	634

TABLE III. Validation of Delay (in seconds)

No. of Nodes	POBA	AMSWR	EB	ELT	Proposed
100	3.76	9.68	5.34	12.3	1.5
200	4.47	9.72	9.31	16.83	1.7
300	6.61	11.38	13.5	19	1.9
400	7.62	12.12	21.4	22.42	2.2
500	10.42	14.13	30	24	4

more in-depth comparison of packet transfer.

The developed SMbNIC technique gained a large rate in packet transmission rate which is 99.02% for using 100 nodes. It shows the packet delivery rate from the SN to the DN. Moreover, POBA and AMSWR methods attained 98.92% and 77.44% which is less when comparing other techniques. Also, the EB and ELT techniques gained 93.54% and 85% rates in packet transmission.

5. CONCLUSION

This paper introduces Spider-Monkey-based Node Identity Confirmation (SMbNIC) framework to overcome the issues of less packet transmission, high packet drop, and attacks. The main aim of the proposed framework is to detect malicious and selfish nodes in DTN network for enhancing security. Initially, the moving node present in the DTN environment is observed and the energy levels of each node are calculated. At last, the selfish node and malicious node are detected using Spider monkey optimization. The selfish and malicious nodes are easily identified and detected using the calculated energy level. Moreover, the proposed model secures the information, provides secure communication, and enhances the performance of the packet transmission rate. Experimental results show that the proposed model outperforms other states of the art models with a high packet transmission rate (99.02%), less packet loss rate (2%), least delay rate (1.5s), least energy consumption (8.23J) and large rate of throughput (1000kbps) for network having 100 nodes. For the network having a larger number of nodes similar results are obtained. Just because of these better results a network with enhanced lifetime and reliability can be realized.

References

[1] S. He, K. Xie, K. Xie, C. Xu, and J. Wang, "Interference-aware multisource transmission in multiradio and multichannel wireless network," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2507–2518, 2019.

[2] P. K. Gantayat, R. G. Tiwari, and A. Misra, "An optimization based anonymous messaging system for data security in delay tolerant network," in *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*. IEEE, 2022, pp. 1–6.

[3] A. Sharma, N. Goyal, and K. Guleria, "Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes," *The Journal of Supercomputing*, vol. 77, no. 10, pp. 6036–6055, 2021.

[4] R. G. Tiwari, A. K. Jain, P. K. Gantayat, N. Jain, and V. Jindal, "Ant lion based optimized leach protocol to enhance the security and transmission of wireless sensor network," in *2022 International Interdisciplinary Conference on Mathematics, Engineering and Science (MESIICON)*. IEEE, 2022, pp. 1–6.

[5] S. Jangra, A. K. Pandit, N. Gupta, R. Jain, and R. Rana, "Performance analysis of vehicular delay tolerant network," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*. IEEE, 2019, pp. 211–216.

TABLE IV. Packet Transmission rate verification using packets (in percentage)

No. of Nodes	POBA	AMSWR	EB	ELT	Proposed
100	98.92	77.44	93.54	85	99.02
200	96.38	72.56	89.34	83.12	99
300	96.29	73.98	85.87	81	98.78
400	94.99	74.16	84.56	79.04	98.54
500	94.03	74.23	82.54	77	98

[6] O. Gupta and N. Goyal, “The evolution of data gathering static and mobility models in underwater wireless sensor networks: a survey,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9757–9773, 2021.

[7] H. Zekkori and S. Agoujil, “Hybrid delay tolerant network routing protocol for heterogeneous networks,” *Journal of Network and Computer Applications*, vol. 148, p. 102456, 2019.

[8] K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang, “Cooperative content caching in 5g networks with mobile edge computing,” *IEEE Wireless Communications*, vol. 25, no. 3, pp. 80–87, 2018.

[9] X. Fan and W. Dong, “Application of dtn protocol in aircraft cluster network,” in *IEEE 20th International Conference on Communication Technology (ICCT)*, 2020.

[10] J. Liu, Z. Liu, C. Sun, and J. Zhuang, “A data transmission approach based on ant colony optimization and threshold proxy re-encryption in wsns,” *Journal of Artificial Intelligence and Technology*, vol. 2, no. 1, pp. 23–31, 2022.

[11] S. Aheleroff, X. Xu, Y. Lu, M. Aristizabal, J. P. Velásquez, B. Joa, and Y. Valencia, “Iot-enabled smart appliances under industry 4.0: A case study,” *Advanced engineering informatics*, vol. 43, p. 101043, 2020.

[12] S. Panchiwala and M. Shah, “A comprehensive study on critical security issues and challenges of the iot world,” *Journal of Data, Information and Management*, vol. 2, no. 4, pp. 257–278, 2020.

[13] S. R. Das, K. Sinha, N. Mukherjee, and B. P. Sinha, “Delay and disruption tolerant networks: a brief survey,” *Intelligent and Cloud Computing*, pp. 297–305, 2021.

[14] N. N. Pal, K. Gaikwad, and D. Das, “Trust calculation and route discovery for delay tolerant networks,” in *TENCON 2018-2018 IEEE Region 10 Conference*. IEEE, 2018, pp. 1533–1537.

[15] Y. Mawad and S. Fischer, “Hidtn: Hybrid dtn and infrastructure networks for reliable and efficient data dissemination,” in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 2018, pp. 1–8.

[16] R. Dalal and M. Khari, “Factual demonstration of blockchain routing in delay tolerant network,” 2021.

[17] N. Xiao, R. Xinyi, Z. Xiong, F. Xu, X. Zhang, Q. Xu, X. Zhao, and C. Ye, “A diversity-based selfish node detection algorithm for socially aware networking,” *Journal of signal processing systems*, vol. 93, no. 7, pp. 811–825, 2021.

[18] M. Kumar, P. Mukherjee, K. Verma, S. Verma, and D. B. Rawat, “Improved deep convolutional neural network based malicious node detection and energy-efficient data transmission in wireless sensor networks,” *IEEE Transactions on Network Science and Engineering*, 2021.

[19] S. Chatterjee, M. Nandan, A. Ghosh, and S. Banik, “Dtnma: identifying routing attacks in delay-tolerant network,” in *Cyber Intelligence and Information Retrieval*. Singapore: Springer, 2022, pp. 3–15.

[20] S. Kumar, “Prediction of node and link failures in mobile ad hoc network using hello based path recovery routing protocol,” *Wireless Personal Communications*, vol. 115, no. 1, pp. 725–744, 2020.

[21] Y. Park, C. Sur, and K.-H. Rhee, “A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency,” *Security and Communication Networks*, vol. 2018, p. 5932183, 2018.

[22] L. Wu, S. Cao, Y. Chen, J. Cui, and Y. Chang, “An adaptive multiple spray-and-wait routing algorithm based on social circles in delay tolerant networks,” *Computer Networks*, vol. 189, p. 107901, 2021.

[23] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, “A delay-tolerant payment scheme based on the ethereum blockchain,” *IEEE Access*, vol. 7, pp. 33 159–33 172, 2019.

[24] S. Saha, S. Nandi, R. Verma, S. Sengupta, K. Singh, V. Sinha, and S. K. Das, “Design of efficient lightweight strategies to combat dos attack in delay tolerant network routing,” *Wireless Networks*, vol. 24, no. 1, pp. 173–194, 2018.

Pradosh Kumar Ghantayat Dr.Pradosh Kumar Gantayat has received Ph.D degree in Computer Science and Engineering from VSS University of Technology, Odisha, India in the year 2021 and M.Tech degree in Computer Science and Engineering from KIIT University, Odisha, India in the Year 2007. He has total 20 years of teaching experience and his major research interests are Ad-Hoc Network, Soft Computing, Cryptography, and Wireless Sensor Network Security. He has received Best paper awards in IEEE conferences and Research Excellence award from Institute of Scholar, Bangalore. He has published more than 20 research papers in different International Journals and Conferences.

Raj Gaurang Tiwari Dr. Raj Gaurang Tiwari received Ph.D. (Computer Science) in 2013, M. Tech. (Computer Science and Engineering) in 2010 and Master in Computer Application in 2002. He has teaching and research experience of 20 years. He is presently working as Professor and Dean in the Department of Computer Science and Engineering at Chitkara University, Punjab. He also worked as Associate Professor in the Department of Computer Science and Engineering at Sri Ramswaroop Memorial Group of Professional Colleges, Lucknow and as Assistant Professor at AZAD Institute of Engineering and Technology, Lucknow. His research interests primarily embrace Knowledge-Based Engineering, Web Engineering, Ad-hoc/Sensor Network, Recommender Systems and Data Science. He has authored more than 70 International and national journal and conference papers. He is member of Programme Committee / Technical Committee /Reviewer for many international conferences/journals.