Renewable Energy, Environment, and Power Quality Journal (REE&PQJ)
ISSN:3020-531X
Volume No.3, July 2025

Enhancing Connectivity and Cybersecurity in Renewable Energy Facilities Using Delay Tolerant Networks approach

J. Lourenço[1], N. Neves[1] and J. Morais[1]

[1] ISPGAYA
Av. dos Descobrimentos 333, 4400-103 V. N. Gaia (Portugal)

Abstract. In the context of renewable energy facilities, ensuring continuous and reliable network connectivity is critical for monitoring, control, and optimization of energy production. As these facilities often operate in remote or resource-challenged locations, maintaining connectivity during catastrophic events, in under developing nations, or in conflict zones becomes a significant challenge. This article explores a proposal for the integration of Delay Tolerant Networks (DTNs) as a robust solution for addressing connectivity issues in such environments. DTNs are designed to operate effectively even with intermittent or unreliable communication links, making them ideal for scenarios where traditional communication infrastructure is unavailable or damaged. The paper discusses the importance of maintaining an always-on connection to enable real-time data collection, fault detection, and system adjustments, which are essential for efficient renewable energy operations. Additionally, cybersecurity concerns associated with remote renewable energy networks are highlighted, particularly in vulnerable regions. Cyber threats targeting critical infrastructure in unstable regions could compromise the reliability and safety of energy systems. The article examines methods for enhancing cybersecurity in DTN-based networks ensuring that the integration of these networks does not expose energy systems to malicious attacks. A novel approach is, also, presented for a secure and resilient communication with DTN between Renewable Energy Facilities with the introduction of a mobile node for extremely severe communication scenarios. At last, this work is the first step towards the evolution into a future prototype phase.

Key words. DTN, IoT, Renewable Energy, Renewable Energy Facilities, Cybersecurity.

1. Introduction

Connecting renewable energy facilities in a network significantly enhances efficiency, operation, and management of energy systems. By integrating various renewable sources like solar, wind, hydro, and biomass into a unified grid, we can optimize energy production and distribution, ensuring a more balanced and reliable supply.

In terms of efficiency, a networked system allows for the seamless transfer of surplus energy from one region to another, reducing waste and maximizing resource utilization. This interconnectedness ensures that energy generated from renewable sources is used effectively, minimizing the need for backup power from non-renewable sources.

From an operational perspective, a networked renewable energy system provides greater flexibility and stability. When one source is not producing (e.g., solar panels at night), other sources can compensate, maintaining a steady energy supply. This redundancy reduces the risk of power outages and enhances the overall resilience of the grid.

In terms of management, a connected network facilitates better monitoring and control of energy flows. Advanced technologies and smart grid solutions enable real-time data analysis, allowing for proactive maintenance and efficient allocation of resources. This leads to improved performance, reduced operational costs, and enhanced decision-making capabilities.

So, connecting renewable energy facilities in a network offers significant advantages in efficiency, operation, and management, contributing to a more sustainable and reliable energy future.

Delay-Tolerant Networking (DTN) is a crucial solution for maintaining connectivity under network constraints and during catastrophes. DTN is designed to handle intermittent and unreliable connections by storing and forwarding data packets until a stable path is available. This approach ensures that information can still be transmitted even when traditional networks fail.

In disaster scenarios, where infrastructure might be damaged or overloaded, DTN provides a resilient communication method. It allows for the gradual and reliable delivery of critical information, such as emergency alerts and coordination messages, ensuring that aid and resources can be effectively managed and distributed.

The resilience of DTN lies in its ability to adapt to changing network conditions. By leveraging opportunistic connections and dynamically adjusting routes, DTN can maintain communication links despite disruptions. This flexibility makes it an invaluable tool for emergency response, remote areas, and any situation where conventional networks are insufficient.

At last, DTN enhances the robustness and reliability of communication systems, making it an essential technology for ensuring connectivity in challenging environments.

Delay-Tolerant Networking (DTN) can enhance cybersecurity by providing robust data transmission methods that are less vulnerable to attacks. DTN's store-and-forward mechanism ensures data is securely held until a reliable path is available, reducing the risk of interception during transmission. Additionally, DTN can operate in isolated or disrupted networks, making it harder for attackers to exploit network vulnerabilities. Its ability to dynamically adjust routes and use opportunistic connections further complicates potential attack vectors. By maintaining secure communication even under adverse conditions, DTN strengthens the overall resilience and security of networked systems.

The article has the following sections: besides this introductory section, a second section with the literature review, a section with the novel approach followed by a last section with the conclusion.

2. Literature Review

A bibliographic search was conducted in December of 2024 up till March of 2025 in IEEE Xplore and Google Scholar with the search keywords: DTN, DTN Security, DTN IoT, Renewable Energy Monitoring and Renewable Energy Security.

DTN, is a type of wireless ad-hoc network. It works when the end-to-end direct path does not exist between source and destination then it's using the Store and Forwarding routing mechanism [1]. Current DTN networks rely on the assumption that all node movements in relation to each other are able to be summarized ahead of time. These movements are stored in the form of static contact plans, which each node independently uses to inform its own routing decisions [2]. Networks must allow data to be exchanged, and these data must be understood by the entities that receive them. Although a lot of DTN routing protocol has been proposed for DTN networks, but with the emergence of new technological applications such as drones, the Internet of Things, etc., the DTN routing protocol is still in use. It is desirable to develop a feasible, reliable and robust protocol for this new range of applications [3].

The DTN architecture and particularly the Bundle protocol, offers solutions in networks where low connectivity, big or variable delays and increased error rates are prevalent. Using persistent storage, a DTN node is able to overcome such limitations; the data can be transmitted several times until it is successfully received by the next hop. However, since the conditions in a DTN network might vary, from time to time we may experience high connectivity and low delays [4]. In DTN the congestion control is the wide researched sector in because as it could be able to establish the network in an unfavourable environment where network infrastructure is not readily available. Even after the successful deployment of a network the high priority messages must be taken care of, and they must not be dropped as it affects the foundation of DTN environment, because some applications are found to be sensitive. Some of the well-known congestion control strategies have been discussed compared after which a routing algorithm is proposed by studying them [5].

Any two nodes that move within each other's transmission range can exchange messages. This may form the basis for future forwarding based on past contact history. Based on these identifiable patterns one may predict contacts in near future. Some existing schemes use utility functions to steer the routing in the right direction but are limited and is unable to capture enough information of the network. In this paper, the Trust Model is further extended to identify cluster heads in DTN environment that results in the optimal utilization of the node's resources. Due to high network mobility, it is assumed that the node's contacts are unpredictable so that it can reflect the most efficient way of message movement [6]. DTN can realize mobile devices communication without constructing infrastructure. DTN is effective at the time of disaster as mobile adhoc network (MANET) [7].

DTN has a broadband of applications that goes beyond classical networks up till space communications or even resilient learning scenarios [8], [9]. Research presents the use of AI over DTN to promote resilience in communications [10].

The application of emerging technologies in the context of renewable facilities has been explored through various approaches, as described in [11–15]. The integration of IoT in this domain is discussed extensively in [16–21]. Security issues, a critical area of concern, are thoroughly researched in [22–27]. Additionally, the preservation and security of data in challenged and intermittent networks are of paramount importance in Delay Tolerant Networks (DTNs), as highlighted in [28, 29].

A border security architecture has been proposed where DTN is used for transferring messages within the army units of a particular region that are deployed in harsh terrains, thereby ensuring integrity and security of the message. In the proposed approach, a special property of the nodes is used which makes them self-disposable in nature after either their mentioned TTL gets over or whenever data tampering takes place in the node. So, the message as well as the node will be definitely safe from getting accessed in an unauthorized manner [30]. DTN is characterized by mobile nodes and dynamic network topology. There are some selfish / malicious nodes (termed as misbehaving) present in the network resulting in the packet loss. Currently these are identified only after data transmission. The core idea is to ensure secure data transmission in DTN in the presence of misbehaving nodes. This is achieved by means of ICN (Information Centric Network) which supports node mobility and interactivity. Here ICN is used along with DTN. ICN intimates about misbehaving nodes in the path so that alternative path is chosen. The packets reach the destination safely [31], [32]. A security management framework to dynamically configure or reconfigure emergency networks, in order to adapt the use of security components according to management information received by the decision-maker entities. The security management model includes the definition of security levels, the management information base, protocol messages and events. The emergency network activates the security mechanisms only, when necessary, which avoid attacks effects and save resources [33]. The DTN architecture allows for secure messaging without requiring a contemporaneous end-to-end path. The implementation of such a system must rely upon per-node autonomy in the absence of timely end-to-end messaging. This autonomy can be built from a combination of in-band security information present in message traffic combined with a local autonomy engine such as one proposed for DTN network management. The following bibliographic reference describes how a DTN network management system can be used to implement a self-managing security service (SMSS) providing an autonomous per-node security policy [34]. The [35] surveys existing terrestrial network security practices, focusing on public key infrastructure with X.509 (PKIX), and identifies ways that the existing systems and protocols can be used in a delay-tolerant networking (DTN) environment. Additional discussion of protocols currently under development shows how PKIX security can be used directly and efficiently within a DTN. These are combined into one possible vision for distributed and autonomous security within the existing LunaNet architecture. A peer-to-peer (P2P) network security pricing model that promotes the growth of P2P networks with an increased resistance to malicious code propagation. The security pricing model integrates findings from recent developments in complex network theory with incentive compatible pricing. The model links file download prices in P2P networks with a metric called the Pearson coefficient. The calculation of the Pearson coefficient indicates a structural dimension of networks called "preferential attachment". The security pricing model employs a mechanism that charges nodes (network users) higher prices for choosing "bad" links, that is links that decrease the Pearson coefficient, because these links inhibit preferential attachment in networks and ultimately degrade networks' resistance to malicious code propagation. The security pricing model provides incentives for nodes to choose the lower priced "good" links (that is, links that increase the Pearson coefficient). Continuing research will focus on formalizing and validating the P2P network security model [36].

In the literature reviewed, the issue of DTN consumption and the adoption of DTN as a solution for communication between renewable energy facilities is also presented. One of the major problems of DTN networks is limited energy resources which impose strict constraints on the operational lifespan of DTN nodes. To solve these problems, we propose the adoption of a long-term strategy for energy management, based on the exploitation of renewable energies and the improvement of the HRTT topological architecture through the direct integration of renewable energy sources within DTN nodes. Indeed, DTN nodes powered by renewable energy resources, such as solar energy, have the potential to recharge themselves, extending their operational lifespan, increasing their storage and transmission capabilities, and reducing dependence on non-renewable energy resources [37]. For energy-harvesting sensor nodes, rechargeable batteries play a critical role in sensing and transmissions. By coupling two simple Markovian queue models in a delay-tolerant networking setting, we consider the problem of battery sizing for these sensor nodes to operate effectively: given the intended energy depletion and overflow probabilities, how to decide the minimal battery capacity that is required to ensure opportunistic data exchange despite the inherent intermittency of renewable energy generation [38].

3. Novel Approach Proposal

A. Solution Description

DTN offers several advantages over traditional IP connections, particularly in environments where connectivity is intermittent or subject to long delays. Unlike ordinary IP connections, which require a continuous end-to-end path for data transmission, DTN uses a store-and-forward approach. This means data packets are stored at intermediate nodes until a connection becomes available, ensuring reliable delivery even in challenging conditions, which is of particular relevance as the Renewable Energy Facilities, as previously described, need the support of data.

One of the primary benefits of DTN is its robustness in environments with frequent disruptions, such as space communications, remote areas, or disaster-stricken regions. DTN can handle long delays and high latency, making it ideal for critical scenarios where communication delays are significant. Additionally, DTN can utilize multiple paths and providers to enhance data delivery efficiency and reliability. Also improves network resource utilization by allowing data to

be transmitted when network conditions are favourable, decreasing the need for permanent connectivity. This flexibility leads to more efficient use of bandwidth and better overall network performance. And its advantage go beyond: DTN includes security features such as integrity checks, authentication, and encryption, ensuring secure data transmission even in disrupted environments.

Overall, DTN's ability to manage disruptions, delays, and intermittent connectivity makes it a superior choice for specific applications compared to traditional IP connections.

A Super Node (SN) can be elected to perform critical functions such as authentication, routing, and implementing security features. To enable this process effectively, several important factors must be taken into account. First, it is essential to conduct a comprehensive node discovery process to identify all nodes in the network and gather detailed information about their capabilities. This includes assessing each node's processing power, storage capacity, and battery life, as these factors determine their ability to handle additional tasks. The criteria for selecting a Super Node should also be clearly defined. An SN must have sufficient computational resources to handle additional tasks efficiently, ample storage capacity to manage data effectively, and a reliable power source or long battery life to ensure continuous operation. Furthermore, the node should maintain strong and stable connections with other nodes in the network to facilitate seamless communication.

To make the selection process systematic, a scoring system should be developed based on the defined criteria. Each criterion should be assigned a weight according to its importance, and nodes should be evaluated against this system. Nodes that achieve higher scores are considered more suitable candidates for the SN role. After scoring, an election algorithm can be implemented to select the SN. Algorithms such as Bully or Ring can be used to choose the node with the highest score, while consensus-based algorithms like Paxos or Raft can help nodes collectively agree on the best candidate for the role.

By following these steps, the network can efficiently identify and elect a Super Node capable of managing additional responsibilities while maintaining network efficiency and security.

The architecture proposed aims to connect multiple renewable energy facilities using a DTN to ensure reliable data transmission even in challenging network conditions. LoRa (Long Range) technology is proposed for its low power consumption and long-range communication capabilities.

The architecture will be supported by the following components:

1) *Renewable Energy Facilities.*
2) *IoT Sensors.*
3) *LoRa Nodes.*
4) *DTN Nodes.*
5) *Gateway Nodes (bridges between the LoRa network and the DTN).*

The IoT sensors will collect all the relevant data (e.g. energy production, equipment status, and environmental conditions). LoRa nodes at each facility broadcast the collected data to nearby DTN nodes. The LoRa nodes use the LoRaWAN protocol to send data to the nearest DTN node. DTN nodes will forward the data to the nearest DTN Node in a store-and-forward solution. Elected SN will handle additional routing and security functions, ensuring efficient data transmission and network security and all the data collected from renewable energy facilities is processed and analysed to monitor energy production, detect anomalies, and optimize operations. The security features comprise the following functions:

1) *Authentication: Ensure that only authorized nodes can join the network and transmit data.*
2) *Encryption: Encrypt data during transmission to protect it from eavesdropping and tampering.*
3) *Integrity Checks: Use cryptographic techniques to verify the integrity of data packets.*

At last, a periodic revaluation is conducted: ensuring that the SN keep meeting the requirements. If not, initiate the election process.

The proposed solution enables a bullet proof connection between the Renewable Energy Facilities to grant access to production data and all the operation and maintenance issues. With DTN the risk of non-connected facility is drastically reduced. The DTN with the SN approach will optimize routing functions and will enhance cybersecurity risks.

B. Solution Computation

In order to validate the proposed approach a 10 Km per 10Km square area was considered. Assuming that each node (renewable energy facility) has a ranging communication of 2 Km, that all the facilities are randomly distributed over the area. The probability calculation of each node having at least two nodes in their range – will enable the chance to build a reliable structure over a stationary network:

The total area is 100 Km2.
The communication range of each node is

$$\boldsymbol{A = \pi 2^2} \quad (1)$$

Each node has a circular "neighbourhood" of radius r=2 km, so its area is:

$$\boldsymbol{A_{Radio} = \pi(2^2) = 12,57\ Km^2} \quad (2)$$

Ignoring boundary effects (or assuming a "wrap□around" model), the probability that any other node lies within a given node's range is:

$$\boldsymbol{p = \frac{A_{Radio}}{A} \approx \frac{12,57}{100} \approx 0,1257} \quad (3)$$

If there are n nodes, then for any given node the number of other nodes falling inside its range is approximately:

$$\boldsymbol{X \approx Binomial(n-1, p)} \quad (4)$$

We want the probability that X≥2
For a single node this probability is:

$$\boldsymbol{P(X \geq 2) = 1 - P(X = 0) - P(X = 1)} \quad (5)$$

Where:

$$\boldsymbol{P(X = 0) = (1-p)^{n-1}} \quad (6)$$

$$\boldsymbol{P(X = 1) = (n-1)p(1-p)^{n-2}} \quad (7)$$

Because the nodes' positions are mutually dependent (their range overlap) a rigorous calculation would require accounting for spatial correlations. However, if we assume independence (a common first approximation), then the probability that every node has at least 2 neighbours is approximately:

$$\boldsymbol{[P(X \geq 2)]^n} \quad (8)$$

Let's compute for several possible number of nodes:

Table I. – Probability of two nodes in range

Nodes	Radio Range	In two nodes range
50	2 Km	57.1%
60	2 Km	81.5%
70	2 Km	93.1%
80	2 Km	97.6%
100	2 Km	99.76%
120	2 Km	99.98%

As described by the table above, even with 80 nodes there is a strong probability that a communication path may be established granted by the presence at least two nodes in the vicinity of each node. This assurer the possibility of assuring a reliable path end-to-end over the area. The assumption of only a 2 Km communication radius also introduces a great tolerance. The network is expected with less nodes if we consider a longer LoRa range (as expected).
In a catastrophic scenario, as demonstrated, there is a dependence on the distribution of the nodes and where even with a smaller amount of nodes - the communication will be possible. For a massive dropout of the existing alive nodes the introduction of mobile nodes (with the singe purpose of relaying the information in a DTN approach) will have to be implemented keeping the communication between all the nodes as described in [39] & [40].

4. Conclusions

The article described a novel approach to achieve the "always-on" even over severe communications scenarios along with cybersecurity concerns. The Renewable Energy Facilities are crucial in the electric energy production chain so to be able to

monitor and control them, is vital. The IoT will enable to retrieve all the relevant data from production while DTN will bring the layer of connectivity and security. The SN approach will grant special functions for nodes that, at an instant, have battery charge, processing power or even storage capacity to lead special and relevant functions in the network. On the other hand – LoRa will enable long range communications, easy new locations setup will low power consumption. A simulated scenario is presented to describe the feasibility and performance of the novel approach proposed.
At last, DTN will also promote a greener solution: store-and-forward data can be done in a store-and-forward approach in moments with less load in the network and without consuming more resources as common always connected solution. At last, LoRA with DTN will provide a sustainable solution.

References

[1] M. A. Hoque, M. Razu, T. Islam, and A. Amin, «SDN-DTN Combined Architecture in Post Disaster Scenario — A new way to start», in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 230–235. DOI: 10.1109/ICACCS48705.2020.9074388.

[2] D. Ta et al., «Roaming DTN: Integrating unscheduled nodes into contact plan based DTN networks», in 2023 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW), 2023, pp. 1–9. DOI: 10.1109/CCAAW57883.2023.10219232.

[3] E. A. A. Alaoui, C. S. T. Koumetio, A. Gallais, and S. Agoujil, «Towards a DTN protocol for the Internet of Things», in 2019 Global Information Infrastructure and Networking Symposium (GIIS), 2019, pp. 1–6. DOI: 10.1016/j.procs.2020.03.107.

[4] S. Dimitriou and V. Tsaoussidis, «Effective buffer and storage management in DTN nodes», in 2009 International Conference on Ultra-Modern Telecommunications & Workshops, 2009, pp. 1–3. DOI: 10.1109/ICUMT.2009.5345376.

[5] P. Patil and M. Penurkar, «Congestion avoidance and control in DTN», in 2015 International Conference on Energy Systems and Applications, 2015, pp. 755–760. DOI: 10.1109/ICESA.2015.7503451.

[6] V. Sharma, N. Pandey, and R. Saggar, «Opportunistic message forwarding in self organized cluster based DTN», in 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), 2017, pp. 497–502. DOI: 10.1109/ICTUS.2017.8286060.

[7] S. Kitada, G. Hirakawa, G. Sato, N. Uchida, and Y. Shibata, «DTN based MANET for disaster information transport by smart devices», in 2015 18th International Conference on Network-Based Information Systems, 2015, pp. 26–31. DOI: 10.1016/B978-0-12-809859-2.00004-8.

[8] J. Lourenço, C. Lucas, J. Becker and J. Morais, «A novel approach for distributed security over IoT in learning environment», at Smart Innovation, Systems and Technologies, Singapore: Springer Nature Singapore, 2023, pp. 621–631. DOI: 10.1007/978-981-99-5414-8_57.

[9] D. J. Israel, F. Davis, and J. Marquart, «A DTN-based multiple access fast forward service for the NASA space network», in 2011 IEEE Fourth International Conference on Space Mission Challenges for Information Technology, 2011, pp. 61–65. DOI: 10.1109/SMC-IT.2011.19.

[10] J. Lourenço, J. Morais, C. Lucas, and J. Paulo, «Delay tolerant network and artificial intelligence technology on resilient learning», at EDULEARN Proceedings, 2024, vol. 1, pp. 2746–2753. DOI: 10.21125/edulearn.2024.0747.

[11] M. Ulrich, «Network quality and network dynamics in relation to renewable energy», at 11th International Conference on Electrical Power Quality and Utilisation, 2011, pp. 1–4. DOI: 10.1109/EPQU.2011.6128903.

[12] L. Coo and K.-H. Liu, «Implementation of a web-based real-time monitoring and control system for a hybrid wind-PV-battery renewable energy system», in 2007 International Conference on Intelligent Systems Applications to Power Systems, 2007, pp. 1–6. DOI: 10.1109/ISAP.2007.4441615.

[13] P. Kanchan, A. K. Singh, and N. Guruprasad, «Revolutionizing renewable sources of energy using IoT: Impact and challenges», in 2023 International Conference on IoT, Communication and Automation Technology (ICICAT), 2023, pp. 1–5. DOI: 10.1109/ICICAT57735.2023.10263688.

[14] C.-S. Choi, J.-D. Jeong, I.-W. Lee, and W.-K. Park, «LoRa based renewable energy monitoring system with open IoT platform», in 2018 International Conference on Electronics, Information, and Communication (ICEIC), 2018, pp. 1–2. DOI: 10.23919/ELINFOCOM.2018.8330550.

[15] R. Byrtus, R. Hercik, J. Dohnal, J. B. Martinkauppi, T. Rauta, and J. Koziorek, «Low-power renewable possibilities for geothermal IoT monitoring systems», in 2022 11th International Conference on Renewable Energy Research and Application (ICRERA), 2022, pp. 164–168. DOI: 10.1109/ICRERA55966.2022.9922835.

[16] V. Singh Thakur and R. Raman, «Efficient fault detection in renewable energy systems through IoT and isolation forest algorithm», in 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2023, pp. 1–6. DOI: 10.1109/ICSES60034.2023.10465413.

[17] J. Li and S.-H. Hwang, «Renewable energy with energy-efficient distributed processing for IoT», in 2022 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 2022, pp. 160–164. DOI: 10.1109/APWCS55727.2022.9906482.

[18] T. S. B. Damodhar, R. Raman, A. A. Gokhale, R. Babuji, K. Sasikala, and S. Srinivasan, «IoT enabled space vector modulation control for multilevel converters in renewable energy systems», in 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), 2023, pp. 1003–1007. DOI: 10.1109/PEEIC59336.2023.10450937.

[19] S. K. Balam, R. Jain, J. S. Alaric, B. Pattanaik, and T. B. Ayele, «Renewable energy integration of IoT systems for smart grid applications», in 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), 2023, pp. 374–379. DOI: 10.1109/ICESC57686.2023.10193428.

[20] R. Nalagandla and B. Pattanaik, «IoT enabled hybrid renewable energy system for street light applications», in 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), 2023, pp. 1464–1468. DOI: 10.1109/ICAISS58487.2023.10250645.

[21] J. Lourenço, N. Neves, F. Reis, and N. Valente, «Developing a platform for energy efficiency monitoring», Renew. Energy Power Qual. J., vol. 10, n.o 9, 2012. DOI: https://doi.org/10.24084/repqj10.649.

[22] J. Lourenço, E. Zanghi, J. Morais, N. Neves, C. Vasques, and F. Figueiredo, «The relevance of IT Security awareness in Renewable Energy facilities», Renew. Energy Power Qual. J., vol. 20, n.o 4, 2024. DOI: 10.24084/repqj20.357.
[23] K. Bhat, V. Sundarraj, S. Sinha, and A. Kaul, «IEEE Cyber Security for the Smart Grid», IEEE, Piscataway, NJ, USA, set. 2013. DOI: 10.1109/IEEESTD.2013.6613505.
[24] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke, and N. Kefalakis, «Scalable and configurable end-to-end collection and analysis of IoT security data: Towards end-to-end security in IoT systems», in 2019 Global IoT Summit (GIoTS), 2019, pp. 1–6. DOI: 10.1109/GIOTS.2019.8766407.
[25] H. Garg e M. Dave, «Securing IoT devices and Securely Connecting the dots using REST API and middleware», in 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1–6. DOI: 10.1109/IoT-SIU.2019.8777334.
[26] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, «An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security», IEEE Internet Things J., vol. 7, n.o 10, pp. 10250–10276, 2020. DOI: 10.1109/JIOT.2020.2997651.
[27] M. S. Sharbaf, «IoT driving new business model, and IoT security, privacy, and awareness challenges», in 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), 2022, pp. 1–4.
[28] K. Urunov, S. Vaqqasov, J.-I. Namgung, and S.-H. Park, «Security issues for DTN mechanism of UIoT», at The 18th IEEE International Symposium on Consumer Electronics (ISCE 2014), 2014, pp. 1–3. DOI: 10.1109/ISCE.2014.6884535.
[29] S. Farrell, «Security in the Wild», IEEE Internet Comput., vol. 15, n.o 3, pp. 86–91, May-June 2011.
[30] A. Fatimah, R. Johari, and M. R. Muddassir, «DTN routing: Secure message transmission in border defence system», in 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 440–445. DOI: 10.1109/CCAA.2017.8229896.
[31] V. Priya and B. Sakthisaravanan, «Information centric network for secure data transmission in DTN», at International Conference on Innovation Information in Computing Technologies, 2015, pp. 1–4. DOI: 10.1109/ICIICT.2015.7396101.
[32] F. Almeida and J. Lourenço, «Information centric networks - design issues, principles and approaches», vol. 3, 2012.
[33] T. R. de Oliveira, S. de Oliveira, D. F. Macedo, and J. M. Nogueira, «An adaptive security management model for emergency networks», in 2011 7th Latin American Network Operations and Management Symposium, 2011, pp. 1–4. DOI: 10.1109/LANOMS.2011.6102261.
[34] E. Birrane and S. Heiner, «Security on the edge: The role of autonomy in securing DTNs», in 2023 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), 2023, pp. 23–28. DOI: 10.1109/WiSEE58383.2023.10289340.
[35] B. J. Sipos, «Toward a distributed and autonomous DTN security environment», in 2024 IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT), 2024, pp. 171–180. DOI: 10.1109/SMC-IT61443.2024.00026.
[36] D. O. Rice, «A Proposal for the Security of Peer-to-Peer (P2P) Networks: a pricing model inspired by the theory of complex networks», in 2007 41st Annual Conference on Information Sciences and Systems, 2007, pp. 812–813. DOI: 10.1109/CISS.2007.4298420.
[36] D. O. Rice, «A Proposal for the Security of Peer-to-Peer (P2P) Networks: a pricing model inspired by the theory of complex networks», in 2007 41st Annual Conference on Information Sciences and Systems, 2007, pp. 812–813. DOI: 10.1109/CISS.2007.4298420.
[37] E. L. M. Sammou, «Impact of renewable energy resources on the performance of DTN networks in the context of hierarchical routing tree topology (HRTT)», Procedia Comput. Sci., vol. 236, pp. 185–193, 2024. DOI:10.1016/j.procs.2024.05.020.
[38] J. D. Deng, «Sizing up the batteries: Modelling of energy-harvesting sensor nodes in a delay tolerant network», *arXiv [cs.NI]*, 2022. DOI: 10.48550/arXiv.2210.05316.
[39] V. Chourasia, S. Pandey, e S. Kumar, «Optimizing the performance of vehicular delay tolerant networks using multi-objective PSO and artificial intelligence», Comput. Commun., vol. 177, pp. 10–23, 2021. DOI: 10.1016/j.comcom.2021.06.006.
[40] H. M. Elhalafawy, A. A. Ali, E. M. G. Younis, K. elBahnasy, e M. Medhat Mokhtar, «Evaluation of delay tolerant network routing protocols for data streaming through LEO constellation», Egypt. J. Remote Sens. Space Sci., vol. 26, n.o 3, pp. 557–561, 2023. DOI: 10.1016/j.ejrs.2023.06.005