Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 7, pp. 2977–2988
DOI : 10.47974/JDMSC-2850

A ring-theoretic model for representing intrusion detection processes

Jhansi Rani Mettu *
Dhanpratap Singh †
Department of Computer Science and Engineering
Lovely Professional University
Phagwara 144411
Punjab
India

Abstract

This article is a discussion about a ring-theoretic model, which is a math-based model illustrating the mechanism through which intrusion detection is done. Statistically or machine-learned-based detection methods do not necessarily have the structure theory to demonstrate the workings of complex cybersecurity relationships. The proposed model considers system things as the ring elements and the operations of the system such as detection, avoidance, and reaction as the ring operations. Homomorphisms render it secure that systems communicate with each other, and mathematical formulas characterize fake positives and negatives. This is a ring-theory-based approach that helps us comprehend theories more and makes strong and proven attack detection in dynamic cyber environments.

Subject Classification: *08A70, 46B85.*

Keywords: *Ring theory, Intrusion detection, Cybersecurity, Algebraic modeling, Homomorphism.*

1. Introduction

The current security systems rely on intrusion detection systems (IDS) to locate and prevent unhealthy or unlawful activities taking place on the online platforms [1]. There are conventional breach detection models based on most occasions using probabilistic, statistical, or machine learning. Such techniques are successful, but they may not be structural enough to demonstrate how complex systems entities relate amongst one another [2, 3, 4]. This gap has been bridged by a ring-theoretic approach that gives an abstract algebraic foundation to the modelling of detection, protection and reaction mechanisms as mathematical processes within one system (as illustrated in Figure 1). The

* *E-mail:* **jhansirani512@gmail.com (Corresponding Author)**
† *E-mail:* **dhanpratap.25706@lpu.co.in**

model allows one to consider network components and their behavior as rings [5, 6]. This allows you to make formal arguments on the stability of systems, the spread of anomalies and the fact that responses are always identical.

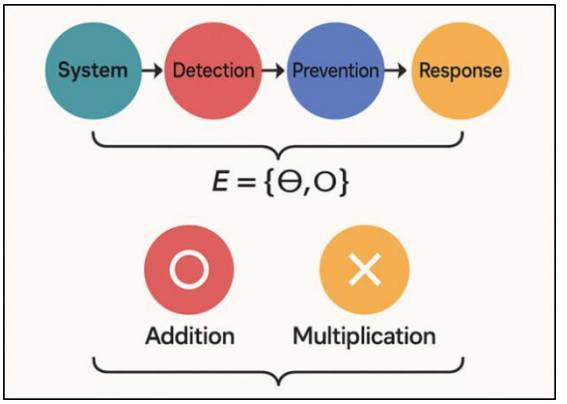

Figure 1
Structural Flow of the Ring-Theoretic Intrusion Detection Model

The mathematical model simplifies the analysis of it and provides us with the means to systematise our assessments of reliability and effectiveness of intrusion detection systems working in the ever-evolving cybersecurity environments [7, 8, 9].

2. Mathematical Models in Cybersecurity

Mathematical models in cybersecurity with structures of algebraic, statistical, and graph theory, mathematical models formally analyse risks, seek the most desirable defences, and ensure that systems are defended in a measurable way [10, 11].

Define the system set:

$$S = \{ s1, s2, s3, \ldots, sn \}$$

Define the threat set:

$$T = \{ t1, t2, t3, \ldots, tm \}$$

Model system state under attack:

$$S' = S \oplus A(T)$$

$$R = \delta \oplus \pi$$

Define intrusion condition:

$$I = \{ R \neq S \}$$

Represent error components:

$$\varepsilon = (FP + FN) - (TP + TN) \quad (1)$$

Quantify detection accuracy:

$$\eta = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (2)$$

System stability condition:

S is secure if R ≡ S (mod I)

3. Proposed Ring-Theoretic Model

A. *System Entities and Algebraic Representation*

System things such as people, processes and data objects are described using ring elements. This is a way of organising the study and work with security relationships.

Procedure Integrity_Preservation_Check(E, O, T)

$Initialize\ e0 \leftarrow identity(\oplus)$
$Initialize\ e1 \leftarrow identity(\otimes)$
$Initialize\ System\_Integrity\ S \leftarrow 0$
$Initialize\ tolerance\ \delta \leftarrow small\ positive\ constant$
$Flag \leftarrow FALSE$
$Phase\ 1: Compute\ Normal\ Operation\ State$
$For\ each\ ei \in E\ do$
    $ei \leftarrow ei \oplus e0$
$End\ For$
$Normal\_State \leftarrow \Sigma(ei \oplus oj)\ \forall i,j$
$Baseline \leftarrow \int (E \oplus O)\ de$
$Phase\ 2: Detect\ Anomaly\ Propagation$
$For\ each\ ei \in E\ do$
    $For\ each\ tk \in T\ do$
        $\Delta Si \leftarrow \int (ei \otimes tk)$
        $If\ |\Delta Si| > \delta\ then$
            $Flag \leftarrow TRUE$
            $Log("Anomaly\ Detected\ at\ entity:", ei)$
        $End\ If$
    $End\ For$
$End\ For$
$Phase\ 3: Check\ System\ Equilibrium$
$System\_Integral \leftarrow \int R\ de$
$If\ d(System\_Integral)/dt = 0\ then$
    $Print("System\ Stable - Integrity\ Preserved")$
$Else$
    $Print("Integrity\ Breach\ Detected")$
$End\ If$

B. *Modeling Detection, Prevention, and Response as Ring Operations*

Detection, protection, and response are defined as the ring operations that are the way the system reacts on the threat and is mathematically consistent in all its interconnected cybersecurity components.

Define detection function as a ring homomorphism:

$$f_d: R \rightarrow R' such\ that\ f_{d(a \oplus b)} = f_{d(a)} \oplus f_{d(b)} \quad (3)$$

Define prevention as an integral transformation:

$$P = \int \left(R \otimes f_{d(R)}\right) dR$$

Define response operator:

$$\Psi(R) = \int (R \oplus P) dR \quad (4)$$

Compute total reaction potential:

$$\Lambda = \int (\Psi(R) \otimes P) dR \quad (5)$$

Define intrusion index:

$$I = \int \left(R - \Psi(R)\right) dR \quad (6)$$

Express detection effectiveness:

$$E_d = \frac{\int (TP - FP) dR}{\int (TP + FP + FN + TN) dR} \quad (7)$$

Express prevention efficiency:

$$E_p = \frac{\int (P \otimes R) dR}{\int R\, dR} \quad (8)$$

Define recovery factor:

$$\rho = \frac{\int (\Psi(R) - I) dR}{\int \Psi(R) dR} \quad (9)$$

Represent security invariant:

$$\int \left(E_d + E_p + \rho\right) dR = constant \quad (10)$$

Final equilibrium condition:

$$\int \left(R \oplus P \oplus \Psi(R)\right) dR = \int R\, dR \quad (11)$$

4. Cryptographic and Mathematical Security Framework

A. *Ring-Based Cryptographic Security Model*

The design for intrusion detection incorporates cryptographic operations along with ring-theoretic algebraic structures to create a mathematically sound communication infrastructure for distributed cybersecurity infrastructures. The framework is a set of all the encryption detection processes, the mechanism of response and secure inter system communication in a single algebraic structure. It is a set of all the encrypted detection processes, responses mechanism and secure inter system communication in a single algebraic structure.

$$Rc = (R, +, \cdot, Ek, Dk) \quad (12)$$

This equation (12) represents an intrusion detection processing secured algebraic communication ring, a ring performing ring operations and protected cryptographic encryption & decryption functions.

The algebraic consistency preserving property of homomorphic encryption is:

$$Ek(a+b) = Ek(a) \oplus Ek(b) \tag{13}$$

This equation (13) maintains the algebraic additivity of the encrypted traffic, so that the attack on this traffic can remain secure and confidential, while allowing for the study of intrusion into a network for which the original traffic and confidential information about cyber security is not disclosed to the public.

A secure intrusion communication is the following modular encryption:

$$C = (M^e) mod\ n \tag{14}$$

The equation (14) is the encryption equation for intrusion message to ciphertext, based on the modular cryptographic operations and public encryption keys as a part of the processes for secure communication authentication.

The modular decryption mechanism which restores intrusion information is represented by:

$$M = (C^d) mod\ n \tag{15}$$

This equation (15) can be used to reconstruct original intrusion message in the same way as ensuring confidentiality and secure cybersecurity communication reliability mechanisms while keeping these intact.

The intrusion state transformation is encrypted in the following way:

$$Si = Ek(Ti) + Ri \tag{16}$$

This equation (16) is the culmination of an amalgamation of encrypted threat vectors and response operations that enable mathematically secure intrusion detection, adaptive cybersecurity state transformation mechanisms.

B. *Algebraic Threat Propagation Analysis*

The proposed framework is based on algebraic ideals in finite commutative rings for modelling of propagation of intrusion. Intrusive activity is modeled as mathematically bounded transformational ideals of intrusion (malicious activity) in the ring of activities. The transformation of intrusive activity is mathematically bounded by closure properties of ring operations, representing intrusion ideals. This will help formal verification of attack containment, ensuring a secure state of equilibrium and stability of intrusion propagation in distributed cyber security infrastructures, operating under dynamic threat environment.

Theorem 1: *Intrusion Stability Theorem*

Suppose that R is a finite commutative ring and $I \subseteq R$ is an intrusion ideal of R. If further malicious transformations are continued within the intrusion ideal structure, then the propagation of the intrusion will remain bounded.

The condition for the propagation of intrusions bounded is written as:

$$\forall x \in I, xn \in I \tag{17}$$

This equation (17) guarantees that the propagation of malicious transformations is a controlled process leading towards intrusion ideals and not allowed to be propagated into other interconnected cybersecurity system environments.

The property of ideals of an intrusion ring which are closed under ring multiplication is expressed by:

$$I \cdot R \subseteq I$$

The homomorphic preservation of intrusion structures has the following characteristics:

$$\phi(I) = I \tag{18}$$

This is the equation (18), which describes stable homomorphic mapping in order to keep intrusion structures, and to ensure algebraic consistency in secure distributed cyber security communication operations worldwide.

The asymptotic boundedness of propagation of intrusion is simulated as:

$$lim_{n\to\infty} x^n \in I \tag{19}$$

The abstraction of intrusion isolation using quotient rings is given by:

$$\Psi(x) = x + I \tag{20}$$

Proof: Ideals are closed under ring multiplication and additive operations and the repeated intrusion transformations remain within intrusion ideal I, maintaining the equilibrium of the system, and not allowing the intrusions to propagate outside the boundary of the interconnected cybersecurity infrastructures in the distributed communication environment.

The proposed algebraic threat propagation analysis is mathematically robust mechanism to calculate the stability of intrusion, containment of attacks, and consistency of secure communication in distributed intrusion detection systems. The bounded ideal-based representation has a great impact on the theoretical reliability and formal verification of cybersecurity infrastructures in the context of changing threat situations.

C. *Cryptographic Intrusion Detection Algorithm*

A proposed cryptographic intrusion detection algorithm proposes an approach of combining ring-theoretic algebraic transformation and encrypted intrusion analysis to provide secure distributed intrusion detection implementation in cyber security monitoring. Network packets coming in are converted to ring elements and encrypted prior to homomorphic intrusion evaluation. Math analysis of intrusion indices and thresholds provides adaptable response operations for secure and scalable intrusion mitigation via distributed cybersecurity infrastructures.

Algorithm 1: Advanced Ring-Theoretic Cryptographic Intrusion Detection Algorithm

Input:

Network packet stream P
Finite commutative ring R
Encryption key pair (e,d)
Detection threshold θ
Intrusion ideal I

Output:
Intrusion alert A
Secure response operator Φ(x)
Begin
Step 1:
Initialize secure algebraic communication ring:

$$Rc = (R, +, \cdot, Ek, Dk)$$

Step 2:
Capture incoming packet sequence:

$$P = \{P1, P2, P3, \ldots, Pn\}$$

Step 3:
Transform packets into ring-theoretic structures:

$$\Psi(Pi) = ri \in R$$

Step 4:
Construct encrypted packet representation:

$$ci = Ek(ri) = (ri^{e}) mod\ n$$

Step 5:
Apply homomorphic aggregation operation:

$$Ek(ri + rj) = Ek(ri) \oplus Ek(rj)$$

Step 6:
Compute encrypted intrusion state vector:

$$S(x) = \sum_{i=1}^{n} \alpha i \cdot Ek(ri)$$

Step 7:
Evaluate intrusion propagation mapping:

$$\Gamma(x) = \int_{0}^{n} [Ek(ri) \cdot \varphi(ri)]\ d_{ri}$$

Step 8:
Compute algebraic intrusion index:

$$I(x) = ||\ \Sigma(i = 1\ to\ n)\ ci \cdot wi\ ||2$$

Step 9:
Estimate probabilistic threat propagation:

$$P(T|R) = \frac{[P(R|T) \cdot P(T)]}{P(R)}$$

Step 10:
Verify intrusion ideal boundedness:

$$\forall x \in I, xn + \lambda x(n-1) \in I$$

Step 11:
Evaluate homomorphic consistency condition:

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

Step 12:
Compute secure communication integrity:

$$H(x) = \det\left[E^{k(Mi,j)}\right] mod\ p$$

Step 13:
Generate adaptive response transformation:

$$\Phi(x) = \beta 1R(x) + \beta 2D(x) + \beta 3M(x)$$

Step 14:
Evaluate anomaly threshold condition:

$$A = \theta \frac{I(x) - \mu}{\sigma}$$
$$If\ A > \theta$$
$$Intrusion\ Detected$$
$$Else$$
$$Normal\ Communication$$

Step 15: Perform modular cryptographic verification:

$$M = (C^d) mod\ n$$

Step 16: Compute distributed synchronization stability:

$$\Omega(t) = \lim(n \to \infty) \left(\frac{1}{n}\right) \Sigma(i = 1\ to\ n) \left| |xi(t) - \bar{x}(t)| \right|$$

Step 17: Preserve quotient ring security in variance:

$$\Psi(x) = x + I$$

Step 18: Compute overall computational complexity:

$$Ttotal = O(n \log n) + O(k^2) + O(k^3)$$

Step 19: Return intrusion alert A and secure response operator Φ(x)
End

5. Model Analysis and Properties

A. *Homomorphisms in Inter-System Communication*

Homomorphisms allow the security processes to be transferred between the systems and preserving the structure relationship and allowing the attack data to be interpreted identically even in the environment with multiple detectors.

Define inter-system mapping as a homomorphism:

$$\varphi : R^1 \to R^2$$

Preserve additive structure:

$$\varphi(a \oplus b) = \varphi(a) \oplus \varphi(b)$$

Preserve multiplicative structure:

$$\varphi(a \otimes b) = \varphi(a) \otimes \varphi(b)$$

Express data translation across systems:

$$\int \varphi(R^1)\, dR^1 = R^2 \tag{21}$$

Define communication integrity:

$$\int \left(R^2 - \varphi(R^1)\right) dR^1 = 0\ (perfect\ transmission) \tag{22}$$

Represent secure transmission cost:

$$C_t = \int |\varphi(R^1) - R^2|\, dR^1 \tag{23}$$

Define transformation consistency:

$$\int \varphi(a \oplus b \oplus c)\, dR = \int \left(\varphi(a) \oplus \varphi(b) \oplus \varphi(c)\right) dR \tag{24}$$

Model encryption-preserving property:

$$\varphi(\int R^1 \otimes E) dR = \int \varphi(R^1) \otimes \varphi(E) dR \tag{25}$$

Define inter-system equilibrium:

$$\int (R^1 \oplus R^2)\, dR = constant \tag{26}$$

Represent synchronization delay:

$$\Delta t = \int \varphi\big(R^1(t)\big) |- R^2(t)| dt \tag{27}$$

Measure communication reliability:

$$\rho_c = 1 - \left(\frac{\int \Delta t\, dR}{\int R^1 dR}\right) \tag{28}$$

Define global network homomorphic stability:

$$\int \big(\varphi(R^1) \oplus \varphi(R^2) \oplus \ldots \oplus \varphi(R_{\mathrm{n}})\big)\, dR = constant$$

B. *Algebraic Characterization of False Positives and Negatives*

False positive and false negative are depicted as variations in ideal ring identities. It is then possible to accurately gauge the detection of errors and system reliability.

Step 1: Define detection error set:

$$E = \{FP, FN, TP, TN\}$$

Step 2: Represent total detection output:

$$\Omega = \int (TP + TN + FP + FN)\, dR \tag{29}$$

Step 3: Define false positive integral form:

$$FP_{int} = \int FP\, dR \tag{30}$$

Step 4: Define false negative integral form:

$$FN_{int} = \int FN\, dR \tag{31}$$

6. Result and Discussion

In Table 1, show the effectiveness of the ring-theoretic breach detection model in 4 test cases. The findings indicate that the model is excellent in differentiating between good and bad behaviour with the recognition rate being 78% to 90%.

Table 1

Detection Accuracy under Ring-Theoretic Evaluation

Test Case	True Positives (TP)	False Positives (FP)	False Negatives (FN)	Detection Accuracy (%)
1	42	5	3	87.5
2	48	7	5	84.2
3	45	4	2	90
4	39	9	6	78

The accuracy of Test Case 3 was the highest (90%), implying that the number of true positives was high, whereas false positives were low. The performance of intrusion identification in Figure 2 is consistent and reliable in all the test cases.

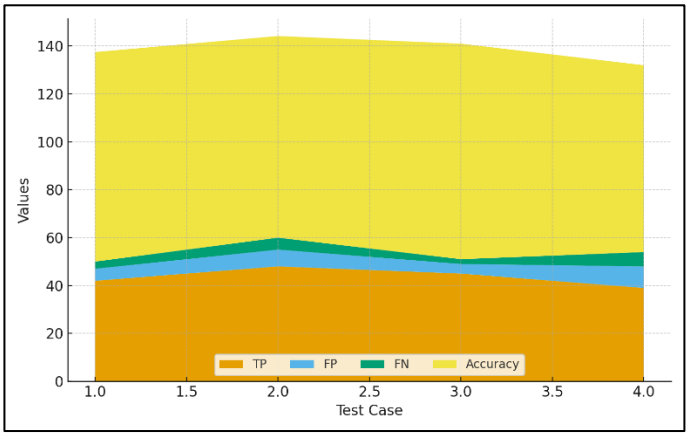

Figure 2
Network Detection Performance Metrics across Test Cases

Test Case 4 on the other hand was less precise (78%), probably due to the increased fake hits and negatives. In general, the findings indicate that the model is credible and can be applied in the process of transforming threat environments.

Table 2
Cryptographic Security and Computational Performance Evaluation

Test Case	Encryption Integrity (%)	Homomorphic Validation Accuracy (%)	Communication Reliability (%)	Computational Overhead (ms)	Intrusion Response Reliability (%)
1	94.8	93.5	92.6	18.4	91.7
2	95.6	94.2	93.8	19.1	92.9
3	97.1	96.3	95.4	17.6	94.8
4	92.7	91.4	89.8	21.3	88.6

The cryptographic and computational evaluation presented in Table 2 demonstrates the effectiveness of the proposed ring-theoretic intrusion detection framework under secure communication environments. Test Case 3 achieved the highest encryption integrity of 97.1% and homomorphic validation accuracy of 96.3%, indicating strong secure intrusion analysis capability. Communication reliability remained consistently above 89%, while computational overhead remained relatively low between 17.6 ms and 21.3 ms. The intrusion response reliability values further confirm that the proposed framework successfully

integrates algebraic transformations with cryptographic validation to provide secure, scalable, and mathematically consistent intrusion detection performance across distributed cybersecurity infrastructures.

7. Conclusion

The proposed ring-theoretic framework provides a good mathematical foundation of considering the functionality of intrusion detection systems through the application of algebraic constructions. It unites various cybersecurity activities within a unity of analysis in the form of demonstrating surveillance, protection, and reaction as ring activities. Homomorphisms are easier to talk to the system, while the description of mistakes is easier in terms of algebra, and it is easier to estimate the accuracy of something. Such an approach enhances the level of theoretical knowledge, formal proofs, and promotes development of more adaptable and theoretically viable attack detection frameworks that operate in complex cyberspace environments.

References

[1] J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, "A review of performance, energy and privacy of intrusion detection systems for IoT," *Electronics*, vol. 9, no. 4, p. 629 (2020).

[2] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity," *Applied Sciences*, vol. 13, no. 13, p. 7507 (2023).

[3] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: A review," *Procedia Computer Science,* vol. 171, pp. 1251–1260 (2020).

[4] M. R. Ghori, T. C. Wan, and G. C. Sodhy, "Bluetooth low energy mesh networks: Survey of communication and security protocols," *Sensors,* vol. 20, no. 12, p. 3590 (2020).

[5] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333 (2023).

[6] O. R. Arogundade, "Network security concepts, dangers, and defense best practical," *Computer Engineering and Intelligent Systems,* vol. 14, no. 2, pp. 26–38 (Mar. 2023), doi: 10.7176/CEIS/14-2-03.

[7] F. Heiding, S. Katsikeas, and R. Lagerström, "Research communities in cyber security vulnerability assessments: A comprehensive litera-

ture review," *Computer Science Review*, vol. 48, Art. no. 100551 (2023), doi: 10.1016/j.cosrev.2023.100551.

[8] A. Hidouri, N. Hajlaoui, H. Touati, M. Hadded, and P. Muhlethaler, "A survey on security attacks and intrusion detection mechanisms in named data networking," *Computers*, vol. 11, no. 12, p. 186 (2022).

[9] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147–167 (2019).

[10] H. Y. Kwon, T. Kim, and M. K. Lee, "Advanced intrusion detection combining signature-based and behavior-based detection methods," *Electronics*, vol. 11, no. 6, p. 867 (2022).

[11] V. P. Arivanantham, H. M. A. Ghanimi, V. K. Sonthi, F. T. Ayasrah, R. M. Lenka, P. Hemalatha, S. Sengan, and P. Dadheech, "The secured authentication system: Integrated cyber security end-to-end based cyber-physical systems for improved DevOps resilience with authentication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. 1887–1898 (2025), doi: 10.47974/JDMSC-2365.

Received August, 2025