Phoenix: International Multidisciplinary Research Journal
Vol 3, No. 4, Oct-Dec, 2025
ISSN:2583-6897

A COMPREHENSIVE REVIEW AND ANALYSIS OF SECURITY ISSUES ON ROUTING PROTOCOLS IN DELAY TOLERANT NETWORKS

B.Rani
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: rani@mrec.ac.in
Vemula Nikitha
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: nikitha479@gmail.com
Dikshendra Daulat Sarpate
Professor, Department of Artificial Intelligence & Data Science, ZEAL College of Engineering & Research, Pune, Email id -dikshendra@gmail.com
B. Sankaraiah
Assistant Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: Shankar61186@gmail.com
Dr. Syed Umar
Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad. Email id.: syedumar@mrec.ac.in

Abstract— In contexts that are characterized by excessive latency and intermittent connectivity, such as interplanetary communication or isolated terrestrial locations, Delay Tolerant Networks (DTNs) are utilized. These networks are designed specifically for usage in these environments. Within the scope of this article, the architectural principles of DTNs are investigated, with a particular focus on the operational contrasts between DTNs and regular Internet protocols. In addition to this, it investigates the ways in which the bundle protocol enables robust communication in spite of disturbances. A comprehensive analysis of their application situations, implementation methodologies, and the most current advancements made in this field is included in the paper. A particular emphasis is placed on the issues that actual deployments present, as well as the ways in which changing architectures might fulfill these requirements.

The Delay Tolerant Network, often known as DTN, is an essential component of today's communications system. DTNs are utilized in a wide range of scenarios, including but not limited to armed conflicts, earthquakes, volcanic eruptions, and terrorist strikes, amongst others. The Distributed Transmission Network (DTN) offers a setting in which two nodes can only communicate with one another when they are within transmission range of one another. This is because the network contains intermittent connectivity. When it comes to these kinds of networks, the most significant challenge is security. In this work, we have explored a variety of DTN routing protocols and their variants, in addition to the various security aspects that require attention.

Index Terms— Delay tolerant networks, DTNs, anonymous routing, DTN Architecture, Interplanetary Internet, etc

INTRODUCTION

DTN is employed in a variety of events, including traffic management systems, wild life tracking systems, terrorist attacks, military wars, earthquakes, storms, floods, hurricanes, and violent volcanic eruptions, among others. Unnecessary delays, severe bandwidth limits, significant node mobility, frequent power outages, and frequent communication issues occur from these demanding situations. As a result, wireless network connectivity becomes significantly erratic under such conditions, and it is no longer possible to guarantee that each source-destination pair will have simultaneous end-to-end connections. As a result, numerous researchers are working in this field and considering these challenges [1].

Delay-Tolerant Networks, also known as DTNs, are a useful solution for networks that are characterized by high latency, inconsistent connectivity, and frequent disruptions.

For these issues, which are frequently encountered in locations that are mobile or remote, customized network protocols and architectures are required. These protocols and architectures must be able to function successfully even in situations when regular networks are unable to function. In response to the limits of traditional networking protocols, which are dependent on continuous end-to-end connectivity, the notion of distributed transmission networks (DTNs) came into being. Data transmission networks (DTNs) offer a viable communication option for situations that are both dynamic and disrupted. This is accomplished through the utilization of the store-and-forward technique, in which data is temporarily saved and then transferred when a suitable path becomes available [2].

Early contributions from key platforms such as the Delay-Tolerant Networking Research Group (DTNRG) and the Internet Protocol for Intermittent Connectivity (IPNSIG) were instrumental in providing the groundwork for strong DTN architectures. These contributions were instrumental in laying the framework for their development. The DTNRG, which was initially launched as a research program by the Internet Research Task Force (IRTF), made a substantial contribution to the creation of essential protocols and architectural frameworks for DTNs. In their study, they concentrated on finding solutions to the problems that are connected with intermittent connectivity. They wanted to make sure that messages could be effectively delivered even in situations that had unpredictable topologies and significant delays. By introducing the idea of bundle protocols, DTNRG was able to offer a framework for the storing, forwarding, and delivery of data packets within a DTN. This framework ensured reliability even in circumstances where network access was extremely poor.

In a similar vein, IPNSIG, which was another early contributor to DTN research, concentrated on establishing network protocols and tactics that may enable reliable communication in situations with intermittent connectivity. The creation of mechanisms to handle routing in DTNs, such as store-carry-forward protocols, which are protocols in which data is kept at intermediate nodes and then forwarded when a valid connection is created, was one of their most significant contributions. Taking this technique was essential in order to enable data to travel via networks that had intermittent connectivity, which ensured that messages could still be properly delivered over the course of additional time [3]. Additionally, the study done by IPNSIG highlighted the need of utilizing mobility and social patterns to forecast the movement of nodes, which could subsequently be utilized for the purpose of achieving efficient routing and message delivery results.

With the maturation of DTNs came the emergence of actual applications, which demonstrated the real-world potential of these networks to handle communication difficulties in situations that are either isolated or mobile. It is important to note that ZebraNet, a project that established the viability of DTNs in the field of wildlife tracking and monitoring, was one of noteworthy applications. The principles of DTN were utilized by ZebraNet in order to facilitate communication between mobile nodes (such as animals, which are equipped with GPS trackers) and remote base stations. Even though they were continuously moving and frequently out of direct communication range with base stations, the animals were nevertheless able to transmit data when they came into close proximity with other animals or base stations [4]. Even in situations with little to no network infrastructure, where conventional wireless communication methods would fail owing to frequent disruptions or significant delays, this unique application proved how DTNs could be used to collect and send data in wildlife monitoring. This was accomplished by demonstrating how DTNs could be used to collect and transmit data.

The accomplishments of ZebraNet represented a significant stage in the process of demonstrating the usefulness of DTNs in real-world situations. During the course of the project, the benefits of utilizing store-and-forward techniques were brought to light. These approaches include temporarily storing data at intermediate nodes and then forwarding it when the conditions of the network permit it. Because of this, it was possible to transfer data effectively in situations when conventional networking technologies would have been considered insufficient. Additionally, the project demonstrated how the mobility of nodes could be utilized to facilitate communication in a network that possessed topologies that were unpredictable and dynamic [5].

The evolution of delay-tolerant networks has been highlighted by substantial theoretical contributions from research groups such as DTNRG and IPNSIG, as well as practical applications such as ZebraNet, which have proved the real-world potential of these networks. These contributions have been made possible by numerous practical applications. DTNs have made it possible to communicate in circumstances where traditional networks are unable to do so. They have provided solutions for a variety of industries, including wildlife tracking, remote sensing, and military communication, by addressing the issues of high latency and frequent disruptions. As the research on DTN continues to improve, additional developments in protocols and methodology will be made, which will result in an increase in the applicability and efficiency of these networks in an even wider variety of application scenarios.

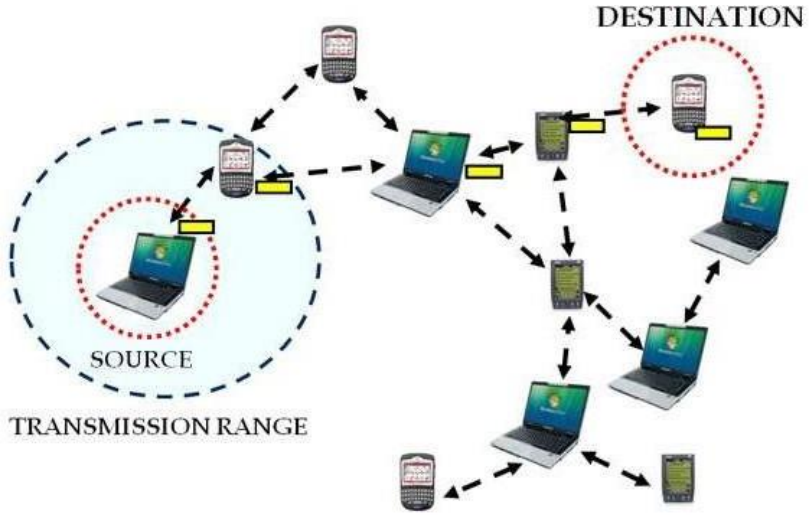

Figure 1: Delay-Tolerant Network [6]

DTNs can be used in military ad-hoc networks (when nodes are constantly moving and are prone to destruction), interplanetary networks (when satellite-to-satellite communication is characterized by long delay and intermittent connectivity) [6], and battery-powered sensor networks (whose consumption causes the nodes to deactivate and subsequently the fall of the related links), as illustrated in fig. 1.

I. DTN's ARCHTECTURE

RFC4838 (DTN Architecture [7]) anticipated a general architecture that would address all of the prior issues in message storage and forward switching. This switching is based on asynchronous messaging, and it makes use of postal mail to replicate delivering semantics and utility classes. Bundles of user data are forwarded from the source to retention on another node, and the custodians nodes are responsible for the bundle's effective delivery to its destination. The bundle would travel through a series of custodians before arriving to the final destination retailer.

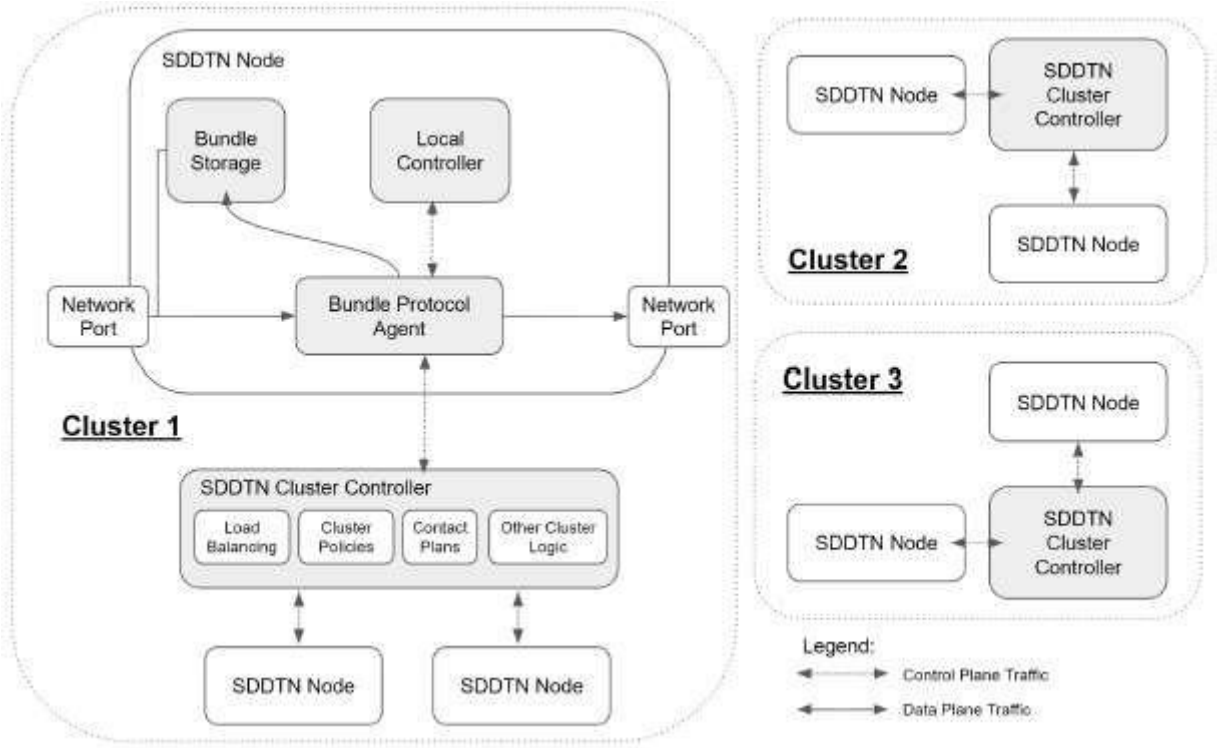

Figure 2: Delay-Tolerant Network Architecture

An SDN method for controlling scalability in space DTN networks is suggested because the scaling of space DTN routing is still a topic of active research. By splitting their networks into a control plane and data plane and centralizing the control plane, network operators can utilize SDN to operate their big networks in a scalable way. The task of passing data across the network is handled by network routers, which make up the data plane. However, a centralized SDN controller controls the routes and policies of this data forwarding. Assuming a control plane link is present, this architecture has the advantage of allowing network operators to quickly monitor and alter the behavior of sizable swaths of the network. These are desirable attributes for a space DTN network operator who might wish to modify the network's behavior in response to shifting political or technical limitations. However, it is unclear how this may be applied to the DTN environment, where links are naturally intermittent, as SDN necessitates control plane links between the SDN controller and the network's nodes [8].

The SDDTN architecture divides the network into clusters in order to address the problem of having dependable links between the controller and network nodes. Each cluster has several SDDTN nodes and a single SDDTN cluster controller, as seen in Figure 2. Along with having a control plane link to its corresponding cluster controller, each SDDTN node shall exhibit all of the characteristics of a typical DTN node as outlined in the BP specification. The cluster controller can receive pertinent network status updates from SDDTN nodes over this link. The controller can then make decisions and spread them across the nodes in its cluster (e.g., by creating and distributing contact plans) based on local neighborhood information from the nodes in its cluster. Although how this is accomplished is outside the purview of this study, it is expected that the clusters are arranged so that these control plane links are largely dependable. The literature on SDN clustering and controller placement techniques is extensive [9], and it should be mentioned that these clusters might be identified similarly to regions in the DTN inter-regional routing approach [10], which was previously described. This architecture allows for more optimal decision-making than would be possible if nodes operated independently and ensures that network updates are reliably propagated over the control plane links. Furthermore, this clustering technique allows for faster decision-making times for large space DTN networks, even though cluster decisions might not be as good as those made with global information.

II. RELATED WORK

Every one of the ad hoc routing approaches presume that the network is resistant to quickly evolving topology and also that the source and destination are associated. A. Vahdat et al. developed a technique to transmit messages when there is no assurance of a connected path from source to destination (DTN) and when a network split occurs at the time a message is created. The author devised the Epidemic Routing protocol, which ensures final message delivery by exchanging messages among moveable nodes. In order to enhance message delivery in unreliable networks, hybrid approaches that integrate several strategies are the main focus of this paper's thorough analysis of Delay-Tolerant Network (DTN) routing protocols. The authors assess the efficiency, dependability, and overhead of DTN routing protocols by grouping them into epidemic, single-copy, and multi-copy protocols. In order to balance resource usage with successful message delivery, the survey emphasizes the adoption of hybrid approaches that combine opportunistic and conventional routing techniques. It offers insightful information for furthering DTN routing research by addressing potential future paths for hybrid protocols to overcome issues like excessive latency, disconnections, and resource limitations [11].

As a component of the Internet Research Task Force (IRTF), the DTNRG is dedicated to creating protocols and architectures for Delay-Tolerant Networks (DTNs), which are typified by protracted delays and sporadic connectivity. The team is in charge of creating essential DTN protocols, like the Bundle Protocol (BP), which facilitates communication in these severely interrupted settings [12]. The development of DTN standards has been greatly impacted by the research and materials produced by DTNRG, such as technical studies and working group talks. By encouraging cooperation between government, business, and academia, the group keeps pushing innovation in DTN routing, mobility management, and security.

Princeton University created ZebraNet, a wildlife tracking technology that uses the principles of Delay-Tolerant Networking (DTN). It makes use of DTN protocols to allow communication between mobile nodes, which are animals with GPS trackers, in settings where sporadic connectivity makes traditional communication methods impractical. When the animal-mounted GPS units in ZebraNet come into contact with other animals or mobile nodes, they record location data and send it to base stations. This system demonstrates the usefulness of DTNs in domains like environmental monitoring and wildlife conservation by efficiently gathering and transmitting wildlife data in faraway areas [13].

With an emphasis on enhancing data delivery efficiency by taking the destination's location and network topology into account, the study presents a destination-based routing protocol (DBRP) for Delay-Tolerant Networks (DTNs). By choosing nodes that have the best chance of arriving at their destination, DBRP lowers overhead and increases message delivery rates by adjusting to node mobility and proximity to the destination. The study demonstrates that DBRP outperforms conventional routing techniques in terms of delivery ratios and latency [14]. In sparse networks, when direct routes to the destination are uncommon, this destination-based strategy is especially advantageous.

The authors of this study provide a novel routing algorithm for Delay-Tolerant Networks (DTNs) that combines opportunistic and store-and-forward strategies. By carefully choosing nodes for data forwarding, the technique reduces message replication and maximizes resource use. The algorithm's capacity to strike a compromise between dependable message delivery and economical resource usage is demonstrated by the paper's simulation evaluation of its performance. The suggested technique provides a scalable answer to DTN routing problems, especially in settings with constrained energy and bandwidth.

III. ROUTING PROTOCOL

As per the processes used to identify a path from source to destination, routing protocols could be grouped into four categories: anticipating Good Forwarders, opportunistically forwarding messages, and meeting the destinations on time. Table 1 explains all types of procedures.

Proposed Year	**Protocol Name**	**Proposed Work**
2022	ITRM(iterative reputation management)	The effectiveness of message passing approaches towards decoding low-density parity-check codes across bipartite graphs inspired the development of a graph-based iterative method.
2022	Control message redundancy mechanism	This approach works by adding an encounter counter to each node based on the epidemic routing strategy
2023	Independent message deletion mechanism	This mechanism is for multicopy routing schemes.
2024	Multi-copy spraying algorithm	The quantity of message duplicates in the network is determined by the importance of reaching the message's delivery schedule.

2019	PRioritized EPidemic (PREP)	PREP ranks packages according to their costs to the destination, source, and expiration date.
2018	Max Prop	MaxProp is focused on prioritising both the packet scheduling and the network traffic. transmitted to other peers and the schedule of packets to be dropped.
2018	Spray and Wait	"sprays" a number of copies into the network, and then "waits" till one of these nodes meets the destination.
2019	PROPHET [15-22]	A probabilistic routing protocol for such networks

Predicting Good Forwarders: Depending on the node's history-encounter information, framework information, or location visiting sample, this approach attempts to predict the nodes that are beneficial for sending messages.

MobiSpace, MV, Seek and Focus, CAR, and MaxProp, RAPID, PROPHET, SMART are some of these routing protocols. All of these approaches make an attempt to predict constructive nodes for delivery based on the encountering history of previous nodes or scenario data like remaining battery lifespan.

a) **Meeting the destinations on time**: In this case, W. Zhao devised the Message Ferry (MF) mechanism [12]. Ferries are unique types of nodes in the MF scheme that can adjust their paths ahead of time to assist other nodes in sending messages. Furthermore, Tariq et al. regularise ferry travel across routes to ensure that concerned nodes are seen with a particular probability.

b) **Messages are forwarded opportunistically**: Protocols in this system, such as Epidemic, opportunistically forward messages to other nodes until they reach their targets [23].

Another protocol that prioritizes packets based on costs to the source, destination, and expiration time is called PRioritized EPidemic (PREP). Per-link "average availability" data that is spread like wildfire is used to compute costs. As the distance between the source and the destination grows, PREP keeps the copying density from increasing.

P. Mundur et al. [24] modified and extended epidemic routing in DTNs. They promoted the inclusion of information based on immunity that is given in reverse after messages have reached their intended receivers. Information about delivered messages is stored by this protocol using an immunity-list, which stops them from being exchanged in the future. Consequently, it outperforms simple epidemic techniques in terms of delay and delivery ratio.

There are numerous approaches to handle message overhead issues in epidemic protocols, including the Prophet Protocol and the Spray and Wait protocol. These techniques restrict the quantity of message copies that are accessible rather than overflowing communications. Prophet is a probabilistic routing method for DTN networks that uses node delivery probability to route messages with a lower communication overhead. The spray routing system spreads a certain number of copies of every message around the network, making it an epidemic routing mechanism. Spray and Wait performs better than any other routing protocols in terms of average message delivery latency and number of transfers per message transmitted. Erasure-coding A message is divided into code blocks by Based Routing (EBR) [25] and "sprayed" to a collection of relays. Any sufficiently significant subset of the generated code blocks can be utilized to reassemble the new message. Information Rahul and associates In order to transmit messages in a sparse sensor network, MULE.'s Routing [26] generates randomly-moving mobile nodes (MULEs), which take in messages from stationary sensors while they are nearby. They send the received messages to wired contact points after buffering them when they are sufficiently close.

For Delay Tolerant Networks (DTNs), a multi-copy routing protocol with an independent message deletion mechanism was created in 2010. You may send your messages more quickly and make the most of your resources by using this tactic. A novel approach based on the epidemic routing protocol was proposed in 2011 to handle message redundancy by coming across a counter, which keeps track of how many times a node comes across other nodes that have the same message copy. Node removes the copy if the counter hits the installed threshold.

Consequently, the different routing methods used in DTN have different overhead ratios, delivery probabilities, and average message delays. In addition to offering a 100% delivery ratio, the Epidemic technique has a greater overhead ratio. To lower the overhead ratio, other protocols, however, employ techniques to restrict message copy forwarding.

IV. Security In Routing Protocols in DTN

A number of malicious node attacks might affect the DTN's performance. Attacks of this nature need to be identified. Many research have been conducted on the security of MANET routing [27], however as DTN routing is frequently opportunistic with intermittent connectivity, it cannot be used to secure DTN. Many DTN routing systems use public key and policy-based cryptography to tie players to a list of allowed nodes. Space and link capacity have been allotted based on the type of service. One such strategy that adds a large amount of handing out overhead is the validation of all routing metadata and packets at each in-between hop. However, key management is challenged by DTN's inconsistent connectivity and may be challenging to execute in various trust strategies and environments.

(A) General Attack

Since the DTN network is susceptible to numerous intrusion attempts, security is a challenging problem. Consequently, a number of assaults have been discovered by various researchers.

Four general attacks are present. Drop Everything: Get rid of every packet that comes in. Attackers send many packets at once, send fraudulent acknowledgements, and invert routing metadata, which involves dropping or transferring data in the wrong sequence.

Despite the failure of the aforementioned attacks, there were still important differences between them. Consequently, Fai Cheong and associates created a variant of these attacks, namely Flooding Non-Deliverable Packets, which transmits data to nonexistent nodes. Impersonating different personas to pretend to be packet destinations is known as identity impersonation.

In addition to those mentioned above, more attacks were described as follows: Self-promotional attacks: by building a solid reputation, it may advertise itself. Attacks known as "badmouthing": subpar suggestions made against outstanding nodes may compromise the reputation of good nodes. In order to send packets through bad nodes, ballot stuffing can assist them improve their reputation.

A trust-based approach has been devised to deal with network spoiling nodes.

The node's reputation against black hole attacks is a determining factor in a reputation-based message forwarding scheme.

In order to improve the preferred delivery ratio by deadline when malicious nodes are present, Bulet et al. introduced a two-period routing strategy.

SPREAD (countermeasure against spoofing by REplica ADjustment), a solution that assesses spoofing evidence and generates countermeasures believed for quota-based multi-copy routing protocols without the use of a network wide verification system, was proposed by a publisher in 2011 in an effort to make DTNs robust against spoofing attacks with localized countermeasures.

Motivated by the prior success of iterative message passing approaches for decoding low-density parity-check codes across bipartite graphs, ITRM is a planned graph method.

With nodes in the network following a trace-based mobility paradigm, a trusted framework for DTN was developed in 2012. The next hop at which to forward the data packets is determined by the trust value and the node's path to the destination. The trust value of the trust framework of the data forwarding node.

According to a Secure User-centric and Social-aware Reputation-based Incentive Scheme for DTNs (SUCCESS [53]), this node can preserve its popularity evidence by showcasing its reputation value.

Give to Get Forwarding is helpful in a social mobile wireless network of selfish people. Since nodes are devoted to one community but not to others, selfishness is taken into account in this work.

V. CONCLUSION

This literature review will discuss the multicast routing methods used in the DTN network. Other methods, such those that exploit opportunities to send messages, have been tested using protocols in the Predicting Good Forwarders domain. The efficiency of routing protocols may be adversely affected by a number of security flaws and exploits that have been discovered.

PRoPHET and its variants were thoroughly examined. There are still a number of attacks that can lead to poor behavior from the PRoPHET routing protocols, as well as methods that can make the attacks ineffective.

REFERENCES

[1] LunaNet Interoperability Specification Document Version 4; Technical Report; National Aeronautics and Space Administration and European Space Agency: Washington, DC, USA, 2022.

[2] Otero, D.G. ESA Moonlight Initiative. Presented at IPNSIG Academy. 2022. Available online: https://ipnsig.org/wp-content/uploads/2022/11/IPNSIG-ESA-Moonlight-overview-Nov-2022-1.pdf

[3] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimizing AI-Driven Security Protocols in IoT Networks Using Metaheuristic Algorithms", International Journal of Intelligent Systems and Applications in Engineering, IJISAE, 2024, 12(23s), 3339–3347.

[4] Habeeb, M. S., & Babu, T. R. (2022). Network intrusion detection system: a survey on artificial intelligence-based techniques. Expert Systems, 39(9), e13066.

[5] R. Gnanakumaran, Divya Rohatgi, A K Sampath, Nidhi Nagar, D. Amuthaguka, Raj Kumar Gupta, "Robust Extreme Learning Machine based Sentiment Analysis and Classification", 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), (2023), DOI: 10.1109/ICSSIT55814.2023.10061017.

[6] Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K.; Weiss, H. Delay-Tolerant Networking Architecture; RFC 4838; IETF: Fremont, CA, USA, 2007. https://doi.org/10.17487/RFC4838.

[7] Naveen Sai Bommina, Nandipati Sai Akash, Uppu Lokesh, Dr. Hussain Syed, Dr. Syed Umar, "A Hybrid Optimization Framework for Enhancing IoT Security via AI-based Anomaly Detection", International Journal on Recent and Innovation Trends in Computing and Communication, (2023) ISSN: 2321-8169 Volume: 11 Issue: 3.

[8] NASA Jet Propulsion Laboratory. Interplanetary Overlay Network (ION). Available online: https://sourceforge.net/projects/ion-dtn/ (accessed on 1 September 2022).

[9] Thakre N, Nimma D, Turukmane AV, Singh AK, Rohatgi D, Bangaru B (2024) Dynamic path planning for autonomous robots in forest fire scenarios using hybrid deep reinforcement learning and particle swarm optimization. Int J Adv Comput Sci Appl 15(9).

[10] Nandipati Sai Akash, Uppu Lokesh, Naveen Sai Bommina, Hussain Syed, Syed Umar, "Swarm Intelligence-Based Hyperparameter Optimization for AI-Powered IoT Threat Detection", International Journal of Intelligent Systems and Applications in Engineering, (2024), 12(17s), 941.

[11] Bormann, C.; Hoffman, P.E. Concise Binary Object Representation (CBOR); RFC 8949; IETF: Fremont, CA, USA, 2020. https://doi.org/10.17487/RFC8949.

[12] Habeeb, M. S., & Babu, T. R. (2024). Coarse and fine feature selection for network intrusion detection systems (IDS) in IoT networks. Transactions on Emerging Telecommunications Technologies, 35(4), e4961.

[13] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[14] K Sankar, Divya Rohatgi, S Balakrishna Reddy, "COX Regressive Winsorized Correlated Convolutional Deep Belief Boltzmann Network for Covid-19 Prediction with Big Data", Grenze International Journal of Engineering & Technology (GIJET), Grenze ID: 01.GIJET.9.1.547, © Grenze Scientific Society, 2023.

[15] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[16] RS Supriya Khaitan, Divya Rohatgi, Sana Nalband, Tejali Mhatre, Shweta Patil, "Enhancing Essay Grading Efficiency and Consistency through Two-Layer LSTM Models and Attention Mechanisms", Journal of Information Systems Engineering and Management 10 (2), 191-202.

[17] Umar, Syed, Bommina Naveen Sai, Nagineni Sai Lasya, Doppalapudi Asutosh, and LohithaRani. "Machine Learning based Sentiment Analysis of Product Reviews Using Deep Embedding." Journal of Optoelectronics Laser 41, no. 6(2022): 108-113.

[18] Habeeb, M. S. (2024). Predictive analytics and cybersecurity. Intelligent Techniques for Predictive Data Analytics, 151-169.

[19] Killi, B.P.R.; Reddy, E.A.; Rao, S.V. Cooperative game theory based network partitioning for controller placement in SDN. In Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 105–112. https://doi.org/10.1109/COMSNETS.2018.8328186.

[20] Isong, B.; Molose, R.R.S.; Abu-Mahfouz, A.M.; Dladlu, N. Comprehensive Review of SDN Controller Placement Strategies. IEEE Access 2020, 8, 170070–170092. https://doi.org/10.1109/ACCESS.2020.3023974.

[21] Hauser, F.; Häberle, M.; Merling, D.; Lindner, S.; Gurevich, V.; Zeiger, F.; Frank, R.; Menth, M. A Survey on Data Plane Programming with P4: Fundamentals, Advances, and Applied Research. arXiv 2021. arXiv:2101.10632.

[22] Musumeci, F.; Fidanci, A.C.; Paolucci, F.; Cugini, F.; Tornatore, M. Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks. J. Netw. Syst. Manag. 2022, 30, 21. https://doi.org/10.1007/s10922-021-09633-5.

[23] NASA Space Communications and Navigation. Cognitive Communications Project. Available online: https://www1.grc.nasa.gov/space/scan/acs/cognitive-communications/

[24] HABEEB, M. S., & BABU, T. R. (2024). WOA-SA: OPTIMIZING NIDS WITH ENHANCED DEEP LEARNING FOR ZERO-DAY ATTACK DETECTION. Journal of Jilin University (Engineering and Technology Edition).

[25] Shamim, M. Z., Syed, S., Shiblee, M., Usman, M., Zaidi, M., Ahmad, Z., & Habeeb, M. (2019, December). Detecting benign and pre-cancerous tongue lesions using deep convolutional neural networks for early signs of oral cancer. In BASIC & CLINICAL PHARMACOLOGY & TOXICOLOGY (Vol. 125, pp. 184-185). 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY.

[26] Sipos, B.; Demmer, M.; Ott, J.; Perreault, S. Delay-Tolerant Networking TCP Convergence-Layer Protocol Version 4; RFC 9174; IETF: Fremont, CA, USA, 2022. https://doi.org/10.17487/RFC9174.

[27] Scott, K.; Burleigh, S. Bundle Protocol Specification; RFC 5050; IETF: Fremont, CA, USA, 2007. https://doi.org/10.17487/RFC5050.