# DEVELOPMENT OF A CRYPTOGRAPHIC MONITORING ALGORITHM FOR REAL-TIME THREAT DETECTION IN A NETWORK ENVIRONMENT

**Azamov Shohruhmirzo Alisher oglu**
Master of Fergana State Technical University
https://doi.org/10.5281/zenodo.17826227

**Abstract.** In this article network real time in the environment in mode threats determination for cryptographic monitoring mechanisms combined RT-CMA (Real-Time Cryptographic Monitoring Algorithm) model offer Algorithm HMAC - SHA3 is used for statistical anomaly analysis and packages authentication to do to the mechanisms is based on. Conducted RT-CMA model experiments to traditional IDS systems relatively high accuracy, low wrong warnings level and fast again work to the possibility has that shows.

**Key words:** network security, HMAC-SHA3, real -time monitoring, anomaly analysis, package authentication, RT-CMA.

**Introduction.** Modern computer real time in networks in mode done increaseable cyberattacks number increasing going because of packages only encryption through protection enough Not. To the network enter coming every one of the package reliability detection, traffic changes assessment and anomalies early determination demand IDS ( Intrusion Detection System) systems many in cases signature based on it works, this and new attack types in determining restrictions brought releases.

That's why the RT-CMA model cryptographic branding and statistic observation combined without real -time packages in mode assessment opportunity creates.

**Methodology (Methods).** Each one to the package the following HMAC-SHA3 code attached:

$$Tag = HMAC_{SHA3}(SrcIP \,||\, DstIP \,||\, Timestamp \,||\, Payload)$$

This is a stamp. of the package legality in inspection is used.

**Statistical monitoring**

Traffic behavior based on the following formula is defined as:

$$A_k = \frac{|X_i - \mu|}{\sigma}$$

- $X_i$ — current package parameters ( delay, port type, packet size ),
- $\mu$ , $\sigma$ — normal distribution parameters.

**Threat probability calculation**

$$P_{threat} = \alpha A_k + \beta(1 - Tag_{valid})$$

If $P_{threat} > 0.6$, package potential is defined as harmful.

**Experiment settings**

| Parameter | Value |
|---|---|
| OS | Ubuntu 22.04 |
| CPU | Intel i5-10400 |
| Network | 100Mbps LAN |
| Test packages | 2500 pieces |
| Analysis tool | Python + Scapy + Wireshark |

**Results .** Packages determination efficiency

| Algorithm | Normal traffic accuracy | Attack determination | Wrong warnings |
|---|---|---|---|
| Snort IDS | 91.4% | 87.2% | 12.8% |
| HMAC-SHA256 | 94.1% | 89.5% | 10.2% |
| RT-CMA ( offer) (made ) | 98.3% | 96.7% | 4.1% |

Package again work speed

| Test | Snort | HMAC-SHA256 | RT-CMA |
|---|---|---|---|
| 1000 packages | 31 ms | 26 ms | 18 ms |
| 2500 packages | 73 ms | 62 ms | 41 ms |

**Analysis**

RT-CMA algorithm:

- By 40% faster,
- 2.5 times less wrong warning gives,
- new attack types to determine flexible.

**Discussion.** Retrieved results based on HMAC-SHA3 package authentication and statistic aside performances evaluation combine the network determination in systems effective approach that it is RT-CMA is different from classic IDS

systems. different accordingly clear to signatures connected It won't stay, it's in traffic. realistic time changes analysis new threats also easy define takes.

This approach especially:

- IoT sensor in networks,
- corporate In LANs,
- security sensitive use in systems for convenient.

**Conclusion:** RT-CMA monitoring cryptography and traffic analysis combined without network safety new stepmother The model provides high accuracy and low resource expense him/her practical to systems current to grow for enough comfortable to the solution converts. Obtained results this algorithm real time in mode worker cybersecurity systems for promising that it is confirms.

## References:

1. Khan, M., & Latif, K. (2021). Real-time network intrusion detection using hybrid anomaly analysis. IEEE Access, 9, 144122–144135.
2. Zhang, Y., Chen, L., & Wu, J. (2022). A high-efficiency HMAC-SHA3 based authentication mechanism for secure packet transmission. Journal of Network and Computer Applications, 205, 103422.
3. Sahoo, K., & Rout, S. (2023). Statistical traffic profiling for early anomaly detection in enterprise networks. Computers & Security, 126, 102996.
4. Ahmed, S., & Dey, N. (2020). Cryptographic integrity tagging for real-time threat identification in network traffic. International Journal of Information Security, 19(5), 521–534.
5. Wang, T., & Li, F. (2024). Real-time packet behavior analysis using machine-aided cryptographic validation. IEEE Transactions on Information Forensics and Security, 19, 887–899.
6. Kim, J., & Park, S. (2023). Enhanced IDS models integrating SHA-3 based verification for detecting spoofed network traffic. Security and Communication Networks, Article ID 1175402.
7. Rahman, M., & Chowdhury, A. (2021). Lightweight cryptographic monitoring techniques for IoT-based threat detection. Sensors, 21(14), 4702.
8. Bansal, P., & Singh, A. (2022). Evaluation of HMAC-based packet authentication schemes in high-speed networks. Journal of Cybersecurity and Privacy, 2(3), 524–538.
9. Li, Z., & Huang, Q. (2020). An adaptive anomaly scoring model for detecting malicious packet flows. Computers, Materials & Continua, 65(3), 2215–2234.

10. Omar, M., Al-Hadhrami, S., & Yaseen, M. (2024). A unified real-time IDS framework combining cryptographic digest validation and statistical learning. Future Generation Computer Systems, 154, 26–39.
11. Ahmedov , S. (2024). “ Digital security : theory and practice ."
12. Alisherov , N. (2021). “ Computer in networks traffic analysis ".
13. Karimov , R. (2020). “ Modern IDS Systems and their efficiency .
14. Haydarov , F. (2023). “ Computer networks and security protocols ”.