# KOMPYUTER TARMOQLARIGA BO‘LADIGAN HUJUMLARNI ANIQLASH VA HUJUMLARNI BARTARAF ETISH ALGORITMINI ISHLAB CHIQISH

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

**Annotatsiya**: Kompyuter tarmoqlarining xavfsizligini ta’minlash bugungi kunda juda muhim ahamiyat kasb etmoqda. Tarmoq xavfsizligi muammolarini hal qilishda, sun’iy intelekt va mashina o‘rganish algoritmlaridan foydalanish samarali yechimlarni taqdim etadi. Ushbu maqolada, kompyuter tarmoqlariga bo‘ladigan hujumlarni aniqlash va ularni bartaraf etish uchun intelektual dastur algoritmi ishlab chiqilgan. Algoritm, tarmoq harakatlarini real vaqtda kuzatib boradi, g‘ayritabiiy yoki xavfli harakatlarni aniqlaydi va hujumlarni avtomatik tarzda bloklash uchun javob choralari ko‘radi. Buning uchun, anomaliya aniqlash, klasterlash, va tasniflash kabi sun’iy intelekt metodlari, shu jumladan, mashina o‘rganish va qayta o‘rganish algoritmlari qo‘llaniladi. Algoritm tarmoqdagi DDoS, MITM, phishing, malware, va SQL injection kabi turli xil hujumlarni aniqlash va bartaraf etishda samarali ishlaydi. Ushbu tizim o‘z-o‘zini o‘rganish imkoniyatiga ega bo‘lib, yangi hujumlarga qarshi moslashib boradi.

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

Kompyuter tarmoqlariga bo‘ladigan hujumlarni aniqlash va ularga qarshi choralar ko‘rish uchun **intelektual tizim** yaratish zarur. Ushbu tizim, tarmoq harakatlarini monitoring qilish va hujumlarni aniqlashda sun’iy intelekt, mashina o‘rganish (Machine Learning) va anomaliya aniqlash texnologiyalarini qo‘llaydi. Quyida hujumlarni aniqlash va bartaraf etish jarayonini boshqaradigan algoritmni taqdim etamiz.

## Algoritm bosqichlari

1. **Tarmoq faoliyatini kuzatish va ma’lumotlarni yig‘ish**

- Tarmoqdagi barcha harakatlar (IP manzillar, portlar, trafik hajmi, protokollar, va boshqa parametrlar) doimiy ravishda to‘planadi.
- **Kuzatish vositalari**: Paket snifferlari, firewalls, IDS (Intrusion Detection System) yoki NetFlow bilan tarmoqdan ma’lumotlar yig‘ish.

2. **Ma’lumotlarni oldindan qayta ishlash (Preprocessing)**

- Olingan tarmoq ma’lumotlari to‘planadi va kerakli formatda ishlov beriladi (normalizatsiya, anomaliyalardan tozalash, va boshqalar).
- **Xususiyatlar tanlash (Feature Selection)**: Trafik hajmi, IP manzillar, portlar, tarmoq protokollari kabi xususiyatlar tanlanadi.

3. **Anomaliyani aniqlash (Anomaly Detection)**

- Ma’lumotlar to‘plamiga asoslanib, **takroriy o‘rganish algoritmlari** (masalan, **Random Forest**, **SVM**, **Neural Networks**) yoki **klasterlash** (masalan, **K-means** yoki **DBSCAN**) yordamida tarmoqdagi g‘ayritabiiy harakatlar aniqlanadi.
- **Anomalniyani aniqlash modeli**:

Agar trafik **oddiy** bo‘lsa, harakatni o‘z holida qoldir.

Agar trafik **g‘ayrioddiy** bo‘lsa, uni hujum deb tasnifla.

4. **Hujum turlari bo‘yicha tasniflash**

- Tarmoq harakatlari tasniflanadi va har bir harakat turli hujumlarga (masalan, **DDoS**, **MITM**, **Phishing**, **SQL Injection**) ajratiladi.

**Tasniflash usullari**:

**Naive Bayes**, **KNN (K-Nearest Neighbors)** yoki **SVM** yordamida harakatni aniq hujumga ajratish.

5. **Hujumni aniqlash va bloklash (Intrusion Prevention)**

- Hujum aniqlanganda, tizim avtomatik ravishda hujumni bloklash uchun chora ko‘radi.
- **Firewall** yoki **Intrusion Prevention System (IPS)** yordamida:

Hujumni kelayotgan IP manzili bo‘yicha bloklash.

Trafikni cheklash va noxush so‘rovlarni o‘chirish.

Agar DDoS hujumi bo‘lsa, tarmoqni qisman yopish.

6. **Ma’lumotlar va tarmoqdan javob choralarini ko‘rish (Incident Response)**

- Hujumni aniqlagandan so‘ng tizim jurnal yozuvlarini (logs) yaratadi va tizim administratorlariga bildirish yuboradi.
- Hujumga qarshi quyidagi javob choralarini ko‘rish:

Hujumni bloklash.

Yangi xavf-xatarlarni qayd etish.

Qayta tarmoq faoliyatini tiklash.

7. **Tizimni yangilash va o‘z-o‘zini o‘rganish (Self-learning)**

-Hujumdan keyin tizim yangi hujum turlarini o‘rganib, uning modellarini yangilaydi.

-**Takroriy o‘rganish** (Reinforcement Learning) va **Yapay Tarmoq** yordamida tizim xavfsizlikka qarshi yangi tahdidlarni aniqlash uchun o‘z-o‘zini yangilab boradi.

**Algoritmning ta’rifi**

1. **Tarmoq faoliyatini kuzatish**:

1.1. Tarmoqdan barcha harakatlarni yig‘ish.

1.2. Trafikni o‘zgaruvchan tarmoq holatiga qarab to‘plang.

2. **Ma’lumotlarni oldindan qayta ishlash**:

2.1. Yig‘ilgan ma’lumotlarni normalizatsiya qilish.

2.2. Harakatlarni asosiy xususiyatlarga ajratish.

3. **Anomaliyalarning aniqlanishi**:

3.1. Harakatlarni o‘rganish uchun mashina o‘rganish modelini tanlash.

3.2. Trafikdagi anomaliyalarni aniqlash.

3.3. Anomal tarmoq harakatlarini «g‘ayrioddiy» deb belgilash.

4. **Hujum turlarini tasniflash**:

4.1. Hujumlar va normal tarmoq harakatlarini tasniflash algoritmlariga kiritish.

4.2. Hujum turlarini aniqlash (masalan, DDoS, MITM, Phishing, Malware, SQL Injection).

5. **Hujumni bartaraf etish**:

5.1. Hujum turlarini aniqlanganda avtomatik bloklash.

5.2. Firewall yoki IPS orqali noxush IP manzillarni bloklash.

5.3. Agar DDoS hujumi aniqlansa, trafikni cheklash.

6. **Javob choralarini ko‘rish**:

6.1. Hujumni aniqlagandan so‘ng, tizim administratorlariga bildirish yuborish.

6.2. Hujumni to‘liq bartaraf etish.

6.3. Yangi tahdidni qayd etish va tizimni yangilash.

7. **O‘z-o‘zini o‘rganish**:

7.1. Hujumdan so‘ng tizimni yangilash.

7.2. Takroriy o‘rganish algoritmi yordamida yangi hujumlarni aniqlash va tizimni moslashtirish.

**Algoritmning vizual taqdimoti**

1. Tarmoq ma’lumotlarini yig‘ish → 2. Ma’lumotlarni qayta ishlash → 3. Anomaliyalarning aniqlanishi → 4. Hujum turlarini tasniflash → 5. Hujumni bloklash → 6. Javob choralarini ko‘rish → 7. Tizimni yangilash va o‘z-o‘zini o‘rganish

**Algoritmning real vaqtda ishlashi**

- **Monitoring bosqichi:** Tarmoqdagi barcha harakatlarni real vaqt rejimida to‘plash.
- **Aniqlash bosqichi:** Olingan ma’lumotlarni algoritmlar yordamida tahlil qilish va g‘ayritabiiy holatlarni aniqlash.
- **Bartaraf etish bosqichi:** Aniqlangan hujumlarni tizim tomonidan avtomatik bloklash va tarmoqni xavfsiz holatga qaytarish.
- **O‘z-o‘zini yangilash:** Yangi hujumlarni tizim tomonidan o‘z-o‘zini o‘rganish orqali aniqlash va tizimni optimallashtirish.
-

## Xulosa

Ushbu algoritm kompyuter tarmoqlaridagi hujumlarni aniqlash va bartaraf etishda samarali ishlaydi. Sun’iy intelekt va mashina o‘rganish texnologiyalaridan foydalangan holda tarmoq xavfsizligini ta’minlash va yangi xavf-xatarlarga qarshi kurashishda yuqori samaradorlikni ta’minlash mumkin.

Kompyuter tarmoqlariga bo‘ladigan hujumlarni aniqlab, hujumlarni bartaraf eta oladigan intelektual dastur yaratish uchun, bir nechta texnologiyalarni qo‘llash kerak bo‘ladi. Bu texnologiyalar tarmoq faoliyatini kuzatish, anomaliyalarga asoslangan tahlil qilish, mashina o‘rganish algoritmlarini qo‘llash va avtomatik hujumlarni bartaraf etish jarayonlarini o‘z ichiga oladi. Quyida bunday intelektual dastur yaratishning asosiy bosqichlarini ko‘rib chiqamiz.

**1. Tizim arxitekturasini yaratish**

Dastur quyidagi asosiy qismlardan iborat bo‘ladi:

- **Ma’lumotlarni yig‘ish**: Tarmoq harakatlarini doimiy ravishda kuzatib borish uchun, tarmoqdan turli xususiyatlarni (IP manzillari, portlar, protokollar, trafik hajmi) yig‘ish kerak. Bu jarayonni amalga oshirish uchun IDS (Intrusion Detection System), NetFlow, yoki SNMP kabi protokollarni qo‘llash mumkin.

- **Ma’lumotlarni qayta ishlash**: Olingan xom ma’lumotlarni tozalash, normalizatsiya qilish va qayta ishlash zarur.
- **Anomaliyani aniqlash va hujumlarni tasniflash**: Mashina o‘rganish yoki chuqur o‘rganish algoritmlarini qo‘llash orqali tarmoqdagi xavfli yoki g‘ayritabiiy harakatlarni aniqlash.
- **Hujumni bartaraf etish**: Aniqlangan hujumga qarshi avtomatik ravishda choralar ko‘rish, masalan, trafikni bloklash yoki firewall yordamida IP manzillarini cheklash.

## 2. Dastur algoritmi

### 2.1. Ma’lumotlarni yig‘ish

Dastur tarmoqdagi barcha harakatlarni (IP manzillari, protokollar, portlar, trafik hajmi va boshqa parametrlar) yig‘adi. Bu ma’lumotlarni olish uchun tarmoqni monitoring qilish vositalarini ishlatish mumkin.

```
python
Копировать код
import psutil

# Tarmoqning umumiy ma’lumotlarini olish
network_info = psutil.net_io_counters(pernic=True)

# Tarmoqdan kirish va chiqish trafik ma’lumotlarini yig‘ish
for interface, stats in network_info.items():
    print(f"Interface: {interface}, Bytes Sent: {stats.bytes_sent}, Bytes
Received: {stats.bytes_recv}")
```

### 2.2. Ma’lumotlarni qayta ishlash

Yig‘ilgan ma’lumotlarni analiz qilish uchun ma’lumotlarni tozalash va normalizatsiya qilish zarur.

```
python
Копировать код
import pandas as pd
from sklearn.preprocessing import StandardScaler

# Misol uchun, tarmoq ma’lumotlarini DataFrame ga o‘tkazish
data = pd.DataFrame({
    ‘ip’: [‘192.168.0.1’, ‘192.168.0.2’],
    ‘sent_bytes’: [1200, 2000],
    ‘received_bytes’: [800, 1500]
})

# Normalizatsiya qilish
scaler = StandardScaler()
data[[‘sent_bytes’, ‘received_bytes’]] =
scaler.fit_transform(data[[‘sent_bytes’, ‘received_bytes’]])
```

```
print(data)
```

### 2.3. Anomaliyalarga asoslangan hujumlarni aniqlash

Anomaliya aniqlash algoritmlarini ishlatish (masalan, Isolation Forest, Random Forest, yoki k-NN).

```
python
Копировать код
from sklearn.ensemble import IsolationForest

# Anomaliya aniqlash modeli
model = IsolationForest(n_estimators=100)
model.fit(data[['sent_bytes', 'received_bytes']])

# Yangi tarmoq harakati ma'lumotini test qilish
test_data = [[1500, 1000]]  # Test ma'lumotlari
prediction = model.predict(test_data)

if prediction == -1:
    print("Xavfli hujum aniqlangan!")
else:
    print("Normal harakat.")
```

### 2.4. Hujumlarni tasniflash

Harakatlarni tasniflash uchun mashina o‘rganish algoritmlaridan foydalaniladi. Misol uchun, **Naive Bayes** yoki **Support Vector Machine (SVM)** kabi tasniflash algoritmlari.

```
python
Копировать код
from sklearn.svm import SVC

# Tasniflash uchun misol model
X = data[['sent_bytes', 'received_bytes']]  # Xususiyatlar
y = [0, 1]  # 0 - normal, 1 - hujum (misol uchun)

# Model yaratish va o'qitish
model = SVC(kernel='linear')
model.fit(X, y)

# Yangi tarmoq harakati uchun tasniflash
new_data = [[1200, 900]]
prediction = model.predict(new_data)

if prediction == 1:
    print("Hujum aniqlangan!")
else:
    print("Normal harakat.")
```

### 2.5. Hujumni bartaraf etish

Agar hujum aniqlansa, tizim avtomatik ravishda hujumni bloklashi kerak. Bunda **Firewall** yoki **Intrusion Prevention System (IPS)** kabi tizimlar yordamida IP manzillarini yoki portlarni bloklash mumkin.

```
python
Копировать код
import os

# Hujumni bloklash (IP manzillarini bloklash)
def block_ip(ip_address):
    os.system(f"sudo ufw deny from {ip_address}")

# Misol uchun, xavfli IP manzilini bloklash
block_ip("192.168.0.1")
```

### 3. O‘z-o‘zini o‘rganish va tizimni yangilash

Model yangi hujum turlarini aniqlashda davom etadi va o‘z-o‘zini o‘rganish imkoniyatiga ega bo‘lishi uchun **takroriy o‘rganish (Reinforcement Learning)** algoritmlarini qo‘llash mumkin.

```
python
Копировать код
# Takroriy o‘rganish (Reinforcement Learning) modeli
# Bu yerda oddiygina agentning harakatini optimallashtirishni ko‘rib
chiqamiz
class SimpleAgent:
    def __init__(self):
        self.state = 0  # Boshlang‘ich holat

    def act(self, state):
        # Qoidalar asosida qarorlar qabul qilish
        if state > 0:
            return 1  # Hujumni bloklash
        else:
            return 0  # Normal harakat

agent = SimpleAgent()
action = agent.act(1)  # Yangi holatga qarab harakat qilish
```

### 4. Dastur va tizimni test qilish

Dastur tugallangach, uni tarmoqda test qilish zarur. Tarmoqda aniq hujumlar yoki xavfli harakatlar simulyatsiya qilinadi, va tizimning qanday javob berishini ko‘rib chiqish kerak.

### Xulosa

Kompyuter tarmoqlariga bo‘ladigan hujumlarni aniqlab, hujumlarni bartaraf eta oladigan intelektual dastur yuqorida keltirilgan metodlar yordamida ishlab chiqilishi

mumkin. Bu dastur tarmoq harakatlarini real vaqt rejimida kuzatadi, xavfli yoki g‘ayritabiiy harakatlarni aniqlaydi va hujumlarga qarshi samarali choralar ko‘radi. Dastur sun’iy intelekt va mashina o‘rganish texnologiyalaridan foydalanish orqali tizimni o‘z-o‘zini takomillashtirish va yangi tahdidlarni aniqlash imkoniyatiga ega.

## Foydalanilgan adabiyotlar ro‘yxati:

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