IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 10, Issue.5, May 2022 E-ISSN: 2347-2693

Mitigating Routing Misbehavior in Disruption Tolerant Networks

S. Devadharshini[1*], R. Vadivel[2]

[1]PG Student, Department of Information Technology, Bharathiar University, Tamil Nadu India
[2]Assistant Professor, Department of Information Technology, Bharathiar University, Tamil Nadu, India

**Corresponding Author: deashinishamara0103@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v10i5.3035 | Available online at: www.ijcseonline.org

Received: 21/Apr/2022, Accepted: 08/May/2022, Published: 31/May/2022

***Abstract*—** Destructive Tolerance Network (DTN) can drop packets received by selfish or malicious nodes. These routing malfunctions slow down packet delivery and waste system resources such as power and bandwidth. Techniques have been proposed to mitigate routing malfunctions in mobile ad hoc networks, but they cannot be applied directly to DTN due to the intermittent connections between the nodes. To address this issue, we propose a distributed method to detect packet drops on the DTN. In our scheme, the node should keep a signed contact record for the previous contact. Based on this, the next node to contact can determine if the node dropped the packet. Rogue nodes can falsely report contact records to avoid detection, so a small portion of each contact record is distributed to the specified number of watch nodes and the appropriate contact record. Can be collected to identify rogue nodes. We also propose a scheme to mitigate incorrect routing behavior by limiting the number of packets forwarded to malicious nodes. Trace-based simulations show that our solution is efficient and can effectively mitigate routing fraud.

***Keywords*—** Disruption Tolerant Networks, Detection, Mitigation, Routing Misbehaviour, Security.

I. INTRODUCTION

Disruption Tolerant Networks (DTN) transfers data using intermittent connections between mobile nodes. Due to the lack of consistent connections, the two nodes exchange data only when they move into each other's range of transmission (called contact between the nodes). Therefore, DTN routing usually follows store carry forward. That is, when a node receives some packets, it buffers them, carries them until it connects to another node, and then forwards the packets. With DTN, even if a node has enough buffers, it can malfunction by dropping packets. Routing malfunctions can be caused by selfish nodes that do not want to consume resources such as power or buffers to forward other packets, or malicious nodes that drop packets to launch an attack.

Routing misbehaviour will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets. To demonstrate this, we will simulate the effects of routing malfunctions with two popular DTN routing algorithms, SimBet and Delegation, based on reality tracing. SimBet is a transfer-based algorithm with only one replica in the package. Delegation is a replication-based algorithm that allows a package to have multiple copies. If 30% of the hottest nodes aren't working properly, SimBet will deliver only 3% of the packets, while the delegation will only deliver 40%. In addition, 95% of SimBet's transmissions and 80% of delegations are wasted because packets are eventually dropped by the failed node.

Although Burgess et al. studied the effect of packet drops on packet delivery rates, but did not take into account the wasted transmission (bandwidth) caused by the drops. Therefore, it is very important to detect packet drops and mitigate routing malfunctions on the DTN.]. Routing malfunctions are widely studied in mobile ad hoc networks. These tasks use adjacency monitoring or acknowledgment (ACK) to detect packet drops and avoid node malfunctions in path selection. However, intermittent connections on the DTN are not considered and cannot be applied directly to the DTN. This white paper addresses DTN routing failures by answering two questions: how to detect packet drops and how to limit the traffic that flows to the failed node. First, we propose a distributed method for detecting packet drops.

This scheme requires the node to have a previously signed contact record. B. Report buffered packets and packets sent or received to the next contact node. This allows you to see from the reported records whether the node dropped the packet. Bad nodes may spoof some records so they are not recognized, but this violates some integrity rules. To detect such inconsistencies, a small portion of each contact record is propagated to several selected nodes. These nodes can collect the appropriate contact records and identify the malfunctioning node with a certain probability. Next, we propose a scheme to mitigate routing malfunctions by limiting the number of packets forwarded to the malfunctioning node.

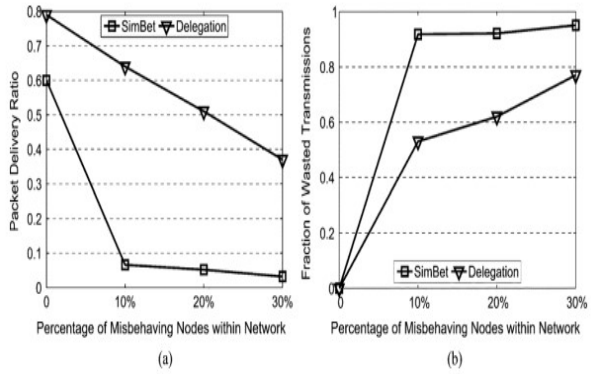


Fig 1. Effects of Routing Misbehaviour when SimBet and Delegation are used as the routing algorithm

II. BACKGROUND STUDY

W. Gao and G. Cao [1] Data distribution is useful for many applications of Fault Tolerant Networks (DTN). Current data delivery schemes are generally network-centric, ignoring user interest. This paper proposes a new approach for user-centered data propagation in DTN that considers user satisfaction and maximizes the cost-effectiveness of data propagation. Our approach is based on social centrality metrics that simultaneously consider the social contact patterns and interests of mobile users and ensure effective relay selection. The performance of our approach is evaluated from both theoretical and experimental perspectives. Through formal analysis, we show the lower limit of cost-effectiveness of data propagation and analyze the trade-off between the effectiveness of relay selection and the maintenance work of network information. Through lane-driven simulation, we show that our approach achieves better cost efficiency than existing data distribution schemes.

H. Yang, J. Shu, X. Meng, and S. Lu [2] Protecting the network layer from malicious attacks is an important but difficult security issue in mobile ad hoc networks. This white paper describes SCAN, an integrated network layer security solution for such networks that protects both routing and data transfer operations through the same reactive approach. SCAN does not apply cryptographic primitives to routing messages. Instead, it protects your network by detecting and responding to malicious nodes. In SCAN, local neighbors jointly monitor and support each other, but one node is no better than the others. SCAN also adopts a new credit strategy to reduce overhead costs over time. Essentially, SCAN uses localized collaboration and cross-validation of information to protect your network in a self-organized way. Through analytical and simulation results, we demonstrate the effectiveness of SCAN even in highly mobile and hostile environments.

K. Fall [3] Most existing ad hoc network designs are based on the premise of a non-hostile environment in which all nodes in the network operate in a coordinated and successful manner. If there are bad nodes in the network, the performance of the current routing protocol will be significantly reduced. Since Ad hoc networks of autonomous nodes are inherently open and distributed, making maintaining a healthy network environment very difficult and costly. In this paper, they propose a new routing service called Best Effort Fault Tolerant Routing (BFTR). The design goal of BFTR is to provide a high delivery rate, low overhead packet routing service in the presence of behaviourally problematic nodes. Instead of deciding whether the path is good or bad, i. H. BFTR evaluates the feasibility of routing a path based on end-to-end performance (such as packet delivery rate and delay), regardless of whether it contains a problematic node. By continuously monitoring routing performance, BFTR dynamically routes packets to the most appropriate path. BFTR provides an efficient and unified solution for various node failures with little assumption of security. The BFTR algorithm is evaluated by both analysis and extensive simulation. The results show that BFTR significantly improves ad hoc routing performance in the presence of problematic nodes.

J. Burgess, B. Gallagher, D. Jensen, and B. Levine [4] They are proposing MaxProp, a protocol for effectively routing DTN messages. MaxProp is based on prioritizing both the schedule of packets sent to other peers and the schedule of packets dropped. These priorities are based on the probability of a path to a peer based on historical data, as well as some complementary mechanisms such as acknowledgments, early initiation of new packets, and a list of previous arbiters. Our opinions display that MaxProp plays higher than protocols which have get admission to to an oracle that is aware of the time table of conferences among peers. Our rating is based on a 60-day trace from an actual DTN network deployed on 30 buses. A network called UMassDieselNet serves a large geographical area between five universities. It also evaluates MaxProp in a simulated topology and shows that it works well in different DTN environments.

E. Daly and M. Haahr [5] They present social network analysis metrics that can be used to support innovative and practical transfer solutions to provide efficient messaging with individual delay-tolerant MANETs. These metrics are based on a social analysis of the node's past interactions and consist of three locally scored components. Node Target Relationship with node. Presenting a simulation with three real-world trace datasets, we show that combining these metrics can achieve delivery performance close to epidemic routing, but with significant overhead savings. In addition, it has improved performance compared to PROPHET routing.

V. Erramilli, A. Chaintreau,M. Crovella, and C. Diot [6] Node speed, which is a generalized random waypoint model with heterogeneous nodes, is considered a transfer metric that includes short-term and long-term velocities. Next, we propose multi-copy delegation transfer based on short-term and long-term speeds of DTN (DFSL). This first determines the comprehensive allocation of short-term

and long-term speeds to the actual transfer metric. Then, according to forwarding metrics and delegation forwarding strategies, DFSL has several efficient nodes with higher forwarding metrics to support message delivery to improve delivery rates while reducing forwarding costs. Use. Finally, run the simulation based on the synthetic mobility pattern and the actual lanes. The results show that DFSL achieves the highest transfer efficiency compared to other multi-copy transfer strategies. This is the delivery rate divided by the transfer cost.

S. Marti, T. J. Giuli, K. Lai, and M. Baker [7] Mobile ad hoc network routing protocols are designed on the assumption that nodes will work together to forward packets between remote nodes using multi hop communication. Coordination between nodes does not always exist. Nodes can malfunction to save on missing resources such as battery power and bandwidth. Reputation-based mechanisms have been proposed to address the issue of fraud detection and isolation. This mechanism allows a node to rank the reputation score of another node based on direct and indirect observations of the behavior of the other node. The root path is created based on this behavior observed between the source and the destination. This method helps identify the failed node in your network.

H. Yang, J. Shu, X. Meng, and S. Lu [8] they describe SCAN, An integrated network layer security solution for such networks that protects both routing and data transfer operations through the same reactive approach. SCAN does not apply cryptographic primitives to routing messages. Instead, it protects your network by detecting and responding to malicious nodes. In SCAN, local neighbors jointly monitor and support each other, but no node is better than the others. SCAN also adopts a new credit strategy to reduce overhead costs over time. Basically, SCAN uses localized collaboration and cross-validation of information to protect your network in a self-organized way. Through both analysis and simulation results, we demonstrate the effectiveness of SCAN even in a highly mobile and hostile environment.

K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan [9] In general, MANET routing protocols are designed on the assumption that all participating nodes are fully coordinated. However, due to the open structure and the battery-based energy that is rarely available, the node can malfunction. One such routing malfunction is that some selfish nodes participate in the route discovery and maintenance process, but refuse to forward data packets. This article proposes a 2ACK scheme. It acts as an add-on technology for routing schemes, detecting routing malfunctions and mitigating their negative effects. The main idea of the 2ACK scheme is to send a 2-hop acknowledgment packet in the opposite direction of the routing path. To reduce additional routing overhead, only some of the received data packets are acknowledged in the 2ACK scheme. Analysis and simulation results are presented to evaluate the performance of the proposed system.

B. Burns, O. Brock, and B.N. Levine [10] A routing protocol MV that learns and uses the structure of network participants' movement patterns to enable informed message forwarding. We also propose the introduction of autonomous agents as additional participants in DTN. These agents adjust their behavior in response to fluctuations in network capacity and demand. Uses multipurpose control techniques derived from robotics to generate movements that can simultaneously optimize multiple network performance metrics. We provide experimental evidence that these strategies, individually or in combination, can significantly improve DTN performance.

J. Davis, A. Fagg, and B.N. Levine [12] Address routing support for wireless ad hoc networks in sporadic connections and ubiquitous network partition conditions. This task proposes a general framework for agent movement and communication in which mobile computers physically forward packets between network partitions. Next, we propose an algorithm that takes advantage of the relative position of quested devices and the non-randomness of mobile agent movement in the network. The trained structure of the network is used to inform adaptive routing strategies. Simulations are used to evaluate these algorithms and their ability to efficiently route packets over a highly partitioned network.

III. PROPOSED METHODOLOGY

A distributed method for detecting packet drops. This scheme requires the node to have a previously signed contact record. B. Report buffered packets and packets sent or received to the next contact node. The following contact node can see from the reported record whether the node dropped the packet. Bad nodes may spoof some records so they are not recognized, but this violates some integrity rules. To detect such inconsistencies, a small portion of each contact record is distributed to several selected nodes. These nodes can collect the appropriate contact records and detect a malfunctioning node with a certain probability. Routing malfunctions are widely studied in mobile ad hoc networks. These tasks use the Adjacent Monitor or Acknowledgment (ACK) to detect packet drops and avoid node malfunctions in path selection.

Our approach consists of a packet drop detection scheme and a routing malfunction mitigation scheme. Contact during each contact and report previous contact records to the contact node. Based on the contact record reported, the contact node detects if the failed node dropped the packet. A misbehaving node can make false reports (that is, report fake contact records) to hide the fraud, but fake records can cause inconsistencies and detect false reports. To detect false reports, the connected node randomly selects a specific number of monitoring nodes for the reported records and sends a summary of each reported record when connecting to them. A Witness node that collects two inconsistent contact records can identify the false reporting

node. Here are some approaches to mitigate routing malfunctions. Reduce traffic to bad nodes in two ways:
If a malfunctioning node makes a false alarm, it will be blacklisted (after the false alarm is detected) and will not receive packets from other nodes.
If you report the contact record honestly, the contact's node can monitor the drop behavior and receive much less packets from the node.

Mitigation node should keep previously signed contact records, such as buffered packets and packets sent and received, and report to the nearest contact node. This allows you to use the reported record to determine if the node dropped the packet.
Mitigate routing misbehavior via way of means of restricting the variety of packets forwarded to the misbehaving nodes.

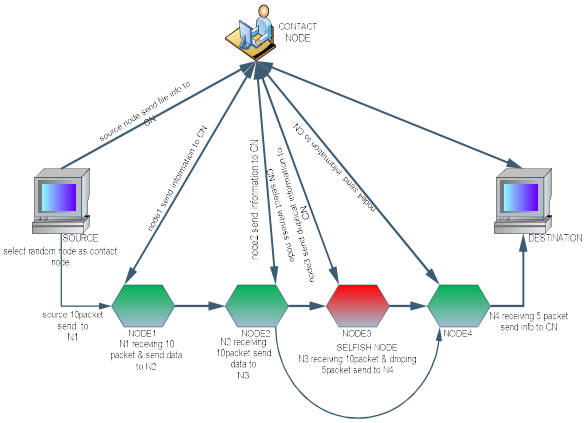
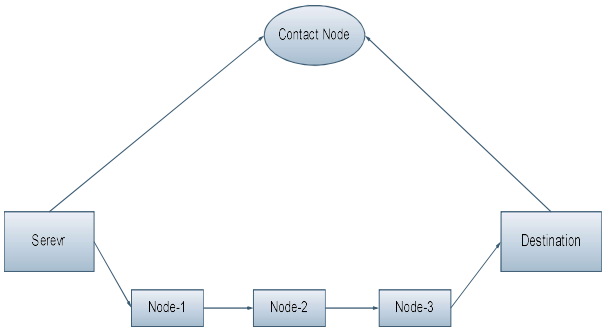
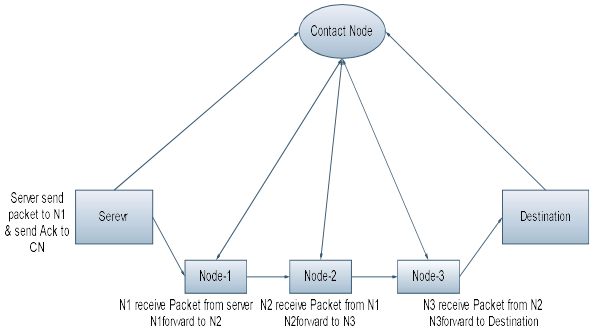


Fig 1. Mitigating misbehaves and misreport node

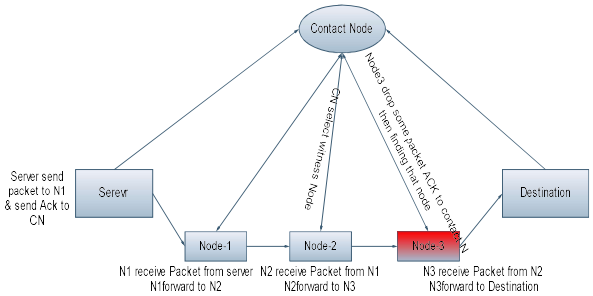
A. Contact Node
In our scheme, the node should keep a signed contact record for the previous contact. Based on this, the next node to contact can determine if the node dropped the packet. Because rogue nodes can incorrectly report contact records to avoid detection, a small portion of each contact record is distributed to a specified number of watch nodes to provide the appropriate contact record. You can collect and identify rogue nodes



B. Forwarding Node
An interesting set of tasks is to attempt a packet forwarding scheme in which each node opportunistically forwards a packet to an adjacent node consisting of multiple candidate nodes. First, consider how to optimize the forwarding scheme to minimize the expected delay in delivering packets from the node to the recipient or destination. Greatly reduces expected shop delays.



C. Witness Node
To detect false reports, the connected node randomly selects a specific number of monitoring nodes for the reported records and sends a summary of each reported record when connecting to them. A Witness node that collects two inconsistent contact records can identify the false reporting node. To detect mistakes, a regular node selects a watch node for each contact record that the regular node creates (or receives) other nodes and sends a summary of the records to them. The summary contains only a portion of the dataset needed to reveal the inconsistencies caused by false positives.



IV. RESULTS AND DISCUSSION

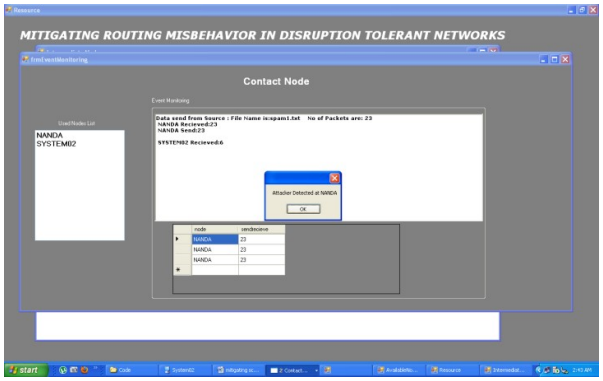


Fig 2. Mitigation Routing Misbehaviour in Disruption Tolerant Network.

The mitigation node should keep a previously signed contact record, such as buffered packets and packets sent and received, and report it to the nearest contact node. This allows you to use the reported record to determine if the node dropped the packet. If an unauthorized user logs in, the recipient will get 50% of the data. The status is then displayed as non-compliant data and a notification is sent to the user.

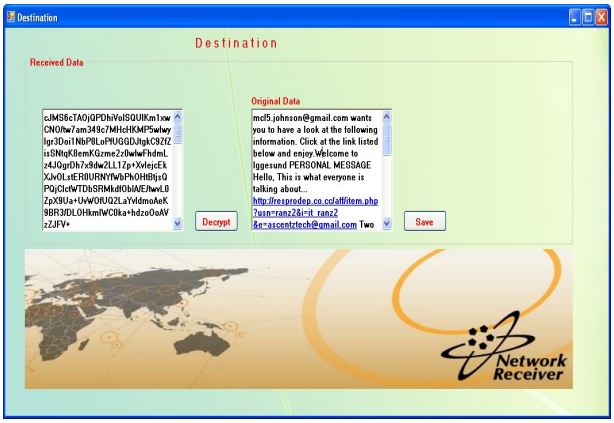


Fig 3. Destination

The encrypted data is decoded into the original file at the final destination.

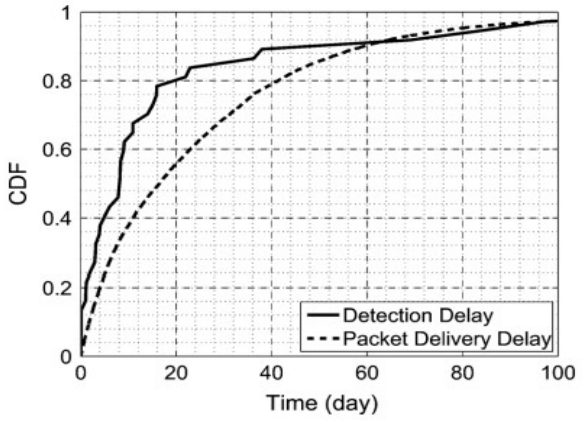


Fig 4. Detection delay compared with the packet delivery delay.

Storage overhead, along with parameters, is significantly increased because record summaries are stored on more nodes for a longer period of time. However, the memory overhead increases only slowly with the packet generation rate. This is because the main source of storage overhead is record summaries that are stored for a relatively long period of time, rather than contact records that are deleted immediately, and the number of record summaries that are generated is contact, not traffic load. This is because it depends only on the previous number. In general, the memory overhead of this scheme is small, less than 200KB on each node.

V. CONCLUSION

This white paper introduced a scheme for detecting DTN packet loss. The discovery scheme works in a distributed manner, with each node detecting local drops of packets based on the information collected. In addition, the detection scheme can effectively detect false positives, even if some nodes are secretly coordinating. Analysis results on detection probability and detection delay were also presented. Next, based on the packet drop detection scheme, we proposed a scheme to mitigate routing malfunctions in DTN. The proposed scheme is very common and does not depend on any particular routing algorithm. Trace-based simulations show that our solution is efficient and can effectively mitigate routing fraud.

REFERENCE

[1] W. Gao and G. Cao, "User-centric data dissemination in disruption tolerant networks," in Proc. IEEE INFOCOM, **pp. 3119–3127, 2011.**

[2] H. Yang, J. Shu, X. Meng, and S. Lu, "Scan: Self-organized network-layer security in mobile ad hoc networks," IEEE J. Sel. Areas Commun., **vol. 24, no. 2, pp. 261–273, 2006.**

[3] K. Fall, "Providing fault-tolerant ad-hoc routing service in adversarial environments," in Proc. SIGCOMM, **pp. 27–34, 2003.**

[4] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in Proc. IEEE INFOCOM, **pp. 1–11, 2006.**

[5] E. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in Proc. ACM MobiHoc, **pp.32–40, 2007.**

[6] V. Erramilli, A. Chaintreau,M. Crovella, and C. Diot, "Delegation forwarding," in Proc. ACM MobiHoc, **pp. 251–260, 2008.**

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviorin mobile ad hoc networks," in Proc. ACM MobiCom, **pp.255–265, 2000.**

[8] H. Yang, J. Shu, X. Meng, and S. Lu, "Scan: Self-organized network-layer security in mobile ad hoc networks," IEEE J. Sel. AreasCommun., **vol. 24, no. 2, pp. 261–273, 2006.**

[9] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior inMANETs," IEEE Trans. Mobile Comput., **vol. 6, no. 5, pp. 536–550, May 2007.**

[10] B. Burns, O. Brock, and B.N. Levine. "MV routing and capacity building in disruption tolerant networks". In Proc. IEEE INFOCOM, **pp.398– 408, March 2017.**

[11] J. Davis, A. Fagg, and B.N. Levine. "Wearable Computers and Packet Transport Mechanisms in Highly Partitioned Ad hoc Networks". In Proc. IEEE Intl. Symposium on Wearable Computers, **pp.141–148, October 2018.**

[12] J. Yang and C.-K. Lee Y. Chen, M. Ammar. "Ferry Replacement Protocols In Sparse Manet Message Ferrying Systems". In Proc. IEEE Wireless Communications and Networking (WCNC), March **2005**.

[13] W. Zhao and M. Ammar. Message Ferrying: Proactive Routing In Highly-Partitioned Wireless Ad Hoc Networks. In Proc. IEEE Workshop on Future Trends in Distributed Computing Systems, May **2003**.

[14] W. Zhao, M. Ammar, and E. Zegura. A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad hoc Networks. In Proc. ACM Mobihoc, May **2004**.

[15] W. Zhao, M. Ammar, and E. Zegura. Controlling the mobility of multiple data transport ferries in a delay-tolerant network. In IEEE INFOCOM, **2005**.

[16]Yookesh, T. L., et al. "Efficiency of iterative filtering method for solving Volterra fuzzy integral equations with a delay and material investigation." Materials today: Proceedings **47: 6101-6104, 2021.**

[17]Kumar E. Boopathi, and V. Thiagarasu. "Segmentation using Fuzzy Membership Functions: An Approach." IJCSE, **Vol.5, Issue.3, pp.101-105, 2017.**

Authors Profile

Ms. S. Devadharshini received Bachelors Degree in Computer Science in the year 2020 from Bishop heber college, Trichy, Tamil Nadu, affiliated to Bharathidasan University. She is currently pursuing a Masters Degree in Information Technology from 2020 to 2022, at Bharathiar University, Coimbatore, Tamil Nadu.

Dr. R.Vadivel is an Assistant Professor in the Department of Information Technology, Bharathiar University, Tamil Nadu, India. He received his Ph.D. degree in Computer Science from Monomaniam Sundaranar University in the year 2013. M.E., Degree in Computer Science and Engineering from Annamalai University in the year 2007. B.E., Degree in Computer Science and Engineering from Periyar University in the year 2002. He obtained his Diploma in Electronics and Communication Engineering from State Board of Technical Education in the year 1999. He had published over 88 journals papers and over 45 International Journal of Computer Sciences and Engineering Vol.10(5), May 2022, E-ISSN: 2347-2693 © 2022, IJCSE All Rights Reserved 7 conferences papers both at National and International level. His areas of interest include Computer Networks, Network Security, Information Security, etc.

