IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMHTA: A Novel Secured Approach For Fake Packet And Selective Packet Drops Attacks Mitigation By Improved Merkle Tree Approach In Dtns

R. Lalasa
Department of Computer Science & Technology
Madanapalle Institute of Technology & Science
Madanapalle, India

M. Pavan Kumar Reddy
Department of Computer Science & Technology
Madanapalle Institute of Technology & Science
Madanapalle, India

K. Pallavi
Department of Computer Science & Technology
Madanapalle Institute of Technology & Science
Madanapalle, India

T. A. Bharadwaj
Department of Computer Science & Technology
Madanapalle Institute of Technology & Science
Madanapalle, India

***Abstract*—** Delay-Tolerant Networks (DTNs) are decentralized networks that operate without a fixed infrastructure. In DTNs, there is no continuous connection connecting devices, and nodes in the network are often disrupted. DTNs are a practical option for applications that experience sporadic connectivity, significant delays, frequent packet errors, and high rates of packet loss. This project analyses false packet and selective packet drops threats and discusses mitigation strategies for misbehaving nodes. In addition, an Improved Merkle Hash Tree Approach (IMHTA) is proposed to mitigate the malicious node. IMHTA uses a root hash with all packets to identify and counteract both sorts of attacks. A malicious node drops or injects bogus packets, and the algorithm detects it. Trace-driven simulations show that the proposed algorithm improves detection accuracy, packet delivery/loss ratios, and false-positive/false-negative rates compared to previous algorithms that only detect one type of attack or malicious paths rather than specific attacking nodes. Additionally, this work quantitatively analyses numerous circumstances to precisely track DTN vehicular node placements. The proposed technique detects and mitigates false packet and selective packet drops attacks, improving communication network security with intermittent connectivity and large delays.

***Keywords*—** Delay Tolerant Networks; Merkle Hash Tree Approach; Network Security; Misbehaving nodes; Packet Drop attacks; Packet Delivery Ratio

I. INTRODUCTION

Delay-Tolerant Networks (DTNs) are decentralized networks that function without a permanent infrastructure. Within Delay-Tolerant Networks (DTNs), devices lack a persistent connection and network nodes frequently experience disruptions. DTNs are mainly introduced for dealing Interplanetary Networks (IPNs) [1]. Furthermore, it is also applicable in emerging networks such as vehicle Ad-hoc Networks (VANETs), Underwater Sensor Networks (USN), and catastrophe applications. DTNs often employ the Story-Carry-Forward (SCF) strategy to facilitate communication between sensors. This approach involves transmitting information in a hop-by-hop and end-to-end manner [2].

DTNs face numerous challenges including unreliable connections, asymmetrical data rates, long delays, difficulties in time synchronization, bundle reordering, node management, identity spoofing, limited resources, routing issues, bundle security, key management, fragmentation, privacy concerns, and routing misbehavior. Despite substantial research on routing protocols in DTNs, insufficient focus has been given to security concerns in DTNs. It should be noted, however, that packet dropping attacks are not exclusive to DTNs. Prior research has

examined them within the framework of ad hoc networks and wireless sensor networks. Nevertheless, the current packet dropping defense techniques, such as those based on multipath routing, reputation, and data provenance, are ineffective in DTNs due to the absence of end-to-end connections [3].

Within DTNs, nodes are susceptible to a range of assaults including black hole, insider, grey hole, wormhole, Denial of Service (DOS), Distributed Denial of Service (DDOS)/flood, malfunctioning node, and packet drop. In addition to the threats discussed before, the presence of misbehaving nodes poses a significant challenge in DTNs. Nodes that misbehave in a malevolent and selfish manner employ different types of attacks, such as flooding, packet dropping, and false packet attacks, in order to excessively utilise limited network resources. Furthermore, this would result in the unavailability of nodes, a low ratio of packet delivery, and the presence of counterfeit messages in DTNs. Nevertheless, the mitigation strategies commonly used in VANETs, MANETs, WSNs, TCP/IP, and UWSNs cannot be applied in DTNs due to the extended delay and frequent intermittent connectivity. Furthermore, security is a crucial consideration in DTNs for addressing flood and packet drop attacks, with the primary goal of eradicating rogue nodes within the network [4].

The motivation for this work stems from the increasing relevance of DTNs in modern communication systems, particularly in scenarios where traditional infrastructure-based networks are impractical or unavailable. DTNs offer a decentralized approach to communication, enabling connectivity in environments characterized by intermittent connections, significant delays, and high rates of packet loss. However, these unique characteristics also make DTNs susceptible to various security threats, including false packet and selective packet drops, which can significantly impact network performance and reliability.

The primary contributions of this study are:

- A novel form of packet dropping attacks, known as packet collusion attacks, has been discovered in DTNs. In these attacks, hostile nodes intentionally discard certain or all packets and subsequently introduce counterfeit packets to evade detection.
- A robust defense against packet collusion attacks involves normal nodes detecting instances of attacks by analyzing received packets, and subsequently tracing back and identifying the rogue nodes responsible for initiating the attack.
- An Improved Merkle Hash Tree Approach (IMHTA) is proposed to mitigate the malicious node. IMHTA uses a root hash with all packets to identify and counteract both sorts of attacks.
- Further, the proposed technique detects and mitigates false packet and selective packet drops attacks, improving communication network security with intermittent connectivity and large delays.
- To evaluate the performance of the proposed algorithm in Network Simulator (NS-2.34) by considering various evaluation metrics like throughput, packet delivery ratio, end-to-end delay, and network lifetime.

The rest of the paper is structured as follows. Section 2 deliberates the related work and limitations. Section 3 provides the proposed methodology. Section 4 illustrates the experimentation and result Analysis. Finally, the paper concludes with future directions in section 5.

II. Related Works

In the realm of DTNs, various routing protocols have been devised to address the challenges of message delivery in intermittently connected environments. One such protocol is Epidemic, noted for its strategy of flooding messages throughout the network to ensure high delivery ratios. However, this method results in significant message overhead, as each node replicates and disseminates the message widely. In contrast, Spray-and-Wait and Spray-and-Focus protocols limit the number of message replications, thus reducing message overhead while maintaining reasonable delivery ratios. RAPID protocol takes a different approach by replicating data until the destination receives a copy, aiming to ensure reliability. PRoPHET, another standard protocol, makes routing decisions based on probabilistic metrics, optimizing message dissemination [5].

Regarding Quality of Service (QoS) considerations in DTNs, factors beyond routing protocols play pivotal roles. Research indicates that the number of nodes in the network is a crucial factor affecting message delay and connectivity [6]. As the number of nodes increases, connectivity improves, leading to enhanced performance metrics. However, certain challenges persist across various DTN applications, prompting investigations into influential QoS issues specific to routing protocols, movement models, and configuration parameters.

Xie and Zhang [7] introduced a priority-based mechanism to counteract selfish behavior in DTNs. Each node's priority is determined based on its role in relaying messages, and virtual credits are allocated accordingly. However, a drawback is the assumption that nodes reliably maintain their priority records, leaving the network vulnerable to malicious nodes. Malathi and Jayashri [8] proposed an energy-based algorithm to detect selfish nodes. By monitoring nodes' energy levels and buffer capacity using a multi-hop forwarding approach, selfish behavior can be identified and mitigated effectively.

In [9], researchers proposed a scheme utilizing 'HeaderField' to detect misbehaving nodes responsible for SPDA (Security and Privacy Data Aggregation). The 'HeaderField,' also termed 'IndicativeField,' comprises 'IdentificationField,' 'FlagField,' and 'OffsetField.' While efficient, the scheme suffers from high algorithmic costs and elevated false positive/negative rates. Alternatively, in [10], a hybrid reputation-trust scheme addresses SPDA by employing a merkle-hash-tree and reputation metrics (direct and indirect trust calculation). Destination nodes assess bundle counts and hashes; equality suggests benign nodes, while discrepancies indicate misbehavior. However, details on bundle counting and comparison remain unspecified. Drawbacks include high processing costs, absence of centralized nodes, and false positive/negative rates.

Existing literature highlights congestion, selfishness, and fairness as significant QoS issues with tangible impacts on performance metrics in DTNs. Congestion arises when network nodes become overloaded, negatively affecting delivery ratios, packet drop rates, latency, and message overhead [21]. In congested DTNs, messages may fail to reach their destinations or be dropped, exacerbating delivery delays and overhead. Resource scarcity and uncontrolled message replication exacerbate congestion, underscoring the need for effective congestion control mechanisms in DTNs. Additionally, application-specific concerns such as queueing delay and jitter emerge, with interplanetary networking applications prioritizing queueing delay and real-time applications focusing on jitter mitigation [22,23]. These issues collectively influence the performance of DTNs, highlighting the importance of comprehensive QoS

management strategies in such environments. The detailed existing methodologies with its limitations is presented in Table 1.

III. PROPOSED METHOGOLOGY

In the proposed system, a Merkle Hash Tree, often employing SHA512, is created by hashing each packet or bundle, forming leaf nodes. These leaf hashes are then iteratively combined using XOR to generate parent hashes, culminating in a root-hash at the tree's apex. This root-hash serves as the point for validating integrity and authenticity across the network's packets.

This research introduces an enhanced algorithm based on the Merkle-Hash-Tree approach, specifically designed to identify and counteract malicious activities by nodes executing False Packet Attacks (FPA) and selective packet drop attacks (SPDA).

Table 1. Various existing methodologies and its limitations

Ref.	Year	Methodology	Operational Network	Routing Strategy	Neighbor Discovery	Lightweight Imp.	Comm. Reliability	Comm. Cost	Limitations
[11]	2017	DTNSec	Wireless Sensor Networks	Opportunistic	Yes	Yes	High	Low	• Fails to mitigate the malicious node.
[12]	2019	DTN7	Terrestrial/Disaster Networks	Opportunistic	No	No	Medium	High	• Communication cost is high; • Less Reliable
[13]	2019	B-DTN	Terrestrial/Disaster Networks	Opportunistic	No	No	Medium	High	• Fails to determine the neighbor discovery. • Packet drops attack ratio is high
[14]	2020	MSR	Terrestrial/Disaster Networks	Opportunistic/ Scheduled	No	Yes	Medium	Low	• High consumption of computation resources
[15]	2021	Enhanced SABR	Wireless Sensor Networks	Opportunistic	No	Yes	High	Medium	• More Computation Overhead
[16]	2021	RUCoP	Wireless Sensor Networks	Opportunistic	Yes	No	Medium	High	• Increase the overhead • Poor Security issues
[17]	2022	ProgDTN	Terrestrial/Disaster Networks	Opportunistic	Yes	No	Medium	High	• Communication cost is high; • Leads to false packet data transfer
[18]	2022	D3TN	WSN/ Terrestrial/Disaster Networks	Opportunistic	-	Yes	High	Low	• security and data transfer rate are poor
[19]	2022	SPSN	Wireless Sensor Network	Opportunistic	Yes	No	High	High	• High Computational Complexity that limits the scalability in certain situations
[20]	2023	CMR	WSN	Opportunistic	Yes	No	High	Low	• Unimproved message delivery ratio and overhead

In this algorithmic framework, each node initially exchanges public keys with all other nodes, including a trusted authority (TA). Before transmitting packets, each node generates a root-hash covering all packets and includes it alongside the packets. Intermediate forwarding nodes then utilize private key signatures to authenticate packets and adhere to a standardized packet structure. Figure 4.1 illustrates the proposed packet format, optimized for efficient packet transmission. The IMHTA-SHA512 utilizes a Merkle Tree constructed with SHA-512 hashes of individual data packets. Each node in the tree represents a hash value computed from two child nodes, propagating up to the root. This structure facilitates efficient packet integrity verification, as any alteration to a single packet triggers hash value changes throughout the tree. Figure 1 illustrates the working process of various nodes and false packet attack with its trust authority.

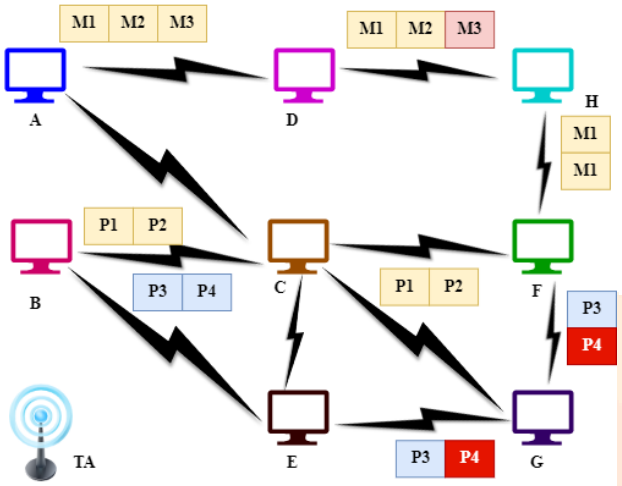

Fig. 1. Attack scenario of malicious nodes

To address false packet injection and selective drops, IMHTA-SHA512 employs a robust verification mechanism. Upon receiving a packet, each DTN node computes its SHA-512 hash and compares it with the corresponding Merkle Tree hash. Discrepancies indicate potential tampering, prompting further action. Additionally, IMHTA-SHA512 enhances security by periodically refreshing and rehashing the Merkle Tree, adapting to network changes and thwarting attacks on the tree's integrity. This proactive approach ensures resilience against evolving threats.

The IMHTA-SHA512 model represents a sophisticated yet practical solution for DTN security. Leveraging SHA-512 robustness and Merkle Tree efficiency, it effectively detects and mitigates attacks, enhancing communication integrity and reliability within DTNs. In this work, three different phases are utilized to determine the proposed model namely network setup phase, forwarder phase and attack detection phase.

Network Setup Phase: The network initializes a Merkle Tree using SHA-512 hashes of individual data packets. The root hash and structure of the Merkle Tree are distributed among network nodes. Nodes establish trust relationships and exchange reputation information to enhance security.

Forwarding phase: Nodes relay data packets through the network using standard routing protocols. Upon receiving a packet, each node computes its SHA-512 hash and compares it with the corresponding Merkle Tree hash to verify packet integrity. Nodes forward packets based on the results of hash verification. Valid packets are forwarded, while suspicious packets trigger further investigation.

Attack detection Phase: Nodes monitor network traffic for anomalies such as unexpected hash mismatches or irregular packet behaviors. Enriched algorithms detect patterns indicative of malicious activities, such as false packet injection or selective drops. Detected anomalies or intrusions prompt nodes to generate alerts, notifying network administrators or initiating automated response mechanisms.

By integrating these phases, the IMHTA-SHA512 model ensures robust security measures throughout the network's operation, from initial setup to ongoing packet forwarding and attack detection.

IV. Experimentation and Result Analysis

A. *Experimental Setup*

To evaluate the effectiveness of our proposed approach, we conducted simulations using the NS-2 simulator, a widely-used tool for network research. The simulation environment incorporated both the MaxProp and First Contact protocols, which are commonly employed DTNs for routing and data dissemination.

B. *Parameter Setting*

The parameter settings, such as simulation duration, update interval, communication technology, and network composition, are meticulously fixed to accurately experiment and evaluate the performance of our proposed model. Table 2 illustrates the proposed model network scenario.

Table 2. Parameter setting of proposed models

Parameter	Values
Simulation Area	1000m*1000m
Simulation Duration	50 seconds
Update Interval	0.5 seconds
Send Range	10 meters
Transmit Speed	1000 kilobits per second
Network Composition	35 operational nodes
Mobility Model	Random waypoint

C. *Performance Metrics*

The Key performance metrics such as packet delivery ratio, packet drop rate, overhead, accuracy of attack detection and energy consumption were measured to evaluate the effectiveness and efficiency of the proposed approach in improving communication reliability and network performance.

D. *Analysis of packet delivery ratio*

Through rigorous experimentation and analysis, it has been observed that IMHTA effectively detects and mitigates security threats, resulting in a higher PDR compared to traditional models. This enhancement in PDR underscores the effectiveness of IMHTA in improving communication reliability and network performance in Delay-Tolerant Networks (DTNs). Figure 2 illustrates the PDR achieved in proposed model compared with existing model.

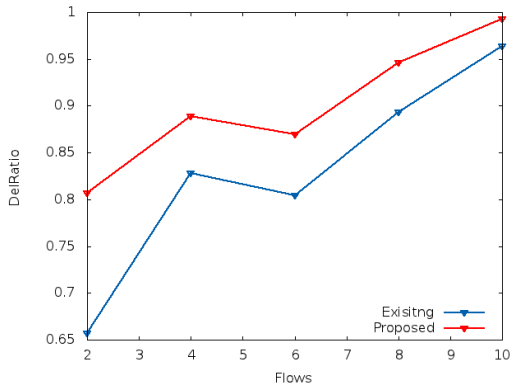

Fig. 2. Packet Delivery Ratio of Proposed vs Existing work

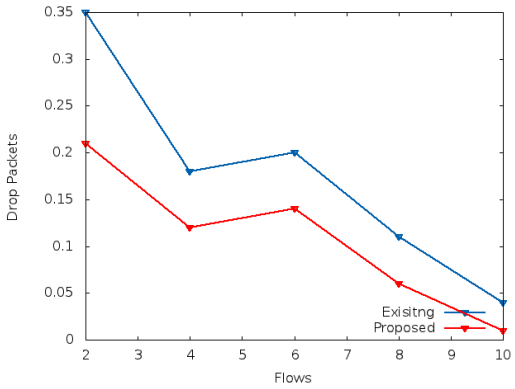

Fig. 3. Number of packets drop in proposed Vs Existing model

E. Analysis of packet drop ratio

The analysis demonstrates a remarkable reduction in packet drop ratio with the Improved Merkle Hash Tree Approach (IMHTA) compared to existing models. IMHTA's effectiveness in minimizing packet drops, validated through meticulous experimentation, underscores its superior performance in ensuring reliable communication within Delay-Tolerant Networks (DTNs). This reduction highlights IMHTA's capability to mitigate security threats and enhance data transmission integrity. Figure 3 provides a visual representation of IMHTA's packet drop ratio compared to existing models.

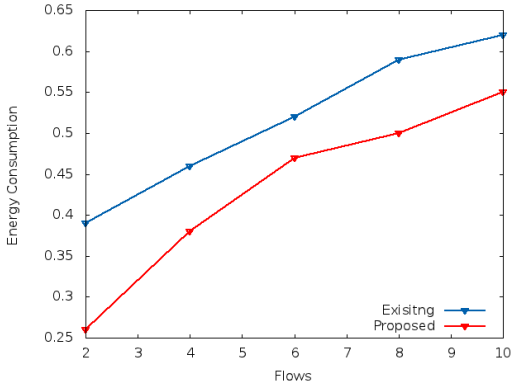

Fig. 4. Energy Consumption in proposed Vs Existing model

F. Analysis of Energy Consumption Ratio

The analysis demonstrates that the Improved Merkle Hash Tree Approach (IMHTA) outperforms existing models in energy consumption. IMHTA shows a significant reduction in energy usage compared to its counterparts, prolonging node lifespan and enhancing network sustainability. These results underscore IMHTA's superiority and potential to address energy-related challenges in DTNs, advancing communication protocols.

G. Analysis of Overhead attained in proposed model

IMHTA optimizes Merkle tree hashing, minimizing computational burden and resource consumption. This efficiency makes IMHTA superior for securing communication in DTNs as shown in Figure 5. It establishes as a premier solution for enhancing network security and reliability.

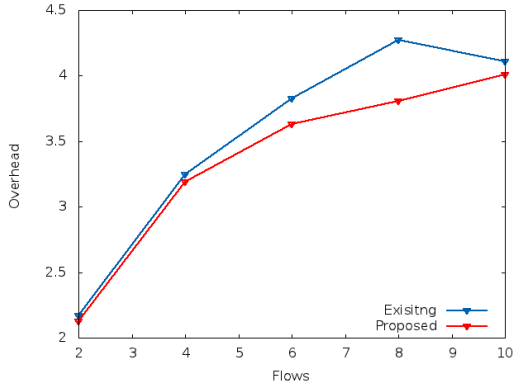

Fig. 5 Overhead in proposed Vs Existing model

H. Analysis of attack detection accuracy

The proposed model significantly improves attack detection accuracy compared to existing approaches, detecting more malicious activities in the network. This heightened accuracy enhances threat identification and strengthens overall network efficacy by swiftly mitigating security risks. By bolstering attack detection capabilities, the proposed model enhances network security, fortifying resilience against malicious actors and ensuring communication integrity. Figure 6 provides a visual comparison of attack detection accuracy between the proposed and existing models.

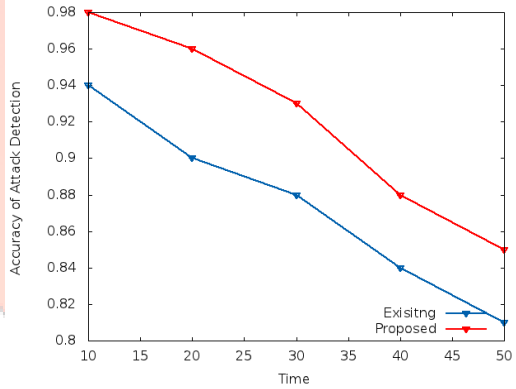

Fig. 6. Accuracy of attack detection in proposed Vs Existing model

V. Conclusion

The security challenges inherent in Delay Tolerant Networks (DTNs) stem from their dynamic topology, lack of centralized management, and susceptibility to packet dropping attacks. This study addresses a specific variant of these attacks by introducing a robust detection and traceback mechanism utilizing Merkle tree hashing. Our approach excels in accurately detecting and identifying malicious nodes, outperforming established methods like Watchdog and Pathrater in simulation scenarios. Moving forward, the integration of such defense mechanisms into secure routing protocols remains a key challenge for enhancing the security of opportunistic networks. The proposed model achieves 8% higher PDR, 10% less drop ratio, 12% higher energy consumption ratio, 15% better accuracy detection rate, respectively. Further, exploring the integration of machine learning and artificial intelligence algorithms for real-time threat detection and adaptive response mechanisms represents a promising avenue for further enhancing the security posture of DTNs in the face of ever-evolving security threats.

REFERENCES

[1] Vasilakos, Athanasios, Yan Zhang, and Thrasyvoulos Spyropoulos. Delay tolerant networks. Boca Raton, FL, USA: CRC press, 2016.

[2] Verma, A., Savita, & Kumar, S. (2021). Routing protocols in delay tolerant networks: Comparative and empirical analysis. Wireless Personal Communications, 118, 551-574.

[3] Chatterjee, Siddhartha, et al. "Dtnma: identifying routing attacks in delay-tolerant network." Cyber Intelligence and Information Retrieval: Proceedings of CIIR 2021. Springer Singapore, 2022.

[4] Sharma, Atul, Nitin Goyal, and Kalpna Guleria. "Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes." The Journal of Supercomputing 77 (2021): 6036-6055.

[5] M. Sommer, J. Hochst, ¨ A. Sterz, A. Penning, B. Freisleben, ProgDTN: Programmable Disruption-Tolerant Networking, in: Networked Systems: 10th International Conference, NETYS 2022, Virtual Event, May 17–19, 2022, Proceedings, Cham, Springer International Publishing, 2022, pp. 184–200.

[6] C. Caini, G.M. De Cola, F. Marchetti, L. Mazzuca, Moderate source routing for DTN space networks, in: 2020 10th Advanced Satellite Multimedia Systems Conference and the 16th Signal Processing for Space Communications Workshop (ASMS/SPSC), IEEE, 2020, pp. 1–7

[7] Xie Y, Zhang Y (2016) A secure, service priority-based incentive scheme for delay tolerant networks. Security and Communication Networks 9(1):5–18.

[8] Malathi M, Jayashri S (2016) Design and performance of dynamic trust management for secure routing protocol. In: 2016 IEEE international conference on advances in computer applications (ICACA), pp 121–124.

[9] A. Ahmad, M. Alajeely, and R. Doss, ‘‘Defense against packet dropping attacks in opportunistic networks,’’ in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Sep. 2014, pp. 1608–1613.

[10] A. Ahmad, M. Alajeely, and R. Doss, ‘‘Reputation based malicious node detection in OppNets,’’ in Proc. 13th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE), Jul. 2016, pp. 1–6.

[11] Obaidat M,Woungang I, Dhurandher S, Koo V. Preventing packet dropping and message tampering attacks on AODV-based mobile ad hoc networks. In: International conference on computer, information and telecommunication systems (CITS). 2012. p. 1–5.

[12] Lee S, Gerla M. Split multipath routing with maximally disjoint paths in ad hoc networks. In: IEEE international conference on communications, vol. 10. 2001. p. 3201–5.

[13] Lu Y,Wong V. An energy-efficient multipath routing protocol for wireless sensor networks. Int J Commun Syst 2007;20(7):747– 66.

[14] Chuah M, Yang P. Impact of selective dropping attacks on network coding performance in DTNs and a potential mitigation scheme. In: Proceedings of the eighteenth international conference on computer communications and networks. 2009. p. 1–6.

[15] Sultana S, Bertino E, Shehab M. A Provenance based mechanism to identify malicious packet dropping adversaries in sensor networks. In: Proceedings of the 2011 thirty first international conference on distributed computing systems workshops. 2011. p. 332–8.

[16] Zhang X,Wu S, Fu Z,Wu T. Malicious packet dropping: how it might impact the TCP performance and how we can detect it. In: Proceedings of the 2000 IEEE international conference on network protocols. 2000. p. 263–72.

[17] Marti S, Giuli T, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the sixth annual international conference on mobile computing and networking. 2000. p. 255–65.

[18] Nasser N, Chen Y. Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. In: IEEE international conference on communications. 2007. p. 1154–9.

[19] D. Schürmann, G. von Zengen, M. Priedigkeit, L. Wolf, µDTNSec: a security layer for disruption-tolerant networks on microcontrollers, in: 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), IEEE, 2017, pp. 1–7

[20] A. Penning, L. Baumgartner, ¨ J. Hochst, ¨ A. Sterz, M. Mezini, B. Freisleben, Dtn7: An open-source disruption-tolerant networking implementation of bundle protocol 7, in: Ad-Hoc, Mobile, and Wireless Networks: 18th International Conference on Ad-Hoc Networks and Wireless, ADHOC-NOW 2019, Luxembourg, Luxembourg, October 1–3, 2019, Proceedings 18, Springer International Publishing, 2019, pp. 196–209.

[21] L. Baumg¨ artner, J. Hochst, ¨ T. Meuser, B-dtn7: Browser-based disruption-tolerant networking via bundle protocol 7, in: 2019 International Conference on Information and Communication Technologies for Disaster Management (ICTDM), IEEE, 2019, pp. 1–8.

[22] F.D. Raverta, J.A. Fraire, P.G. Madoery, R.A. Demasi, J.M. Finochietto, P. R D’argenio, Routing in Delay-Tolerant Networks under uncertain contact plans, Ad Hoc Networks 123 (2021), 102663.

[23] Z. Ghafouri-ghomi, M.H. Rezvani, an optimized message routing approach inspired by the landlord-peasants game in disruption-tolerant networks, Ad Hoc Networks 127 (2022), 102781.