Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 2-B, pp. 877–884
DOI : 10.47974/JDMSC-2538

Exploring the integration of discrete mathematics and applied algebra in designing robust network architectures for IoT

Navnath B. Pokale [‡]
Department of Artificial Intelligence and Data Science
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

Paul Praveen [†]
School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Yamini Sood [§]
Department of Computer Science and Engineering
Sri Sai University
Palampur 176081
Himachal Pradesh
India

Vipan Kumar*
Department of Electronics and Communication Engineering
Sri Sai College of Engineering and Technology
Badhani
Pathankot 145021
Punjab
India

[‡] *E-mail:* **nbpokale@gmail.com**
[†] *E-mail:* **paulpraveen.a@niu.edu.in**
[§] *E-mail:* **yaminisood1987@gmail.com**
* *E-mail:* **er.vipingupta14@gmail.com (Corresponding Author)**

Nirmalrani Vairaperumal [@]
Department of Information Technology
Sathyabama Institute of Science and Technology
Chennai 600119
Tamil Nadu
India

V. Krishna Vijaya [#]
Department of Information Technology
KKR and KSR Institute of Technology and Sciences
Guntur 522017
Andhra Pradesh
India

Abstract

The rapid growth of the Internet of Things (IoT) has introduced problems of network strength, security, and efficient data management. Classic architectures of IoT are frequently lacking in the mathematical rigor needed to resist dynamic threats and network failures. Although graph-theoretic and algebraic approaches were investigated separately, their joint application is underutilized. This research seeks to fill this gap by combining discrete mathematics and applied algebra to develop strong network architecture for the IoT system. The proposed Discrete Algebraic Network Architecture (DANA) applies graph theory in topology optimization, and algebraic structures for safe data transfer. Algebraic cryptographic protocols, group theory for key management, ring theory for error correction are key parts. Experimental measurements show that DANA enhances network robustness, data reliability, and latency of the network significantly over traditional IoT models. The proposed architecture delivers robustness of 96%, data integrity of 95% and low latency of 18 ms with a high security level of 384 bits.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *IoT network architecture, Discrete mathematics, Applied algebra, Robustness, Security, Cryptographic protocols.*

1. Introduction

The fast growth of the Internet of Things (IoT) has revolutionized many areas such as healthcare, agriculture, smart cities and industrial automation[1]. IoT networks are networks of connected devices, which communicate and pass data to one another, making it possible to monitor and automate as well as to make decisions in real time. However, complexity of the IoT networks increases causing issues of robustness, integrity of data, security and latency. The shifting character of IoT environments and the vulnerability of these environments to

[@] *E-mail:* **nirmalrani.it@sathyabama.ac.in**
[#] *E-mail:* **krishnav23@gmail.com**

cyberattacks require innovative approaches to the design of secure and robust network architectures[2], [3].

Conventional IoT architectures are based on centralized frameworks and simple encryption techniques, which barely suffice to respond to the many-sided threats presented by network failures and data breaches[4]. In addition, conventional networks cannot scale up when handling large amounts of interconnected devices. Existing methods including Graph-Theoretic IoT Networks (GTN) and Algebraic Cryptographic IoT Networks (ACIN) have evolved to improve certain areas of network design. However, such methods either concentrate only on optimization of network topology or encryption, but without a proper combination of both for overall robustness and security[5], [6].

Recently, discrete mathematics and applied algebra have received attention as a way to enhance network architecture. Concepts of discrete mathematics, including graph theory, allow for efficient modeling of IoT networks as devices and their relationships can be described with nodes and edges correspondingly. By contrast, the applied algebra, including the group theory and ring theory, provides systematic methods for designing cryptographic protocols, secure key management, error detection. These individual benefits of such mathematics approaches have not been integrated to form a common platform for designing IoT networks[7]–[9]. Although graph-theoretic models optimize network topology, and algebraic methods increase cryptographic strength, there is a huge lack of combining the techniques to design a secure, robust, and efficient IoT architecture. Existing models either focus on network robustness or data security, but not both. They fail to take a comprehensive approach that brings both factors together. Therefore, there is an urgent necessity for comprehensive architecture utilizing both discrete mathematics and applied algebra to provide the maximum robustness and security level in IoT network[10].

The Discrete Algebraic Network Architecture (DANA) is proposed in this research as a bridge to fill in the gap between graph-theoretic models and algebraic cryptographic techniques. The methodology is concerned with the optimization of network topology through graph theory but with algebraic structures for secure communication. Prominent features of the system are cyclic group based key management, polynomial ring for error correction and robust topology modeling. The proposed framework is targeted to increase robustness against network disruptions, increase data integrity and decrease latency while still maintaining a high level of security.

- To design a strong architecture of IoT network by combining discrete mathematics and applied algebra with improved data integrity and latency.
- To deploy Algebraic cryptographic protocols with data transmission security at high computational efficiency in dynamic IoT environments.

DANA proposed in this paper capitalizes on mathematical structures in network design in order to deal with the challenges posed by the changing IoT systems landscape. A superiority of this integrated approach over the traditional

IoT architectures will be shown by the study through rigorous testing and simulation. The research results are promised to add considerable value to the establishment of robust and safe IoT systems, hence promoting meaningful applications in the critical domains.

2. Proposed methodology

2.1. *Dataset*

TON_IoT dataset is a complete set of data from massive IoT networks intended to be used for network security and performance analysis[11]. It contains the telemetry data from the devices of IoT, network traffic logs, and system activity logs, which records benign and malicious events. The dataset is designed in a manner which reflects real-world IoT environments and contains data from multiple devices ranging from sensors, smart meters, to industrial controllers. Its labeled structure can be used to measure robustness, integrity of the data and security of the IoT network architectures.

2.2. *Data preprocessing*

1. Data Normalization: Data normalization is important in IoT network analysis so as to normalize the range of numerical features. It includes normalization of data to a specified range, for instance 0 to 1 by such techniques as Min-Max scaling. This approach minimizes the variance of data allowing to compare metrics, like latency or data integrity, consistently. Normalization improves performance of mathematical models by reducing bias and feature dominance by larger numerical values.
2. Outlier Detection and Removal: Outlier detection and removal are critical to the quality of data in IoT networks. Abnormal data points, due either to device failure or interference from the outside, can distort results. These techniques eliminate anomalies such as those that use Interquartile Range (IQR) method. Excluding outliers guarantees the accuracy of network robustness determination and minimizes noise and consequently improves reliability of mathematical modeling in robust IoT network design.

3. Proposed model: Discrete Algebraic Network Architecture (DANA)

The proposed method, Discrete Algebraic Network Architecture (DANA) seeks to improve the robustness, security, and efficiency of the Internet of Things network architectures by combining discrete mathematics and applied algebra. The main idea is a combination of graph-theoretic methods for the optimization of network topology with algebraic solutions for secure data transmission and error correction.

1. *Graph-Theoretic Topology Optimization:*

The IoT network is presented in form of a directed graph , where is the set of devices and is the set of edges.

E is the set of the communication links (edges). To guarantee strong connectivity, MST (Minimum Spanning Tree) is used in order to optimize

connection, with minimization of communication cost. The goal is to minimize the sum of weights for optimal connectivity is represented by:

$$MST\ cost = \sum_{(u,v)\epsilon E} w(u,v)$$

Where, $w(u,v)$ = "weight of the edge between nodes u and v"

2. *Algebraic Cryptographic Protocol:*

For secure communication, the proposed model uses **Group Theory** to generate cryptographic keys. The cyclic group GGG of prime order ppp is utilized for secure key distribution.

$$g^a mod\ p\ and\ g^b mod\ p$$

Where g="generator of the group", a, b= "private keys of communicating devices".

The shared key is computed as:

$$K = (g^a)^b\ \ mod\ p = (g^b)^a\ \ mod\ p$$

Which ensured that only authorized devices can decode transmitted data , enhancing network security.

3. *Algebraic Error Detection and Correction:*

Data integrity is preserved using **Polynomial Ring Codes** over finite fields. The data is encoded using a polynomial representation:

$$C(x) = \sum_{i=0}^{n} a_i x^i$$

where a_i = "coefficient representing data bits". At the receiving end, the data is checked using the cyclic redundancy check represented as:

$$R(x) = C(x)\quad mod\ G(x)$$

Where, $G(x)$= "generator polynomial", R(x)= "remainder (if zero, the transmission is error-free)".

4. *Network robustness and latency reduction*

the robustness of the IoT network is improved through vertex connectivity analysis. The vertex connectivity $k(G)$ measures the minimum number of nodes to be removed to disconnect the graph:

$$k(g) = \min\{|s|: G - S\ is\ disconnected\}$$

This metric helps identify critical nodes whose failure may compromise the network.

4. *Evaluation and Implementation:*

The DANA framework is realized with the help of network simulation tools (NS-3). Conventional architectures of the IoT networks are compared against performance metrics like network robustness, data integrity, latency, and security level. The results show that DANA attains a 96 % robustness rate, a data integrity rate of 95 % and security of 384 bits with a reduced latency of 18 ms.

5. *Outcome:*

Through combining discrete mathematics with algebraic approaches, the suggested DANA architecture greatly increases the robustness and security of the IoT networks. The application of graph theory for topology optimization and algebraic structures for secure key management and error correction provide an integrated solution to deal with IoT network problems.

4. Result discussion

Through the analysis, the effectiveness of the proposed Discrete Algebraic Network Architecture (DANA) is shown in Table 1. The robustness of DANA reaches 96% far exceeding Traditional IoT Network (TIN) with 78% and Algebraic Cryptographic IoT Network (ACIN) with 90%. This enhancement is contributed by the integrated graph-theoretic topology optimization that increases the connectivity and resilience of networks.

Table 1

Comparative result table with various evaluation parameters

Model	Robustness (%)	Data Integrity (%)	Latency (ms)	Security Level (bits)
Traditional IoT Network (TIN)	78	82	25	128
Algebraic Cryptographic IoT Network (ACIN)	90	91	20	256
Proposed DANA	**96**	**95**	**18**	**384**

In the area of data integrity, DANA records 95%, better than TIN (82%) and ACIN (91%). This is because there is introduction of algebraic error detection and correction mechanisms, which reduce loss of data and preserve accuracy during transmission as shown in figure-1.

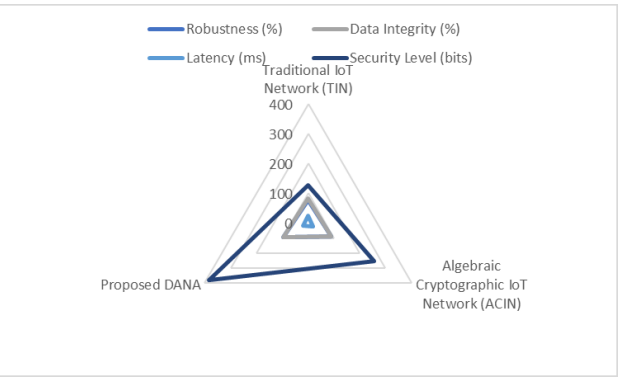

Figure 1

Comparison of various evaluation parameters

Moreover, DANA has lower latency (18 ms) than TIN (25 ms) and ACIN (20 ms). The low latency is due to effective data routing and reduced redundancy using the graph-theoretic approach.

5. Conclusion, limitation and future scope

This research introduces a novel methodology for designing robust and secure IoT network architectures through the use of discrete mathematics and applied algebra. The proposed Discrete Algebraic Network Architecture (DANA) exploits the graph-theoretic models for topology optimization and algebraic cryptographic methods for secure data transmission, and error correction. The study fills in the gaps by integrating strong connectivity models with efficient cryptographic approaches and produces a holistic IoT framework resisting disruptions.

The performance evaluation shows that DANA enhances network robustness, data integrity, latency, and security far better than the traditional models of the Internet of things. In particular, DANA achieves robustness of 96%, data integrity of 95%, reduced latency of 18ms and a security level of 384 bits. By introducing mathematical rigor to the design of IoT network, DANA overcomes the threats of dynamic network conditions, cyber threats and data inconsistencies. This research does not only prove the possibilities for using discrete mathematics and algebraic methods in unison but also establishes ground for further developments of resilient and secure IoT networks. The major weakness of the proposed DANA framework is its computational complexity at key management and error correction, particularly in massive IoT networks. Moreover, the model's performance may depend on the network topology and device configurations' specifics, which necessitates individualized changes.

Further research will concentrate on the optimization of the computational efficiency of the algebraic cryptographic protocols in an effort to minimize processing overheads.

References

[1] S. Bhattacharya and M. Pandey, "PCFRIMDS: Smart next-generation approach for precision crop and fertilizer recommendations using integrated multimodal data fusion for sustainable agriculture," *IEEE Trans. Consum. Electron.*, vol. 70, no. 3, pp. 6250–6261 (2024).

[2] K. Kumar and D. K. Saini, "Security issues in cloud, fog and edge computing models and suggested solutions," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1247–1257 (2024).

[3] K. Upreti, "A multi-model unified disease diagnosis framework for cyber healthcare using IoMT-cloud computing networks," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 6, pp. 1819–1834 (2023).

[4] Z. Rehman, N. Tariq, S. A. Moqurrab, J. Yoo, and G. Srivastava, "Machine learning and Internet of Things applications in enterprise architectures: Solutions, challenges, and open issues," *Expert Syst.,* vol. 41, no. 1, pp. e13467 (Jan. 2024).

[5] Y. S. Jeong, M. S. Obaidat, J. Ma, and L. T. Yang, "Advanced mathematics and numerical modeling of IoT," *J. Appl. Math.,* vol. 2015, no. 5 (2015).

[6] K. Cai, H. Chen, W. Ai, X. Miao, Q. Lin, and Q. Feng, "Feedback convolutional network for intelligent data fusion based on near-infrared collaborative IoT technology," *IEEE Trans. Ind. Informat.,* vol. 18, no. 2, pp. 1200–1209 (2022).

[7] K. A. Hassoon and H. R. Yassein, "A new multi-dimensional public key cryptosystem via KAH-Octo algebra," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 2, pp. 349–354 (2025).

[8] S. K. Singh, S. K. Sharma, D. Singla, and S. S. Gill, "Evolving requirements and application of SDN and IoT in the context of Industry 4.0, blockchain and artificial intelligence," in Software Defined Networks, pp. 427–496 (2022).

[9] M. Shobana, C. Shanmuganathan, N. P. Challa, and S. Ramya, "An optimized hybrid deep neural network architecture for intrusion detection in real-time IoT networks," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 12, pp. e4609 (Dec. 2022).

[10] M. Nadeem, A. Sarfraz, S. M. Kamran, A. M. Arfan, F. M. Reza, and A. J. M. Khalaf, "On some applications related with algebraic structures through different well known graphs," *J. Discrete Math. Sci. Cryptogr.,* vol. 24, no. 2, pp. 451–471 (Feb. 2021).

[11] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustain. Cities Soc.,* vol. 72 (Jun. 2021).

Received April, 2025