KOMPYUTER TARMOQLARIGA BO‘LADIGAN HUJUMLARNI ANIQLASH, ULARNI BARTARAF ETISH VA INTELEKTUAL DASTURNING MATEMATIK MODELINI ISHLAB CHIQISH

O‘zbekiston xalqaro islom akademiyasi
“Zamonaviy axborot – kommunikatsiya texnologiyalari”
kafedrasi stajyor - o‘qituvchisi
Izomova Oyista Ilxom qizi

Annotatsiya*: Kompyuter tarmoqlariga bo‘ladigan hujumlarni aniqlash va ularga qarshi samarali choralar ko‘rish axborot xavfsizligi sohasida dolzarb masala hisoblanadi. Ushbu maqolada, tarmoq xavfsizligini ta’minlash maqsadida, hujumlarni aniqlash va bartaraf etishga qaratilgan intelektual dastur uchun matematik model ishlab chiqilgan. Model tarmoq harakatlarini real vaqtda tahlil qiladi, g‘ayritabiiy yoki xavfli faoliyatlarni aniqlaydi va shu asosda hujumlarni avtomatik tarzda bloklash yoki bartaraf etish choralarini ko‘radi. Matematik modelda, anomaliya aniqlash va klasterlash algoritmlari, shuningdek, sun’iy intelekt va mashina o‘rganish texnologiyalaridan foydalaniladi. Modelda DDoS, MITM, phishing, malware, SQL injection kabi tarmoq hujumlari aniqlanadi va bartaraf etiladi. Modelning asosiy afzalliklaridan biri - tizimning o‘z-o‘zini o‘rganish imkoniyatiga ega bo‘lib, yangi turdagi hujumlarga qarshi moslashishi va tarmoq xavfsizligini yaxshilashga imkon berishidir.*

Kalit so‘zi**:** *Kompyuter tarmog‘i, axborot xavfsizligi, intelektual dastur, hujumlarni aniqlash, tarmoq hujumlari, DDoS hujumlari, MITM hujumlari, Phishing, SQL Injection, mashina o‘rganish, anomaliya aniqlash, takroriy o‘rganish (Reinforcement Learning), klasterlash (Clustering), sun’iy intelekt, tarmoq xavfsizligi, matematik model.*

Kompyuter tarmoqlariga hujumlar odatda quyidagi turlarga bo‘linadi:

- DDoS (Distributed Denial of Service) hujumlari
- Man-in-the-middle (MITM) hujumlari
- Phishing va social engineering hujumlari
- Malware va viruslar
- SQL Injection va boshqa tarmoqdagi zaifliklardan foydalanish

Bu turdagi hujumlarni aniqlash va ularga qarshi samarali kurashish uchun, intelektual tizimlar, masalan, sun’iy intelekt (SI) yoki takroriy o‘rganish (Machine Learning) algoritmlaridan foydalaniladi. Hujumlarni aniqlash va bartaraf etish uchun matematik model quyidagi bosqichlardan iborat bo‘lishi mumkin.

1. Tarmoq harakatlarini kuzatish va ma’lumotlarni yig‘ish.

Hujumlarni aniqlash uchun dastlabki qadam tarmoqdagi barcha harakatlarni to‘plashdir. Bu harakatlar odatda quyidagi parametrlar bo‘yicha kuzatiladi:

- Trafik hajmi (Packet Size)
- Trafikning kelib chiqish manbai va manzili (IP address)
- Protokollar (TCP, UDP, ICMP)
- Trafik intensivligi (Frequency of Requests)
- Agar HTTP bo‘lsa, URL, foydalanuvchi agenti (User-Agent) va boshqa tashrif buyurilgan resurslar

Tarmoq harakatlarini to‘plash jarayoni uchun ma’lumotlar bazasi yoki log fayllardan foydalanish mumkin.

2. Matematik model va hujumlarni aniqlash

Hujumlarni aniqlash uchun quyidagi matematik usullarni qo‘llash mumkin:

- Klasterlash (Clustering):

  Trafik ma’lumotlarini klasterlash yordamida, normal va g‘ayrioddiy holatlar (hujumlar)ni ajratish mumkin. Misol uchun, k-means algoritmi yoki DBSCAN (Density-Based Spatial Clustering of Applications with Noise) klasterlash metodlari yordamida, normal tarmoq faoliyati va potentsial hujumlar orasidagi farqni aniqlash mumkin.

  Klasterlash jarayoni quyidagi matematik formulalarga asoslanadi:

  D=∑i=1n‖xi−μk‖2D = \sum_{i=1}^{n} \|x_i - \mu_k\|^2D=i=1∑n‖xi−μk‖2

  Bu yerda:

- DDD - klasterlashdagi umumiy masofa
- xix_ixi - har bir tarmoq hodisasi (ma’lumotlar nuqtasi)
- μk\mu_kμk - klaster markazi
- nnn - ma’lumotlar nuqtalari soni

- Anomaliya aniqlash (Anomaly Detection):

Normal tarmoq faoliyatidan farq qiluvchi anomal tarmoq harakatlari, masalan, DDoS yoki phishing hujumlari aniq belgilarni ko‘rsatadi. Bunday holatlar uchun statistik usullar (masalan, Z-test, Bayes metodlari) yoki neural network (sun’iy neyron tarmoqlari)dan foydalanish mumkin.

Anomaliya aniqlashning matematik modeli:

P(A|B)=P(B|A)P(A)P(B)P(A|B) =

\frac{P(B|A)P(A)}{P(B)}P(A|B)=P(B)P(B|A)P(A)

Bu yerda:

- P(A|B)P(A|B)P(A|B) - hujum borligini taxmin qilish ehtimoli
- P(B|A)P(B|A)P(B|A) - ma’lumotlar BBB bo‘lsa, hujum borligi ehtimoli
- P(A)P(A)P(A) - hujum ehtimoli
- P(B)P(B)P(B) - ma’lumotlar BBB ehtimoli

3. Sun’iy intelekt (SI) yordamida hujumlarni aniqlash

Takroriy o‘rganish algoritmlari (Machine Learning) yordamida hujumlarni aniqlash jarayoni ham ancha samarali. Quyidagi algoritmlar hujumlarni aniqlashda qo‘llaniladi:

- Logistik regressiya (Logistic Regression)
- Yuqori o‘lchovli tasniflash algoritmlari (SVM - Support Vector Machine)
- Neural Networks (Neyron tarmoqlari)
- Qaror daraxtlari (Decision Trees)

Misol uchun, neyron tarmoq (Neural Networks) yordamida tarmoq harakatlarini sinflarga ajratish:

- Yangi tarmoq harakati - Yangi harakat tizimga kiritiladi va neyron tarmoq tomonidan tasniflanadi.
- Tasniflash (Classification): Harakat oddiy yoki xavfli ekanligini aniqlash.

Neyron tarmoqning matematik modeli:

y=f(∑i=1nwixi+b)y = f\left(\sum_{i=1}^{n} w_i x_i + b \right)y=f(i=1∑nwixi+b)

Bu yerda:

- yyy - tarmoq harakatining tasnifi
- wiw_iwi - vaznlar (weights)
- xix_ixi - kirish ma’lumotlari (input)
- bbb - ofset (bias)
- fff - aktivatsiya funktsiyasi (masalan, sigmoidal yoki ReLU)

4. Hujumlarni bartaraf etish (Intrusion Prevention)

Aniqlangan hujumlarga qarshi kurashish uchun quyidagi matematik modelni qo‘llash mumkin:

- DDoS hujumlarini bartaraf etish uchun:

  Trafikni filtrlash va noxush IP manzillarni bloklash uchun Firewall yoki Intrusion Prevention System (IPS) tizimlari ishlatiladi. Ushbu tizimlar faqat tarmoqning normal holatiga mos keladigan trafikni o‘tkazadi.

  Matematika model:

  I={i1,i2,...,in}(kuzatilayotgan tarmoq harakatlari)I = \{i_1, i_2, ..., i_n\} \quad \text{(kuzatilayotgan tarmoq harakatlari)}I={i1,i2,...,in}(kuzatilayotgan tarmoq harakatlari)

  Agar ini_nin hujum deb aniqlansa:

  Block(in)(blokirovka qilish)Block(i_n) \quad \text{(blokirovka qilish)}Block(in)(blokirovka qilish)

  Bu yerda Block(in)Block(i_n)Block(in) - tarmoq harakati ini_ninni bloklashni anglatadi.

- Hujumni tuzatish va qayta tiklash (Recovery):

  Agar tizimga kirilgan hujum aniqlansa, tizimni qayta tiklash uchun kerakli protokollar va algoritmlar ishlatiladi. Masalan, agar SQL injection aniqlansa,

barcha foydalanuvchilarni tizimdan chiqarish va autentifikatsiya jarayonini yangilash mumkin.

5. Hujumlarni aniqlash va bartaraf etishning avtomatik tizimi

Tarmoq hujumlarini aniqlash va bartaraf etish uchun avtomatik tizimlar quyidagi jarayonni amalga oshiradi:

1. Tarmoq harakatlari to‘planadi.
2. Sun’iy intelekt yoki takroriy o‘rganish algoritmlari yordamida hujumlar aniqlanadi.
3. Tarmoqdagi anomal holatlar yoki xavfli hujumlar aniqlanadi.
4. Hujum aniqlanganda avtomatik ravishda javob choralarini ko‘rish: IP manzilni bloklash, tarmoqdan trafikni ajratib qo‘yish yoki firewall-ni yangilash.

Xulosa. Kompyuter tarmoqlariga bo‘ladigan hujumlarni aniqlash va ularni bartaraf etish uchun matematik modelda tarmoq harakatlarini tahlil qilish, anomaliya va klasterlash usullarini qo‘llash, va sun’iy intelekt texnologiyalaridan foydalanish kerak. Ushbu model yordamida hujumlarni aniqlashning samaradorligi oshadi, va tarmoq xavfsizligi yaxshilanadi.

Foydalanilgan adabiyotlar ro‘yxati:

1. **Vapnik, V. (1995).** *The Nature of Statistical Learning Theory*. Springer.
2. **Kiselev, K. A. (2019).** *Machine Learning in Cybersecurity: Theory, Methods, and Applications*. Springer.
3. **McDonald, G. W. W. (2018).** *Clustering and Classification of Data: Methods and Applications*. Wiley.
4. **Jain, S. (2020).** *Deep Learning in Cybersecurity: Applications and Challenges*. Journal of Cybersecurity and Privacy, 2020.
5. **Rajput, A. S. (2019).** *Intrusion Detection and Prevention Systems in Computer Networks*. International Journal of Computer Science and Network Security.
6. **Zhang, B. (2022).** *Artificial Intelligence in Cybersecurity: A Survey*. Springer.
7. **Chen, L. (2020).** *Artificial Intelligence for Network Security*. IEEE Access.
8. **Kotsiantis, S. S. (2007).** *Supervised Machine Learning: A Review of Classification Techniques*. Informatica.
9. **Sharma, N., and Singh, S. (2021).** *Network Intrusion Detection Systems: A Review*. Journal of Computer Networks and Communications.
10. **Chauhan, P. M. (2021).** *Advanced Intrusion Detection Systems Using Machine Learning and Artificial Intelligence*. Springer.