International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume 12, Issue 5, September-October 2023

Secure Group Communication in Delay Tolerant Mobile Ad-Hoc Network

Prachi Tiwari
Computer Science and Engineering Department
Radharaman Institute of Technology and Science, Bhopal, M.P, India
prachi.38@gmail.com

Abstract— *Delay-tolerant networks (DTNs) are well-known for delivering various types of information from different senders in a multicast manner, both in centralised and decentralised networks. Wireless mobile nodes form small networks in which one or more senders transmit data to one or more destinations through intermediate nodes. DTN routing protocols differ from traditional wireless routing protocols. There are security threats in DTNs, such as blackhole attackers dropping data, jamming attacks consuming bandwidth, and Vampire attacks depleting battery power and available bandwidth. This paper proposes a prevention scheme to detect and mitigate all three types of attackers in multicast communication. These attackers can impact performance by generating false replies, flooding with redundant information, and wasting communication power. The primary focus of this paper is on security issues related to DTN routing protocols. In order to counter malicious nodes, a blacklist is maintained, and if a neighbour identifies a node as malicious, it excludes packets from that node. Meanwhile, the neighbour continues sending packets to the malicious node, except for broadcast packets, which are dropped. If a node is found to forward no packets or only some packets by all its neighbours, any reply it gives to route requests is disregarded, and any request it initiates is ignored. Successful data reception at the destination indicates that hop-based data delivery maintains a record of successful transmissions. The proposed security scheme demonstrates improved performance.*

Keywords:- DTN, Blackhole, Jamming, Vampire, Multicasting, Routing.

I. INTRODUCTION

Delay-Tolerant Networks (DTNs) represent a network class that does not assume a well-defined path between two nodes wishing to communicate. In particular, source and destination systems may never be connected to the network simultaneously, and connections among wireless nodes are temporary. Such networks may have sparse node densities, with limited communication capabilities for each node. One-hop connections are often disrupted due to node mobility, energy conservation, or interference. However, these networks can still establish a link when two nodes come into each other's coverage range. The DTN concept suggests that these temporary links can be used to exchange information on behalf of other nodes, hoping it will eventually reach the destination. Although this communication paradigm typically involves overhead regarding additional delay since packets are often buffered in the network, it appears to be the only viable solution for such specific environments.

The existing TCP/IP-based Internet operates under the assumption of end-to-end communication using a combination of various data-link layer technologies. The rules specifying how IP packets are mapped into network-specific data-link layer frames at each router provide the necessary level of interoperability. However, the IP protocol makes several key assumptions about lower-layer technologies, ensuring seamless IP layer communications. These assumptions include: (i) there is an end-to-end path between two communicating end systems, (ii) the round-trip time between communicating end systems is not excessively high, and (iii) the end-to-end packet loss probability is relatively low. Unfortunately, one or more of the assumptions mentioned earlier are violated in DTN networks due to mobility, power conservation schedules, or a high bit error rate [11].

A significant challenge in achieving end-to-end communication in DTN topology is that IP packet delivery relies on the existence of an uninterrupted end-to-end path. In practice, according to classic IP routing mechanisms, an IP packet is dropped at an intermediate system where no link to the next hop currently exists. This design restricts end-to-end communication to scenarios where intermediate nodes must buffer received packets to deliver them whenever they have an opportunity to contact their destinations [12].

II. OVERVIEW OF DTN CHARACTERISTICS

To discuss the routing problem, we need a model that captures the most important characteristics of a DTN network. This section explores these characteristics, focusing on those that have the most significant impact on the implementation of routing and forwarding protocols, such as path properties, network architectures, and end-node resource constraints.

Intermittent connection: One of the most crucial characteristics of DTNs is that the end-to-end connection between communicating end systems may not always be available. Generally, intermittent connections can be broadly categorised as either fault-related or non-fault-related. Non-faulty disconnections occur in wireless environments and are primarily caused by mobility and the short duty cycle of system operation. The intermittence of connections due to mobility depends on the application area of DTNs. Communication schedules can be established based on predictability or can be entirely opportunistic. In the latter case, nodes come into the coverage area of each other due to their random movement or the movement of other objects [13,14]. Figure 1 demonstrates the predictability of communication schedules for mobile nodes in different scenarios. Figure 1: The range of predictability for communication schedules in intermittent connections caused by short duty cycles is common among devices with limited resources (e.g., sensor networks). These connections are often predictable. Dealing with disconnections requires the routing protocol to understand that the lack of connectivity between nodes occurs due to normal situations rather than force majeure, and it should not be considered an outage due to faulty operation [14, 15].

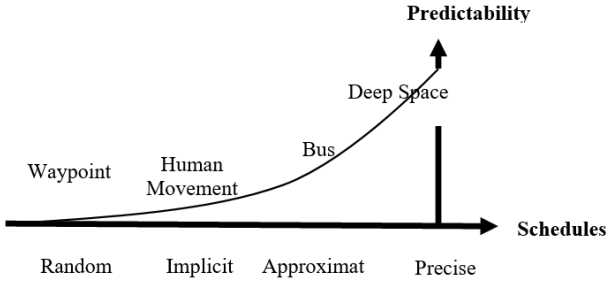

Figure 1 Predictability of communication schedules for mobile nodes

Delivery latency and low data rate: Delivery latency refers to the amount of time between message injection into the network and its successful reception at the destination. Many applications benefit from short delivery times, making latency one of the most important performance metrics. This delay includes transmission time, processing time, propagation time over all links, and queuing delay at each system along the path. In DTNs, transmission rates are often relatively small, and latencies can be large. Data transmission rates vary significantly between uplinks and downlinks [11]. In some application scenarios (e.g., deep-space communications), delivery latency may range from a few minutes to hours or even days, with a significant fraction of messages possibly not being delivered at all. Effective operation in DTNs with high latencies and low link rates requires designing routing protocols and forwarding algorithms that match the actual mobility patterns [16, 13].

Long queuing delay: Queuing delay is the time it takes to clear the queue of messages ahead of the tagged one. The queuing delay depends on the data rate and the amount of competing traffic traversing the network. In DTNs, where a disconnected end-to-end path is common, the queuing time can be extremely long, ranging from minutes to hours or even days.

Resource limitation: Nodes in DTNs often have very limited energy sources, either because they are inherently mobile or because the power grid is non-existent in their location. End systems consume energy by sending, receiving, storing messages, and performing route discovery and computation. Therefore, routing strategies that send fewer bytes and require fewer computation operations are often more energy-efficient [14]. In some application scenarios (e.g., wireless sensor networks), nodes are characterised by limited memory and processing capability [17].

Limited longevity: In some DTNs, end nodes may be deployed in hostile environments, especially in sensor networks, military applications of DTNs, and networks of devices used by emergency personnel [14]. In such cases, network nodes may break down and are not expected to last long. Considering that the end-to-end path between two communicating entities may not exist for a long period, there could be cases where the delay in message delivery exceeds the lifetime of a transmitter node.

Security: DTNs are vulnerable to many malicious actions and pose several new security challenges. Using intermediate nodes as relays provides opportunities for security attacks, including compromising information integrity, authenticity, user privacy, and system performance. Using specific routing mechanisms, including flooding-based ones, may increase the risks of inserting false information into the network. The extra traffic injected by malicious nodes creates another serious threat due to resource scarcity in some application scenarios. Unauthorised access and utilisation of DTN resources for specific malicious actions are also significant concerns. It's important to note that research on DTN security is more challenging compared to conventional mobile ad hoc networks due to its unique security characteristics, including exceptionally long delivery delays, sporadic connectivity, and opportunistic routing, which make most existing security protocols designed for conventional ad hoc networks unsuitable for DTNs [18, 15].

III. LITERATURE SURVEY

In this section, we present various proposals from the literature aimed at improving routing performance in spontaneous Mobile Adhoc Networks (MANETs). Lobiyal Savita et al .[1] address the issue of high delay in Delay Tolerant Networks (DTNs), often caused by the lack of a complete path from source to destination. The primary challenge in DTNs is to establish end-to-end communication in a heterogeneous environment with severe performance limitations. The DTN routing problem is treated as a constrained optimisation problem, considering that edges may be unavailable for extended periods and storage constraints exist at each node. The proposed protocol aims to minimise energy consumption by reducing various overheads. It calculates delivery probability through each of its neighbours and delivers message copies accordingly. Yun Won Chung et al. [2] focus on enhancing the dissemination speed of the PRoPHET (probability routing protocol using history of encounters and transitivity) protocol by incorporating the epidemic protocol for disseminating messages when forwarding counter and hop counter values are below or equal to specified threshold values. The performance of the proposed protocol is analysed in terms of delivery probability, average delay, and overhead ratio. Numerical results demonstrate that the proposed protocol can enhance the delivery probability, average delay, and overhead ratio of the PRoPHET Protocol by appropriately selecting the threshold forwarding counter and threshold hop counter values. Chenqian Zhou et al. [3] introduce a new routing protocol named Scheduling-Probabilistic Routing Protocol using the History of Encounters and Transitivity (PROPHET). The protocol calculates delivery predictability based on the encountering frequency among nodes and incorporates two scheduling mechanisms to enhance traditional PROPHET protocol performance, both in terms of storage and transmission within DTNs. Simulations are conducted to evaluate the proposed

routing protocol, comparing it with other routing protocols using the Opportunistic Network Environment (ONE) simulator. Ratneshwer Gupta et al.[4] focus on Delay Tolerant Networks (DTNs) and address their architectural, routing, congestion, and security aspects. Opportunistic networks, which must tolerate delays, are a fundamental component of DTNs, utilising a "store-carry-forward" approach for data packets. DTNs find applications in various scenarios, including providing cost-effective internet access in remote areas, vehicular networks, noise monitoring, and extreme terrestrial environments. The study explores the potential for integrating opportunistic network methodologies and technologies into DTNs, making it a promising area for further investigation. Asri Ngadi, Qaisar Ayub, et al. [5] propose a Priority Queue-Based Reactive Buffer Management Policy (PQB-R) for Delay Tolerant Networks (DTN) under city-based environments. The PQB-R classifies buffered messages into source, relay, and destination queues, applying a separate drop metric to each queue. This approach, known as reactive drop, addresses buffer overflows by selectively dropping messages. In contrast to existing reactive buffer management policies that use a single metric for source, relay, and destination messages, PQB-R recognises that each message type may consume different network resources. Additionally, the authors introduce the concept of time-to-live (TTL) parameters in DTN, which defines the lifetime of a message. However, ttl does not apply to messages that have reached their destinations, leading to unnecessary message replication until ttl expires. Mario Gerla Tuan Le et al. [6] explore a contact duration-aware (CDA) routing strategy focused on single-copy message forwarding. Two critical questions are addressed: (1) the selection of the next-hop relay node and (2) the order of message forwarding. Relay nodes are chosen from current and past contacts to reduce transmission costs based on one-hop and two-hop delivery probabilities, respectively. These probabilities are derived from the contact duration and inter-contact times distribution. Message scheduling prioritises messages with the highest delivery probabilities for transmission. Gaochao Xu, Xiangyu Meng, et al. [7] introduce a more accurate and comprehensive metric for evaluating the quality of relationships between nodes in social Delay-Tolerant Networks (DTNs), considering contact time, contact frequency, and contact regularity. An overlapping hierarchical community detection method is proposed based on this metric, leading to the creation of a tree structure. The overlapping community and tree structures are leveraged to establish message-forwarding paths from source to destination nodes. Kyung Min Baek et al. [8] enhanced opportunistic routing protocol, utilising context information related to the average distance travelled and average time elapsed from message reception to delivery at the destination node. The protocol updates these averages whenever a message is successfully delivered. The average distance, average time, and delivery predictability are employed to make decisions regarding message forwarding. The performance of this protocol is evaluated and compared to the PRoPHET and reachable probability centrality (RPC) protocols, which use contact history information of mobile nodes. El Arbi Abdellaoui Alaoui et al. [9] present a DTN protocol for Internet of Things (IoT) applications. While IoT technologies demand new communication systems like delay-tolerant networks, ensuring that data exchange is effective and understandable by receiving entities is equally important. Despite numerous DTN routing protocols being proposed, the emergence of new technological applications such as drones and IoT necessitates the development of feasible, reliable, and robust protocols tailored to these new applications. R. Amirthavalli et al. [10] provide a survey of machine learning (ML) techniques used in Delay Tolerant Networks (DTNs). It is one of the first surveys to examine ML techniques in DTNs. DTNs are characterised by intermittent connectivity, long delays in packet delivery, and sparse node distribution. They find applications in scenarios like underwater communication, interplanetary communication,

disaster management, and wildlife tracking. DTNs are highly affected by environmental changes, making adaptability crucial. ML techniques enhance network lifetime, facilitate routing by adapting to network changes, mitigate congestion, and reduce overhead.

IV. PROPOSED WORK

Delay Tolerant Networks (DTNs) provide group communication using a bundle-based data forwarding method to enhance network efficiency. However, when DTNs are adopted within a Mobile Ad Hoc Network (MANET), network maintenance becomes necessary due to MANET's limitations. Therefore, dynamic routing is often adopted to improve service quality. Another significant challenge in MANET communication is security since nodes frequently change their locations, making it challenging to determine their trustworthiness. The proposed trusted technique offers cross-layer security to enhance network security during communication. In our simulation, three types of attack behaviours are simulated: blackhole, vampire, and jamming attacks. In the first step, all three attacks are detected, and in the second step, the proposed trusted method prevents all three attacks, thereby enhancing network security. The proposed collaborative trust method operates in two layers: vampire and jamming attacks are data link layer attacks as they consume network resources and interfere with the data link layer's channels.

In contrast, the blackhole attack is a network layer attack, generating higher sequence numbers and spoofing the source node during route formation, allowing it to intercept data from the source node. The proposed collaborative trust method identifies attacks through the start-up and data transmission phases. The initial node trust level is set to zero in the start-up phase, and a sample data transmission process begins. Over time, the trust value is updated based on behaviours such as the percentage of successful data forwarding, data drops, network resource utilisation, and route table modifications. At the end of the start-up phase, the behaviour of all nodes is analysed, and nodes are categorised as trusted (if their trust value is greater than 0.5 or their behaviour is normal) or non-trusted (if their trust value is less than 0.5 or their behaviour is abnormal). Trusted nodes are assigned to collaboratively prevent attacks, while non-trusted nodes are further divided into three categories: vampire, jamming attack, and blackhole attack. The collaborative decision-making system initially blocks these attacker nodes, and their characteristics are stored in the trusted node table to detect new attacker nodes. In the data transmission phase, actual communication occurs, and during this time, sender nodes initiate data transmission towards their destinations through intermediate trusted mobile nodes. Node trust is continuously calculated during every event occurrence (send, forward, receive, and drop) by neighbouring trusted nodes. Collaboratively, the average trust calculation helps make fair decisions about node trust. If a node's trust value continually decreases and falls between 0 and 0.5, neighbouring trusted nodes block the identified node and provide an alternative route without disrupting communication. This scheme prevents the network and data from being compromised by attacker infections. Additionally, when a new node joins the network, its behaviour is assessed through analysis by neighbouring trusted nodes (based on abnormal and normal behaviour), ensuring the network is more secure against known attacks such as vampire, jamming, and blackhole attacks.

V. PROPOSED FLOW ARCHITECTURE

In the collaborative trust-based system, the first step involves initialising all mobile nodes and configuring both the routing protocol and the DTN technique, which enables bundle-based group communication. After this initial setup, the collaborative trust system is executed to calculate trust values and identify attack types. The trusted system subsequently blocks These detected attack types when their trust value falls below 0.5. On the other hand, nodes with trust values equal to or greater than 0.5 are designated as trusted nodes and actively participate in identifying

new attacker nodes within the network. The proposed flow diagram illustrates how secure and reliable group communication is established in a mobile ad hoc environment.

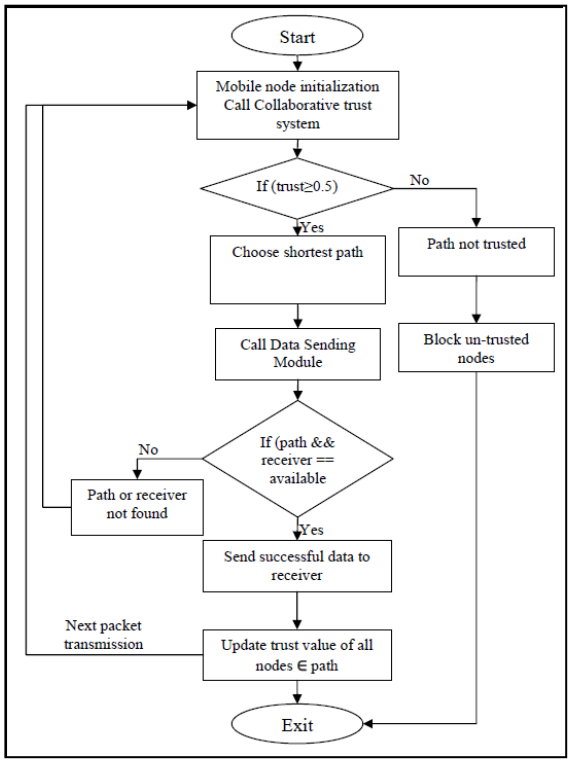

Figure 2 Collaborative trust-based security system

VI. SIMULATION OVERVIEW AND PARAMETERS

The simulation used the freeware software network simulator-2 [19], specifically version NS 2.31 on the Cygwin platform. Using the simulator, various scenarios of mobile ad hoc networks were generated and integrated with our proposed security technique. The performance of the collaborative trust system was then assessed and compared based on attack behaviour and its corresponding impact.

A. Simulation Parameter

Multicast communication is efficient when receivers receive the same messages. However, delivering different messages to various senders in DTN is possible. The simulations for both routing schemes are based on the simulation parameters listed in Table 1.

Table 1 Performance Parameters

Parameters	Value
Number of nodes	50
Dimension of the simulated	800×800
Routing Protocol	AODV
Network Type	DTN
Simulation time (seconds)	100
Transport Layer	TCP, UDP
Attack Type	Blackhole, Jamming,
Prevention Type	Collaborative Neighbor
Traffic type	CBR, FTP
Packet size (bytes)	512
Antenna Type	Omni Antenna
Node Speed (m/s)	Random

VII. RESULTS EVALUATION

The simulation results are evaluated using the considered parameters, and the proposed scheme is applied to modify the routing and channel access. The description of performance metrics is provided below:

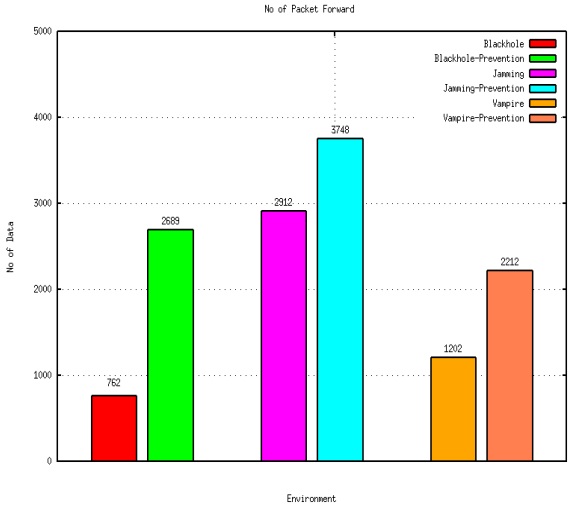

Figure 3 correlates with Table 2, which displays the packets forwarded by intermediate nodes.

A. Packet Forward Analysis

The number of data packets forwarded to the destination reflects network performance. In this

context, the number of nodes establishes dynamic connections, which are not secure due to malicious nodes that drop data from senders. As a result, senders face challenges in delivering data to destinations, mainly due to Blackhole, Jamming, and Vampire attacks. The graph represents the performance of data reception in the presence of these attackers and the effectiveness of the proposed prevention schemes. Notably, the proposed scheme exhibits the highest data forwarding performance in the network, attributed to its efficient routing approach.

Table 2: Analysis of No of Packet Forward

Description	Total Packets Forward
Black hole	762
Prevention-Black hole	2689
Jamming	2912
Prevention-Jamming	3748
Vampire	1202
Prevention-Vampire	2212

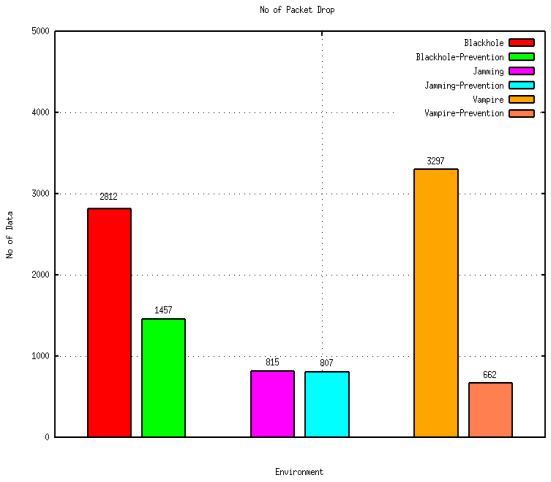

Figure 4: Packet Drop Analysis

B. Packet Drop Analysis

Multicasting is designed for group-oriented computing, and it finds applications in scenarios where one-to-many or many-to-many dissemination of information is crucial. In the context of DTN networks, each node along the route detects whether its link to the next hop has been disrupted when transmitting packets to the next hop. Data drop issues in DTN networks often stem from the mobility of mobile nodes and are addressed by mitigating the malicious activities of attackers. The graph illustrates the performance of data drop in the presence of Blackhole attacks, Jamming attacks, Vampire attacks, and the proposed prevention scheme protocol for DTN networks. In Table 3, the number of packet drops was calculated for all scenarios, and it was observed that the data drop is minimised when the collaborative trust system for security is applied.

Table 3: Analysis of Total Packet Drop

Description	Total Packets Drop
Blackhole	2812
Prevention-Blackhole	1457
Jamming	815
Prevention-Jamming	807
Vampire	3297
Prevention-Vampire	662

C. Average Hop Count Analysis

A higher hop count in the network increases the likelihood of longer routes and the potential for routing loops. In this graph, the hop counts are examined in a dynamic environment, and it is observed that the proposed reliable security scheme delivers better results than the performance of Blackhole attacks, Jamming attacks, and Vampire attacks. The highest hop count is only observed in Jamming attacks. The primary objective of the proposed approach is to reduce the hop count after applying the proposed security scheme in DTN.

Table 4: Average Hop Count Analysis

Description	Average Hop Count
Black hole	7
Prevention Black hole	13
Jamming	113
Prevention Jamming	8
Vampire	31
Prevention-Vampire	5

In the proposed scheme, efficient routing significantly improves performance by enhancing packet reception and reducing packet loss. Table 4 displays the average hop count in all cases, including Vampire, Blackhole,

and Jamming attacks, and their respective protection measures. The results show that the protection mechanisms reduce the number of required hop counts, ultimately improving network efficiency.

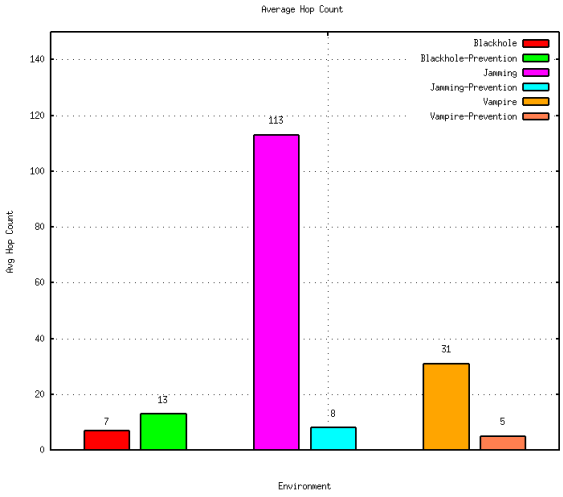

Figure 5: Average Hop Count

D. Throughput Analysis

In a mobile network, every node can be considered a multicast router, and these nodes are logically connected to each other, either directly or indirectly. These mobile routers manage group membership and collaborate to route data to all hosts interested in participating in a multicast group. The proposed protocol for group communication relies on specific bundle-based communication between the sender and receiver.

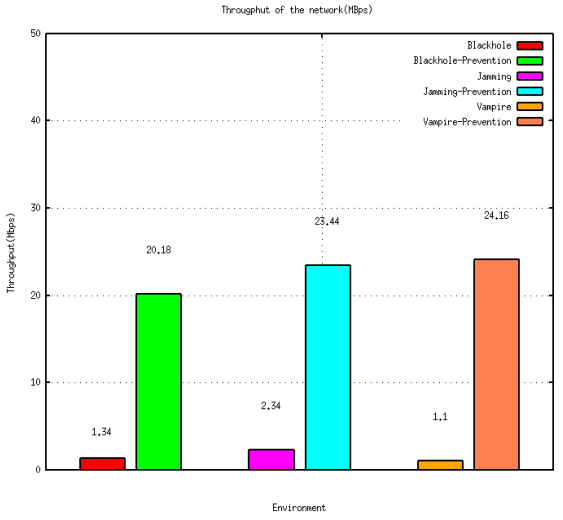

Figure 6: Throughput Analysis

The throughput performance of the proposed prevention scheme in the DTN network is significantly superior. In this scheme, the throughput exceeds 20 Mbps, while in the case of an attack, it only reaches approximately 2.4 Mbps in the network. This represents an improvement ratio of about 90% when employing the prevention measures against attacks. The specific figures are provided in the table provided.

Table 5: Analysis of Throughput [Mbps]

Description	Throughput (Mbps)
Black hole	1.34
Prevention-Black hole	20.18
Jamming	2.34
Prevention-Jamming	23.44
Vampire	1.1
Prevention-Vampire	24.16

VIII. CONCLUSION

In multicast communication, the actions of attackers can adversely affect multiple nodes within the network. Even a single attacker can severely disrupt normal multicast communication. Blackhole attacks, Jamming attacks, and Vampire attacks are particularly harmful, each exhibiting distinct behaviour patterns. In Delay Tolerant Networks (DTNs), where nodes communicate without relying on a central base station, they are vulnerable to attacks within an open communication environment. The dynamic nature of the network makes it challenging to confirm and capture attackers. Routing protocols are vital in efficiently transmitting information from a specific source to the destination. However, attackers, such as those executing Blackhole, Jamming, and Vampire attacks, engage in malicious activities that undermine network integrity. Various authors have proposed numerous security techniques to secure communication within DTNs, either between senders and receivers or between senders and base stations at different network layers. These techniques highlight the susceptibility of dynamic, wireless, and infrastructure-less networks to

various attacks. DTNs can be categorised as mobile or static, and attackers pose a significant threat to both types. Attackers aim to disrupt or drop user data transmitted by senders. The proposed prevention scheme effectively reduces data drops and outperforms Blackhole, Jamming, and Vampire attacks. These attackers attempt to disrupt the network's normal operation by isolating crucial nodes. However, the proposed security scheme excels in identifying attacker profiles. Network throughput is significantly enhanced, achieving approximately 90% improvement compared to previous attacks in DTNs. The performance analysis of attackers reveals degradation and increased overhead, but the proposed prevention scheme alleviates the burden by selecting attacker-free communication paths. Attackers are particularly detrimental in decentralised networks compared to centralised ones. Additionally, Jellyfish attacks represent another harmful passive attack with distinct behaviour. In the future, enhancing the security scheme to protect against Jellyfish attacks in DTNs is essential.

REFERENCES

[1]. Savita, Prof. D.K. Lobiyal, "Location Information and Inter-Contact based Routing approach for Delay Tolerant Networks" Elsevier Procedia Computer Science 57 (2015) 1367 – 1375.

[2]. Seung Deok Han and Yun Won Chung "An Improved PRoPHET Routing Protocol in Delay Tolerant Network" Hindawi Publishing Corporation Scientific World Journal Volume 2015.

[3]. Yuxin Mao, Chenqian Zhou, Yun Ling, et al. "An Optimised Probabilistic Delay Tolerant Network (DTN) Routing Protocol Based on Scheduling Mechanism for Internet of Things (IoT)" Sensors (Basel). 19(2): 243. 2019 Jan;

[4]. Vandana Kushwaha, Ratneshwer Gupta, "Delay Tolerant Networks Architecture, Routing, Congestion, and Security Issues" Research gate April 06 2019.

[5]. Qaisar Ayub, Asri Ngadi, Sulma Rashid, et al."Priority Queue Based Reactive Buffer Management Policy for Delay Tolerant Network under City Based Environments" Research Article. February 13, 2018.

[6]. Tuan Le, Mario Gerla, "Contact Duration-Aware Routing in Delay Tolerant Networks" 2017 IEEE.

[7]. Xiangyu Meng, Gaochao Xu, Tingting Guo, et al." A Novel Routing Method for Social Delay-Tolerant Networks" Volume 24, Number 1, February 2019.

[8]. Kyung Min Baek , Dong Yeong Seo,et. al." An Improved Opportunistic Routing Protocol Based on Context Information of Mobile Nodes" August 08 2018; Published: August 10 2018.

[9]. El Arbi ABDELLAOUI ALAOUI et al. "DTN Routing Hierarchical Topology for the Internet of Things" Elsevier Computer Science pp. 490–497 (2020).

[10]. R. Amirthavalli, S. Thanga Ramya [10] "Machine Learning in Delay Tolerant Networks: Algorithms, Strategies, and Applications" (IJITEE) Volume-9 Issue-1S, November 2019.

[11]. Kevin Fall. "A Delay-Tolerant Network Architecture for Challenged Internets," February 2003.

[12]. David (Bong Jun) Choi BBCR Lab., "A Tutorial y Challenges and Applications of Delay Tolerant Networks," ECE, University of Waterloo,

[13]. Evan P. C. Jones, Lily Li, Jakub K. Schmidtke, Paul A. S. Ward, "Practical Routing in Delay-Tolerant Networks," in IEEE Trans. Mob. Comput. , 2007.

[14]. J. Shen, S. Moh, and I. Chung, "Routing Protocols in Delay Tolerant. Networks: A Comparative Survey", 23rd International Conference on Circuits/system, Computer and Communication (ITC-CSCC 2008), Aug 2007.

[15]. L. Pelusi, A.Passarella, and M.Conti, "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks," IEEE Commun. Mag., 2006.

[16]. Haris, Abdullah, "A DTN study analysis of implementations and tools," Master`s Thesis, TKK / Informaatio- ja luonnontieteiden tiedekunta, 2010.

[17]. Evan P.C. Jones and Paul A.S. Ward, "Routing Strategies for Delay-Tolerant Networks", 2006.

[18]. Haojin Zhu," Security in Delay Tolerant Networks," Doctor of Philosophy Thesis, Electrical and Computer Engineering Waterloo, Ontario, Canada, 2009.

[19]. Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns