PeerJ Preprints NOT PEER-REVIEWED

Data Security Analysis Based On Blockchain Recurrence Qualitative Analysis (BRQA)

M. A.El-dosuky [1], Gamal H. Eladl [2]

[1] Computer Science Department, Faculty of Computers & Info, Mansoura University, Egypt
[2] Information Systems Department, Faculty of Computers & Info, Mansoura University, Egypt

Corresponding Author:
M. El-dosuky [1]
Faculty of Computers & Info, Mansoura University,P.O. 35516, Egypt
Email address: mouh_sal_010@mans.edu.eg

Abstract

There is no doubt that the Blockchain has become an important technology that imposes itself in its use. With the increasing demand for this technology it is necessary to develop and update techniques proposed to deal with other technologies, especially in the field of cyber-security, which represents a vital and important field. This paper discussed the integration of Recurrence Qualitative Analysis (RQA) technology with the blockchain as well as exciting technical details of RQA operation in increasing Blockchain security. This paper found significant improvements, remarkable and differentiated compared to previous methods.

Introduction

There is no doubt that the Blockchain has become an important technology that imposes itself in its use. With the increasing demand for this technology it is necessary to develop and update techniques proposed to deal with other technologies, especially in the field of cyber security, which represents a vital and important field.

Intrusion detection systems (IDSs) are divided into a dichotomy of anomaly-based and signature-based (AXELSSON 1998). For a detailed survey of IDS types, refer to (LIAO et al. 2013). Detecting denial of service (DoS) can be detected by many ways by Gyanchandani et al. (2012). But Raut and Singh (2014) proved the limitation of those ways, when considering network nonlinear dynamic behavior (Palmieim and Fiore, 2010). This dynamicity manifests itself as recurrence (Palmieim and Fiore, 2010).

Recurrence Quantification Analysis (RQA), proposed by (ECKMANN 1995), is a powerful nonlinear tool in analyzing such behavior (Weber and Marwan, 2015; Righi and Nunes, 2018). RQA has many features such as entropy (H) determinism (Ɗ), Laminarity (Ŀ). RQA is armed with recurrence plot (RP) that is a powerful visualiza-tion tool.

This paper presents the integration of Recurrence Qualitative Analysis (RQA) technology in the blockchain.

The remaining of this paper is decomposed as follows. Section2 is for related works and theoretical foundation of the RQA. Section3 provides proposed system. Section4 presents the results and its validation. Conclusion and recommendations for future work are at the end of the paper.

Previous Work

This section is for related works and theoretical foundation of the RQA.

1.1 Related works

RQA is successful in medical field. For instance, Moridani et al (2015) scrutinized heart rate using the RQA. Schlenkeri, Funda & Nedelka (2011) scrutinized heart rate too.
Regarding security, Wu et al. (2011) proposed a decision-tree malicious attack classifier. Many studies focus on studying non-linear aspects of a network (Palmieri and Fiore, 2010 and Jeyanthi et al., 2014). However, some focused on the visualization RQA presents (Jeyanthi et al., 2014 and Jeyanthi et al., 2011) .
Determinism and entropy help in predicting the behavior (Fabretti and Ausloos, 2005). Phase-space trajectory is reconstructed based on observations (Kantz et al., 2002; Abarbanel, 1997).

1.2 RQA foundations

A recurrence matrix is denoted as:

$$R_{i,j}(\varepsilon)=\theta(\varepsilon - \|\, x_i - x_j \,\|) \qquad (1)$$

where $\vec{x}$ represents the state vector , while θ is a discrete function defined as (*if x >= 0 return 1 else return 0*). The || . || denotes Euclidean norm. The greater the Ɗ, the more predictability is the system. It is calculated as:

$$\text{Ɗ} = \frac{\sum_{l=lmin}^{N} lp(l)}{\sum_{l=1}^{N} lp(l)} \qquad (2)$$

where *l is length of* diagonal, and *P(l)*is the count of diagonal lines with length *l*.
L_{avg} is the mean of all lines diagonally viewed in RP. It is defined as:

$$L_{avg} = \frac{\sum_{l=lmin}^{N} l\,P(l)}{\sum_{l=lmin}^{N} P(l)} \qquad (4)$$

Finally, Shannon entropy is defined as:

$$\mathrm{H} = -\sum_{l=lmin}^{N} p(l) \ln p(l) \qquad (5)$$

Proposed Framework

The proposed operational framework is adapted from (Pfleeger& Pfleeger 2002) by augmenting it with the blockchain component, and adding RQA analysis in the Analysis component.

PeerJ Preprints NOT PEER-REVIEWED

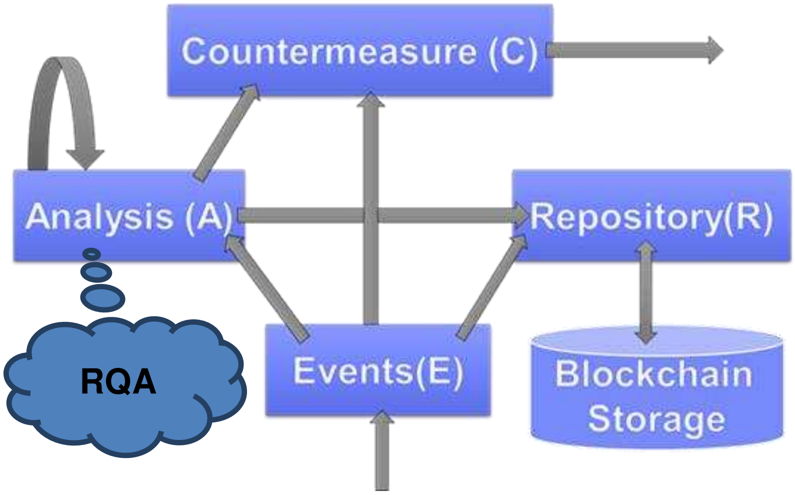

Fig1 modified operational framework (based on Pfleeger& Pfleeger 2002)

Results and Validation

RQA was implemented by Matlab© R2015a on a 32-bit Windows© 7. Results are gained from NSL-KDD dataset (DARPA İntrusion dataset, 1999).

Features selected are those concerning with DoS, Probe, R2L and U2R. But let us focus on DoS, as Table 1 shows its confusion matrix. Thus Accuracy: 0.9964, Precision: 0.9951, and Recall: 0.9967.

Table 1: Confusion matrix for classifying DOS

Test if it is DoS attack	**Attack present**	**Attack absent**
Positive	True Positive (9499)	False Positive (212)
Negative	False Negative (2830)	True Negative (4630)

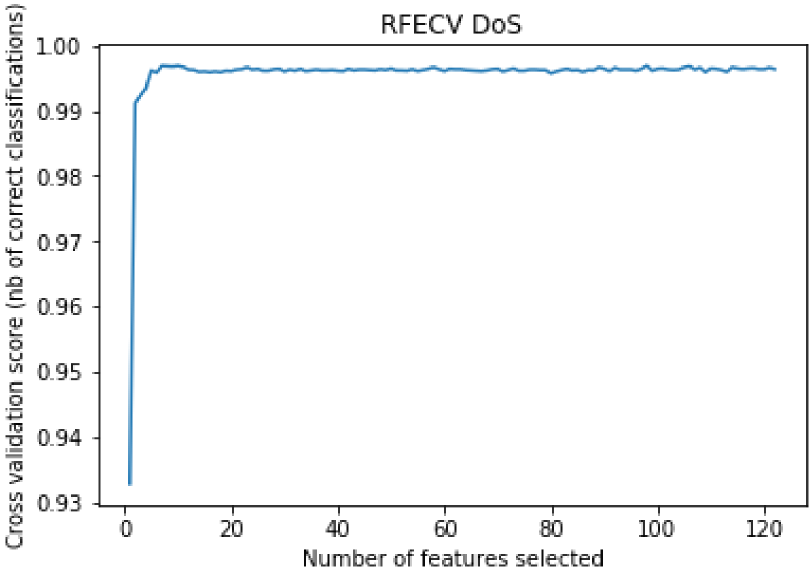

Fig2. Recursive feature elimination with cross-validation(RFECV)

Fig2 shows Recursive feature elimination with cross-validation(RFECV). **Fig3**, shows RP for DoS with threshold ε, DoS Attack has the highest Ɗ, and the highest H and the longest L_{avg}..

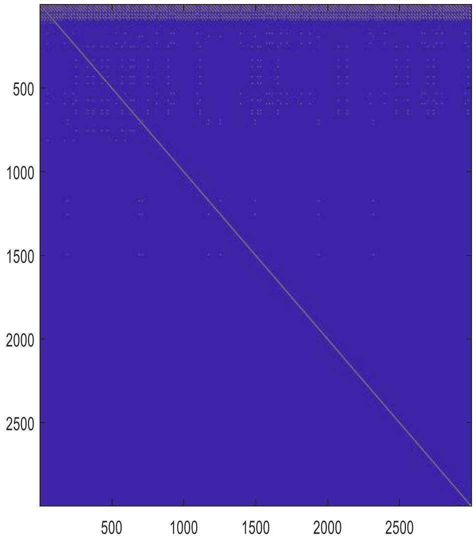

Figure 3: RP for DoS (ε = 0.5)

Conclusion and future work

This paper presents discussed the integration of Recurrence Qualitative Analysis (RQA) technology in the blockchain as well as exciting technical details of RQA operation in increasing Blockchain security. Significant improvements were noticed.

Results are gained from NSL-KDD dataset (DARPA İntrusion dataset, 1999). It was criticized to be a toy dataset (BORISANIYA and PATEL 2015 ; CREECH and HU .2013). This forced authors of the paper in hand to consider ADFA advanced dataset (Creech 2014) too.

In future, we will consider real-time dataset, such that the proposed BRQA guarantees more security.

References

1. AXELSSON, Stefan. Research in intrusion-detection systems: A survey. Technical report 98–17. Department of Computer Engineering, Chalmers University of Technology, 1998.
2. M. Gyanchandani, J. L. Rana, and R. N. Yadav.Taxonomy of Anomaly Based Intrusion Detection System: A Review,. In: International Journal of Scientific and Research Publications, 2:12, 2012.
3. A. S. Raut and K. R. Singh. Anomaly Based Intrusion Detection-A Review, Int. J. on Network Security, 5, 2014.
4. B. Al-Musawi P. Branch. Identifying OSPF Anomalies using Recurrence Quantification Analysis. 2018.
5. F. Palmieri and U. Fiore. Network anomaly detection through nonlinear analysis, Computers & Security, 29(7):737–755, 2010.

PeerJ Preprints NOT PEER-REVIEWED

6. W. Willinger, V. Paxson, and M. S. Taqqu. “Self-similarity and heavy tail: structural modeling of network traffic,” A Practical Guide to Heavy Tails. BirkhRăuser, Boston, USA, 1998.
7. M. A. Righi R.C. Nunes. ‘Combining Recurrence Quantification Analysis and Adaptive Clustering to Detect. 2018.
8. M. Grossglauser and J. C. Bolot. On the relevance of long-range dependence in network traffic,. IEEE/M Transactions on Networking, 7(5):629–640, 1999.
9. M. K. Moridani, S. K. Setarehdan, A. M. Nasrabadi, and E. Hajinasrollah, “Analysis of heart rate variability as a predictor of mortality in cardiovascular patients of intensive care unit,” Biocybernetics and Biomedical Engineering, vol. 35, no. 4, pp. 217–226, 2015.
10. J. Schlender, Funda T, Nedelka T, ‘Evaluatıon of Heart Rate VariabilityUsing Recurrence Analysis’, Measurement 2011, Proceedings of the 8th International Conference, Smolenice, Slovakia.
11. N. Jeyanthi, R Thandeeswaran, and J. Vinithra (2014), ‘RQA Based Approach to detect and prevent DDoS attacks in VoIP Networks’, cybernetics and information Technologies, vol.14, no.1.
12. C. L. Webber and N. Marwan. “Recurrence Quantification Analysis: Theory and Best Practices,” Springer series: Understanding Complex Systems. Springer International Publishing, Cham Switzerland, 2015.
13. A. Fabretti and M. Ausloos. Recurrence plot and recurrence quantification analysis techniques for detecting a critical regime. Examples from financial market indices, International Journal of Modern Physics C, 16:671–706, 2005.
14. H. Kantz, T. Schreiber, and R. Hegger Nonlinear Time Series Analysis. Cambridge University Press, 2002.
15. H.D.I. Abarbanel Analysis of Observed Chaotic. Data Springer, 1997
16. N. Jeyanthi, J. Vinithra, S. Sneha, R. Thandeeswaran, and N.C.S.N. Iyengar. A Recurrence Quantification Analytical Approach to Detect DDoS Attacks,. Washington, DC, USA, 2011.
17. N. Jeyanthi, R. Thandeeswaran, and J. Vinithra. RQA based approach to detect and prevent DDoS attacks in VoIP networks, In: Cybernetics and Information Technologies. v.14, n.1, pp. 11-24,2014.
18. J. P. Eckmann, S. Oliffson Kamphorst, D. Ruelle, and Europhys Lett, 4 (9), pp. 973-977 ,1987.
19. Darpa Intrusion dataset (1999) with the following link: https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-data-set
20. P. Laso, Brosset D., and Puentes J. Dataset of anomalies and malicious acts in a cyber physical system. Data in Brief, 186-191, 2017.
21. Oo, T.T., Phyu, T.: A statistical approach to classify and identify DDoS attacks using UCLA dataset. Int. J. Adv. Res. Comput. Sci. Technol. (IJARCET) 2(5) (2013).

22. Y. C. Wu, H. R. Tseng, W. Yang, and R. H. DDoS detection and traceback with decision tree and grey relational analysis, International Journal of Ad Hoc and Ubiquitous Computing, 7:121–136, 1 2011.
23. Pfleeger, Charles P.; Pfleeger, Shari Lawrence. Security in computing. Prentice Hall Professional Technical Reference, 2002.
24. LIAO, Hung-Jen, et al. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 2013, 36.1: 16-24.
25. ECKMANN, J. P., et al. Recurrence plots of dynamical systems. World Scientific Series on Nonlinear Science Series A, 1995, 16: 441-446.
26. CREECH, Gideon; HU, Jiankun. Generation of a new IDS test dataset: Time to retire the KDD collection. In: 2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2013. p. 4487-4492.
27. BORISANIYA, Bhavesh; PATEL, Dhiren. Evaluation of modified vector space representation using adfa-ld and adfa-wd datasets. Journal of Information Security, 2015, 6.03: 250.
28. G. Creech. Developing a high-accuracy cross platform Host-Based Intrusion Detection System capable of reliably detecting zero-day attacks, 2014