TARMOQ TRAFIGI ANOMALIYALARINI ANIQLASHDA KASKADLI KO‘P-ENTROPIYALI ANIQLASH ALGORITMI

Suhrobjon Bozorov[1], Doniyorbek Usmanbayev[1]

[1]Muhammad al-Xorazmiy nomidagi TATU,
E-mail: mr.bozorov95@gmail.com, doniyorbekush@gmail.com
ORCID 0000-0002-2377-934X, ORCID 0000-0002-2048-2946

K E Y W O R D S

entropiya, tarmoq trafigi, anomaliya aniqlash, Shannon entropiyasi, Rényi entropiyasi, kiberxavfsizlik, kaskadli algoritm, CUSUM, F1-mezon

A B S T R A C T

Ushbu ishda tarmoq trafigi anomaliyalarini aniqlashda qo‘llaniladigan entropiya asosidagi usullarning tizimli tahlili taqdim etiladi. Klassik Shannon entropiyasidan tortib umumlashtirilgan (Rényi, Tsallis) va vaqt qatoriga asoslangan (taxminiy, namuna, permutatsion, loyqa, ko‘p-masshtabli) entropiya turlarigacha bo‘lgan o‘n uchta usulning matematik asoslari, hisoblash murakkabligi, sezuvchanligi va real vaqt sharoitida qo‘llanilishi mumkinligi bo‘yicha qiyosiy baholash o‘tkaziladi. Tahlil natijalari asosida mavjud usullarning umumiy kamchiliklarini bartaraf etuvchi, kaskadli ko‘p-entropiyali fuzion (KKEF) deb nomlangan yangi algoritm ishlab chiqiladi va uning arxitekturasi hamda to‘liq matematik modeli taqdim etiladi. Algoritmning samaradorligi maxsus generatsiya qilingan sintetik tarmoq trafigi ustida o‘tkazilgan hisoblash tajribasi orqali baholanadi. Natijalarga ko‘ra, KKEF yagona Shannon entropiyasiga asoslangan bazaviy usulga nisbatan F1-mezon bo‘yicha taxminan 2,7 barobar yuqori ko‘rsatkichga erishadi, soxta signal darajasi (FAR) esa mutlaq qiymatda past (2% dan kam) darajada saqlanadi. Olingan natijalar sintetik ma’lumotlarga asoslangan bo‘lib, ishlab chiqarish sharoitida qo‘llashdan oldin standart ochiq ma’lumotlar to‘plamlarida qo‘shimcha tekshiruvdan o‘tkazilishi tavsiya etiladi.

Kirish

Zamonaviy tarmoq infratuzilmalarining hajmi va murakkabligi tobora ortib borishi kiberxavfsizlik tizimlaridan trafikdagi g‘ayrioddiy holatlarni tezkor va aniq aniqlashni talab qiladi. An’anaviy imzo-asoslangan tizimlar faqat oldindan ma’lum bo‘lgan hujum naqshlarini aniqlay olishi sababli, noma’lum yoki yangi turdagi hujumlarga nisbatan cheklangan samaradorlikka ega. Shu sababli statistik va axborot-nazariy yondashuvlar, xususan entropiya asosidagi usullar, anomaliyaga asoslangan aniqlash tizimlarining muhim tarkibiy qismiga aylangan.

Entropiya tushunchasi dastlab Shannon tomonidan axborot nazariyasi doirasida taqdim etilgan bo‘lib [1], u tizimdagi noaniqlik darajasini miqdoriy baholash imkonini beradi. Tarmoq xavfsizligi sohasida entropiyadan foydalanish g‘oyasi Feinstein va boshqalar tomonidan DDoS hujumlarini aniqlashda [11], keyinchalik Lakhina va boshqalar tomonidan trafik xususiyatlari taqsimotini tahlil qilishda [12], hamda Nychis va boshqalar tomonidan turli entropiya turlarining aniqlash qobiliyatini empirik baholashda [13] keng qo‘llanilgan. Bereziński va boshqalar esa entropiya asosidagi usullarning umumlashtirilgan tizimli sharhini taqdim etgan [15]. Parallel ravishda, matematika va statistik fizika sohalarida Shannon entropiyasining bir qator umumlashmalari - Rényi entropiyasi [2], Tsallis entropiyasi [3] va Havrda–Charvát strukturaviy entropiyasi [4] - ishlab chiqilgan bo‘lib, ular keyinchalik tarmoq trafigini tahlil qilishga ham moslashtirilgan. Bundan tashqari, tibbiyot va nochiziqli dinamika sohalarida vaqt qatorlarining murakkabligini o‘lchash uchun ishlab chiqilgan taxminiy entropiya [6], namuna entropiyasi [7], permutatsion entropiya [8], loyqa entropiya [9] va ko‘p-masshtabli entropiya [10] usullari ham tarmoq trafigining vaqtinchalik tuzilmasini tahlil qilish uchun salohiyatga ega.

Mavjud adabiyotlarning ko‘lami sezilarli bo‘lishiga qaramay, entropiya usullarining barcha zarur mezonlar (hisoblash murakkabligi,

(cc) BY dtai.uz

sezuvchanlik, shovqinga chidamlilik, real vaqt sharoitida qo‘llanilishi) bo‘yicha yagona tizimli qiyosiy tahlili adabiyotda yetarlicha aks etmagan, bu esa amaliyotchilar uchun mos usulni tanlashni murakkablashtiradi. Shuningdek, alohida entropiya usullarining har biri ma’lum turdagi anomaliyalarni aniqlashda samarali bo‘lsa-da, boshqa turlarini o‘tkazib yuborishi mumkinligi haqidagi kuzatuv [13] yangi, ko‘p mezonli va moslashuvchan yondashuvlar zarurligini ko‘rsatadi.

Ushbu tadqiqotning maqsadi ikki qismdan iborat: birinchidan, tarmoq trafigi anomaliyalarini aniqlashda qo‘llaniladigan mavjud entropiya usullarining tizimli qiyosiy tahlilini o‘tkazish; ikkinchidan, aniqlangan kamchiliklarni bartaraf etuvchi, kaskadli arxitekturaga asoslangan yangi aniqlash algoritmini ishlab chiqish va uning samaradorligini sintetik trafik ustida baholash. Maqolaning qolgan qismi quyidagicha tashkil etilgan: 2-bo‘limda tadqiqot uslubiyoti, entropiya usullarining tavsifi va taklif etilgan algoritm keltiriladi; 3-bo‘limda qiyosiy tahlil va sinov natijalari taqdim etiladi; 4-bo‘limda esa xulosalar umumlashtiriladi.

Tadqiqot usullari

Tadqiqot ikki bosqichda amalga oshirildi. Birinchi bosqichda tarmoq trafigi anomaliyalarini aniqlashda qo‘llaniladigan o‘n uchta entropiya usuli ilmiy adabiyot asosida tizimlashtirildi va ular hisoblash murakkabligi, sozlanuvchi parametrlar soni, vaqtinchalik tartibni hisobga olish qobiliyati, past intensivlikdagi anomaliyalarga sezuvchanlik, shovqinga chidamlilik hamda real vaqt rejimida qo‘llanilish imkoniyati kabi mezonlar bo‘yicha qiyosiy baholandi. Ikkinchi bosqichda, aniqlangan umumiy kamchiliklarni bartaraf etish maqsadida, kaskadli ko‘p-bosqichli arxitekturaga asoslangan yangi algoritm (KKEF) ishlab chiqildi. Algoritmning samaradorligi Python dasturlash tilida amalga oshirilgan referens implementatsiya yordamida, maxsus generatsiya qilingan sintetik tarmoq trafigi ustida, sakkizta mustaqil tasodifiy seed (random seed) bo‘yicha takrorlangan hisoblash tajribasi orqali baholandi.

Entropiya asosidagi usullarning tavsifi

Shannon entropiyasi. Tarmoq trafigi xususiyati taqsimotidagi umumiy noaniqlikni o‘lchaydi: $H(X) = -\Sigma\, p_i \cdot \log2(p_i)$, bu yerda p_i - i-toifaning ehtimoli [1].

Rényi entropiyasi. Shannon entropiyasining α tartib parametri orqali umumlashtirilgan ko‘rinishi: $H\alpha(X) = (1/(1-\alpha)) \cdot \log2(\Sigma\, p_i\text{^}\alpha)$; $\alpha \to 1$ da Shannon entropiyasiga aylanadi [2].

Tsallis entropiyasi. Nolinear tizimlar uchun ishlab chiqilgan: $Sq(X) = (1/(q-1)) \cdot (1 - \Sigma\, p_i\text{^}q)$; uzoq masofali bog‘liqlikka ega trafikni tahlil qilishda samarali hisoblanadi [3].

Havrda–Charvát entropiyasi. Tsallis entropiyasiga matematik jihatdan ekvivalent, mustaqil ravishda axborot nazariyasi doirasida taqdim etilgan: $H\beta(X) = (2\text{^}(1-\beta) - 1)^{-1} \cdot (\Sigma\, p_i\text{^}\beta - 1)$ [4].

Shartli entropiya. Ikki xususiyat (masalan, manba IP va port) orasidagi statistik bog‘liqlikni $H(Y|X) = H(X,Y) - H(X)$ ko‘rinishida tahlil qiladi.

Birgalik entropiya. Ikki xususiyatning umumiy noaniqligini $H(X,Y) = -\Sigma\Sigma\, p(x,y) \cdot \log2\, p(x,y)$ ko‘rinishida o‘lchaydi.

Nisbiy entropiya (Kullback–Leibler divergensiyasi). Joriy taqsimot P bilan bazaviy taqsimot Q orasidagi farqni $D_KL(P\|Q) = \Sigma\, p_i \cdot \log2(p_i/q_i)$ ko‘rinishida o‘lchaydi [5].

O‘zaro (cross) entropiya. Nisbiy entropiya bilan bog‘liq bo‘lib, $H(P,Q) = H(P) + D_KL(P\|Q)$ ko‘rinishida ifodalanadi [5].

Taxminiy entropiya (ApEn). Vaqt qatorining bashoratlanmaslik darajasini $ApEn(m,r,N) = \Phi^m(r) - \Phi^{m+1}(r)$ formulasi orqali baholaydi, bu yerda m - naqsh uzunligi, r - moslik chegarasi [6].

Namuna entropiyasi (SampEn). ApEn’ning o‘z-o‘ziga moslik xatosidan xoli, statistik jihatdan barqarorroq varianti: $SampEn(m,r,N) = -\ln(A/B)$ [7].

Permutatsion entropiya. Vaqt qatoridagi qiymatlarning nisbiy tartibiga asoslanadi: $Hp(m) = -\Sigma\, p(\pi) \cdot \log2\, p(\pi)$, bu yerda π - mumkin bo‘lgan ordinal naqshlar [8].

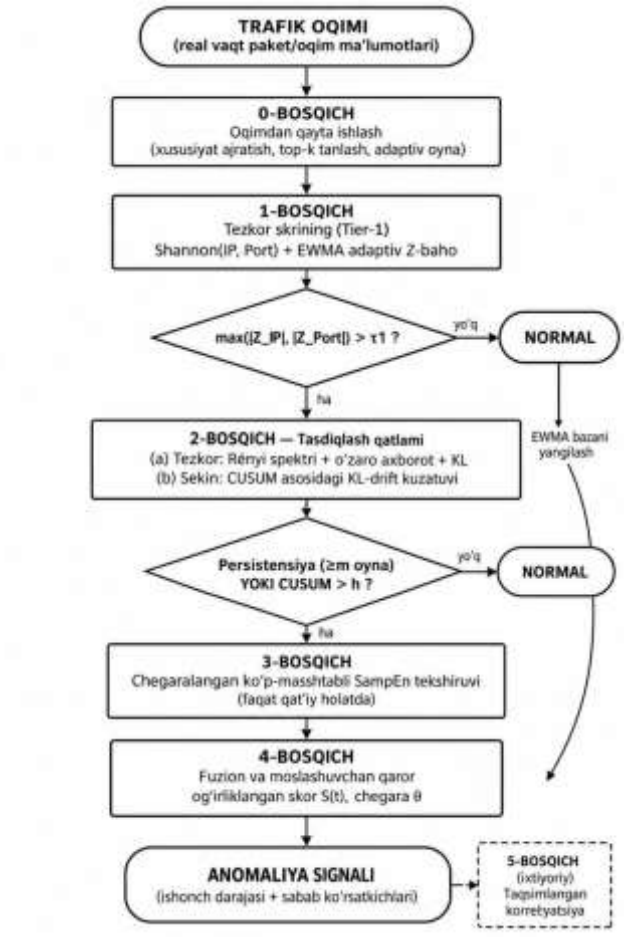
Loyqa entropiya. SampEn’ning qattiq chegaraviy funksiyasi o‘rniga silliq eksponensial a’zolik funksiyasidan foydalanadigan varianti bo‘lib, natijaning r parametriga sezuvchanligini pasaytiradi [9].

(cc) BY dtai.uz

Ko‘p-masshtabli entropiya (MSE). Trafik qatorini turli vaqt masshtablarida yiriklashtirib, har bir masshtabda namuna entropiyasini hisoblash orqali tizim murakkabligini bir necha vaqt o‘lchamida tavsiflaydi [10].

Taklif etilgan KKEF arxitekturasi

O‘tkazilgan qiyosiy tahlil shuni ko‘rsatdiki, yuqorida keltirilgan usullarning hech biri barcha mezonlar bo‘yicha bir vaqtning o‘zida ustunlikka ega emas: klassik usullar (Shannon, Rényi, Tsallis) hisoblash tezligi bilan ajralib tursa-da, vaqtinchalik tartibni hisobga olmaydi; vaqt qatoriga asoslangan usullar (SampEn, MSE) chuqurroq tahlil bersa-da, hisoblash murakkabligi yuqori. Ushbu kuzatuv asosida *kaskadli ko‘p-entropiyali fuzion (KKEF)* - deb nomlangan yangi algoritm taklif etiladi. Algoritm yagona formulaga emas, balki besh bosqichli kaskadli arxitekturaga asoslanadi: tezkor va sodda usullar katta hajmdagi trafikni birlamchi filtrlaydi, murakkabroq usullar esa faqat shubhali holatlarda ishga tushiriladi. Arxitekturaning umumiy ko‘rinishi 1-rasmda keltirilgan.



1-rasm. KKEF arxitekturasining besh bosqichi.

Birinchi bosqichda (Tier-1) Shannon entropiyasi EWMA (eksponensial vaznlangan harakatlanuvchi o‘rtacha) asosidagi adaptiv chegara bilan birgalikda qo‘llaniladi va trafikning katta qismini (odatda 90% dan ortiq oynalarni) tezkor tarzda normal deb belgilaydi. Faqat chegaradan chetga chiqqan holatlar ikkinchi bosqichga - tasdiqlash qatlamiga - uzatiladi. Ikkinchi bosqich ikki parallel yo‘ldan iborat: (a) tezkor yo‘lda Rényi entropiyasi spektri, o‘zaro axborot (mutual information) va Kullback–Leibler divergensiyasi hisoblanadi; (b) sekin yo‘lda esa CUSUM (kumulyativ yig‘indi) nazorat jarayoniga asoslangan KL-drift kuzatuvi amalga oshiriladi, bu past intensivlikdagi (‘stealth’) anomaliyalarni aniqlash imkonini beradi. Uchinchi bosqichda, faqat qat’iy tasdiqlash talab qilingan holatlarda, chegaralangan ko‘p-masshtabli namuna entropiyasi hisoblanadi. To‘rtinchi bosqichda barcha signal turlari moslashuvchan og‘irliklar bilan yagona qarorga birlashtiriladi. Beshinchi, ixtiyoriy bosqich esa taqsimlangan joylashtirish sharoitida bir nechta monitoring nuqtalari natijalarini korrelyatsiya qilish imkonini beradi.

KKEF algoritmi va matematik modeli

Birinchi bosqichning adaptiv Z-bahosi quyidagicha aniqlanadi:

$$Z_IP(t) = (H(IP_t) - \mu_IP(t)) / \sigma_IP(t),$$
$$Z_Port(t) = (H(Port_t) - \mu_Port(t)) / \sigma_Port(t)$$
$$Trigger(t): max(|Z_IP(t)|, |Z_Port(t)|) > \tau 1$$

bu yerda EWMA statistikasi faqat normal deb topilgan oynalarda yangilanadi: $\mu(t) = (1 - \lambda) \cdot \mu(t-1) + \lambda \cdot H(t)$; $\sigma(t) = (1-\lambda) \cdot \sigma(t-1) + \lambda \cdot |H(t) - \mu(t)|$. Bu cheklov tajovuzkor trafikning bazaviy statistikani ‘ifloslantirishi’ning oldini oladi.

Ikkinchi bosqichning tezkor tasdiqlash skori quyidagi ko‘rinishda hisoblanadi:

$$S2(t) = w1 \cdot |Z_IP(t)| + w2 \cdot |Z_Port(t)| + w3 \cdot \Delta Rényi(t) + w4 \cdot MI(t) + w5 \cdot D_KL(t)$$

bu yerda ΔRényi(t) $-$ Rényi spektri ($\alpha \in \{0{,}5;\ 2;\ 4\}$) bilan Shannon entropiyasi orasidagi o‘rtacha farq, MI(t) - IP va port taqsimotlari

(cc) BY dtai.uz

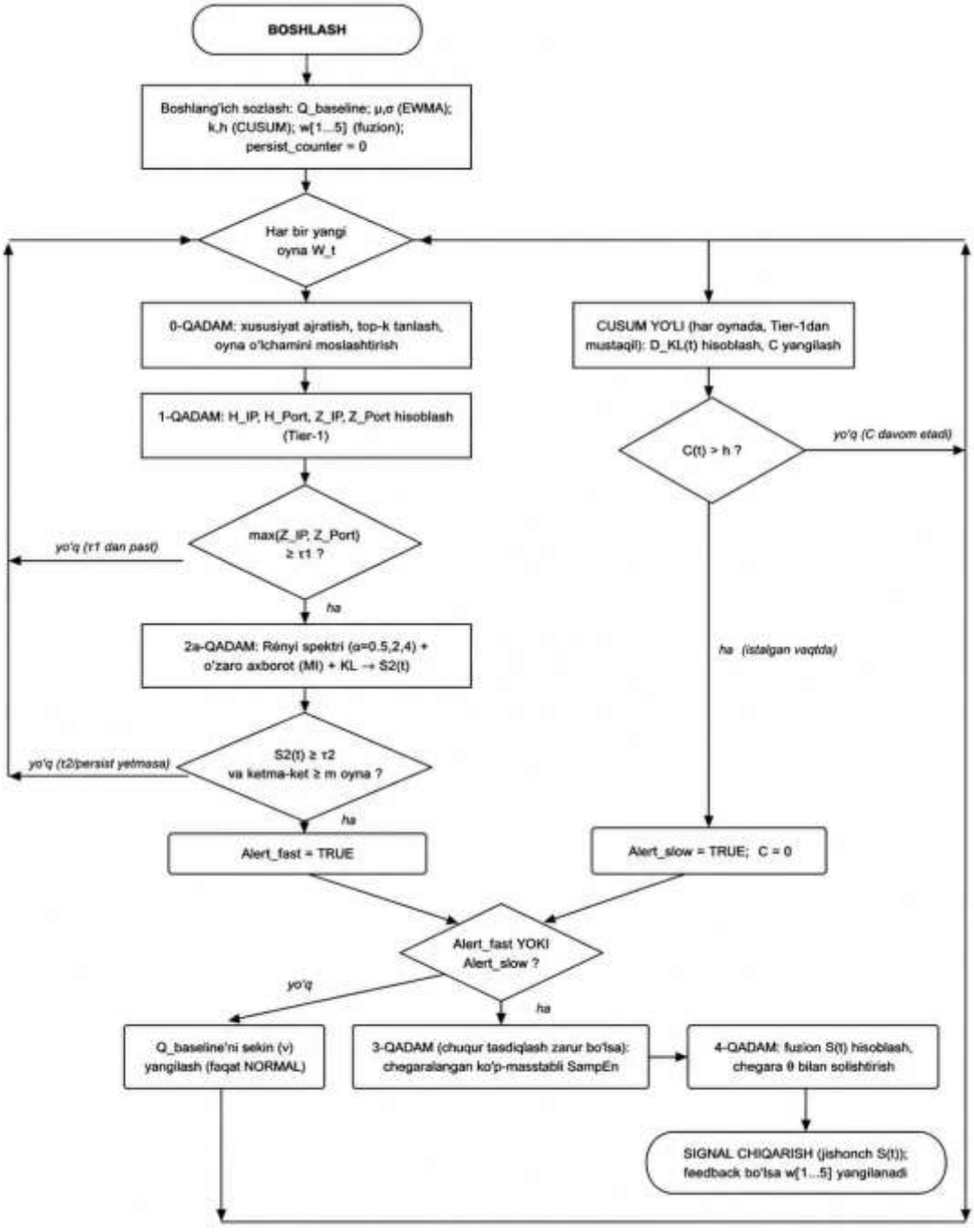
orasidagi o‘zaro axborot, D_KL(t) - Laplas silliqlash bilan hisoblangan nisbiy entropiya. Soxta signallarni bostirish uchun persistensiya sharti qo‘llaniladi: Alert_fast(t) = 1, agar $S2(\tau) > \tau 2$ sharti ketma-ket m ta oyna ($m \geq 3$) davomida bajarilsa.

Sekin drift yo‘li CUSUM jarayoni orqali amalga oshiriladi:

$$C(t) = max(0, C(t-1) + D_KL(t) - k);$$

$$Alert_slow(t) = 1, agar\ C(t) > h$$

bu yerda k - tayyorlov davridagi o‘rtacha KL qiymati asosida aniqlangan ‘erkinlik’ parametri, h - qaror oralig‘i (C(t) chegaradan oshgach nolga tushiriladi). Yakuniy qaror Alert(t) = Alert_fast(t) ∨ Alert_slow(t) ko‘rinishida shakllantiriladi, bazaviy taqsimot esa faqat normal deb topilgan holatlarda $Q(t+1) = (1-\gamma) \cdot Q(t) + \gamma \cdot P_t$ formulasi bilan sekin yangilanadi. Algo ritmning to‘liq blok-sxemasi 2-rasmda keltirilgan.



2-rasm. KKEF algoritmining blok-sxemasi

(cc) BY dtai.uz

Sintetik trafik generatsiyasi va sinov

Taklif etilgan algoritmning dastlabki baholanishi uchun sintetik tarmoq trafigi generatsiya qilindi. Trafik 1500 vaqt oynasidan iborat bo‘lib, har bir oynada 120 ta noyob manzil IP va 60 ta port toifasi Zipf taqsimoti asosida modellashtirildi - bu yondashuv haqiqiy tarmoq trafigida IP va port chastotalari taqsimotining og‘ir dumli (heavy-tailed) tabiatini aks ettiradi, bu esa Lakhina va boshqalar [12], hamda Nychis va boshqalar [13] tomonidan ham qayd etilgan. Generatsiya qilingan trafikka ettita haqiqiy hujum bloki - uchta hajm-asoslangan (DDoS), ikkita port-skanerlash va ikkita past intensivlikdagi (‘stealth’) chetlanish - hamda qirqta tabiiy tasodifiy tebranish (haqiqiy hujum emas, faqat soxta signal darajasini baholash uchun) kiritildi. Har ikkala usul (bazaviy va KKEF) sakkizta mustaqil tasodifiy seed bo‘yicha alohida ishga tushirildi va natijalar o‘rtacha hamda standart chetlanish ko‘rinishida umumlashtirildi. Sinov uslubiyoti CICIDS2017 [14] kabi standart ma’lumotlar to‘plamlarida qo‘llaniladigan real dunyo trafik xususiyatlariga (taqsimotlarning og‘ir dumliligi, aralash hujum turlari) yaqinlashtirishga qaratilgan bo‘lsa-da, u hali standart benchmark ma’lumotlar to‘plamlarida tasdiqlanmagan; bu holat 4-bo‘limda batafsil muhokama qilinadi.

Natijalar

Entropiya usullarining solishtirma tahlili

1-jadvalda o‘n uchta entropiya usulining olti mezon bo‘yicha qiyosiy tahlili keltirilgan.

1-jadval.

Entropiya usullarining ko‘p mezonli solishtirma tahlili

Usul	Murakkablik	Sozlanuvchi parametr	Vaqtinchalik tartib	Real vaqt moslik	Asosiy qo‘llanilish
Shannon	O(n)	Yo‘q	Yo‘q	Juda yuqori	Hajm-asoslangan hujumlar
Rényi	O(n)	1 (α)	Yo‘q	Yuqori	Moslashuvchan sezuvchanlik
Tsallis	O(n)	1 (q)	Yo‘q	Yuqori	Self-similar trafik
Havrda–Charvát	O(n)	1 (β)	Yo‘q	Yuqori	Ierarxik tahlil
Shartli	$O(n^2)$	Yo‘q	Qisman	O‘rta	Xususiyatlar bog‘liqligi
Birgalik	$O(n^2)$	Yo‘q	Qisman	O‘rta	Ko‘p xususiyatli anomaliya
Nisbiy (KL)	O(n)	Baza modeli	Yo‘q	Yuqori	Bazadan chetlanish
O‘zaro	O(n)	Model	Yo‘q	Yuqori	ML integratsiyasi
ApEn	$O(N^2)$	2 (m,r)	Ha	Past	Vaqtinchalik notekislik
SampEn	$O(N^2)$	2 (m,r)	Ha	Past	ApEn muqobili
Permutatsion	O(N)	1 (m)	Ha	Yuqori	Real vaqt tartib tahlili
Loyqa	$O(N^2)$	3 (m,r,n)	Ha	Past	Barqaror murakkablik
Ko‘p-masshtabli	Juda yuqori	2+	Ha	Juda past	Ko‘p masshtabli anomaliya

Jadvaldan ko‘rinib turibdiki, klassik entropiya oilasi (Shannon, Rényi, Tsallis, Havrda–Charvát) past hisoblash murakkabligi va real vaqt rejimiga yuqori moslik bilan ajralib turadi, biroq

(cc) BY dtai.uz

vaqtinchalik tartibni hisobga olmaydi. Vaqt qatoriga asoslangan usullar (ApEn, SampEn, ko‘p-masshtabli entropiya) esa yuqori sezuvchanlikka ega bo‘lsa-da, $O(N^2)$ darajasidagi hisoblash murakkabligi sababli real vaqt monitoringida cheklangan qo‘llanilishga ega. Permutatsion entropiya bundan istisno bo‘lib, past hisoblash murakkabligi (O(N)) bilan vaqtinchalik tartibni hisobga olish qobiliyatini birlashtiradi.

KKEF sinov natijalari

2-jadvalda bazaviy usullar va taklif etilgan KKEF algoritmining sakkizta sinov bo‘yicha o‘rtacha natijalari keltirilgan.

2-jadval.

Bazaviy usul va KKEF algoritmining solishtirma natijalari

Mezon	Bazaviy usul	KKEF
FAR	0.0058 ± 0.0038	0.0188 ± 0.0050
Precision	0.827 ± 0.098	0.849 ± 0.033
Recall	0.188 ± 0.003	0.780 ± 0.031
F1	0.305 ± 0.006	0.813 ± 0.025

3-jadvalda esa har ikkala usulning hujum turlari bo‘yicha aniqlash darajasi keltirilgan.

3-jadval.

Hujum turlari bo‘yicha aniqlash darajasining taqqoslanishi

Hujum turi	Bazaviy	KKEF
DDoS (3 blok)	100%	100%
Port-skanerlash (2 blok)	0%	92–100%
Low-rate ‘stealth’ (2 blok)	0%	67–80%

Minnatdorchilik

Ushbu maqola AL-9224104800 “Intellektual usullar asosida axborot-kommunikatsiya tizimlarida tarmoq hujumlarini aniqlash va himoya qilish mexanizmlarini ishlab chiqish” loyihasi doirasida chop etildi.

Xulosa

Ushbu tadqiqotda tarmoq trafigi anomaliyalarini aniqlashda qo‘llaniladigan o‘n uchta entropiya asosidagi usulning tizimli qiyosiy tahlili o‘tkazildi va ularning har biri uchun matematik asoslar, afzallik hamda kamchiliklar aniqlandi. O‘tkazilgan tahlil asosida aniqlangan umumiy kamchiliklarni - past intensivlikdagi anomaliyalarga sezuvchanlikning pastligi, sobit parametrlarga bog‘liqlik, yuqori hisoblash murakkabligi va yagona xususiyatga asoslanish - bartaraf etish maqsadida Adaptive Cascaded Multi-Entropy Fusion (KKEF) deb nomlangan yangi, besh bosqichli kaskadli algoritm ishlab chiqildi. Algoritmning arxitekturasi, to‘liq matematik modeli va blok-sxemasi taqdim etildi. Sintetik trafik ustida o‘tkazilgan hisoblash tajribasi KKEF’ning yagona entropiya usuliga asoslangan bazaviy yondashuvga nisbatan F1-mezon va Recall ko‘rsatkichlari bo‘yicha sezilarli ustunlikka ega ekanligini, soxta signal darajasining esa mutlaq qiymatda past bo‘lib qolishini ko‘rsatdi. Shu bilan birga, olingan natijalar sintetik ma’lumotlarga asoslanganligi sababli, taklif etilgan algoritmni amaliy tizimlarga joriy etishdan oldin standart ochiq ma’lumotlar to‘plamlarida qo‘shimcha tasdiqlashdan o‘tkazish zarurligi ta’kidlanadi.

Foydalanilgan adabiyotlar

1. C. E. Shannon, “A mathematical theory of communication,” Bell Syst. Tech. J., vol. 27, no. 3, pp. 379–423, 1948.
2. A. Rényi, “On measures of entropy and information,” in Proc. 4th Berkeley Symp. Mathematical Statistics and Probability, Berkeley, CA, USA, 1961, vol. 1, pp. 547–561.
3. C. Tsallis, “Possible generalization of Boltzmann-Gibbs statistics,” J. Stat. Phys., vol. 52, no. 1–2, pp. 479–487, 1988.
4. J. Havrda and F. Charvát, “Quantification method of classification processes: concept of structural α-entropy,” Kybernetika, vol. 3, no. 1, pp. 30–35, 1967.
5. S. Kullback and R. A. Leibler, “On information and sufficiency,” Ann. Math. Statist., vol. 22, no. 1, pp. 79–86, 1951.
6. S. M. Pincus, “Approximate entropy as a measure of system complexity,” Proc. Natl. Acad. Sci. USA, vol. 88, no. 6, pp. 2297–2301, 1991.
7. J. S. Richman and J. R. Moorman, “Physiological time-series analysis using

(cc) BY

approximate entropy and sample entropy," Am. J. Physiol. Heart Circ. Physiol., vol. 278, no. 6, pp. H2039–H2049, 2000.
8. C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," Phys. Rev. Lett., vol. 88, no. 17, p. 174102, 2002.
9. W. Chen, Z. Wang, H. Xie, and W. Yu, "Characterization of surface EMG signal based on fuzzy entropy," IEEE Trans. Neural Syst. Rehabil. Eng., vol. 15, no. 2, pp. 266–272, 2007.
10. M. Costa, A. L. Goldberger, and C.-K. Peng, "Multiscale entropy analysis of complex physiologic time series," Phys. Rev. Lett., vol. 89, no. 6, p. 068102, 2002.
11. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in Proc. DARPA Information Survivability Conf. and Exposition (DISCEX), Washington, DC, USA, 2003, vol. 1, pp. 303–314.
12. A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," in Proc. ACM SIGCOMM 2005, Philadelphia, PA, USA, 2005, pp. 217–228.
13. G. Nychis, V. Sekar, D. G. Andersen, H. Kim, and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection," in Proc. 8th ACM SIGCOMM Conf. Internet Measurement (IMC), Vouliagmeni, Greece, 2008, pp. 151–156.
14. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. 4th Int. Conf. Information Systems Security and Privacy (ICISSP), Portugal, 2018, pp. 108–116.
15. P. Bereziński, B. Jasiul, and M. Szpyrka, "An entropy-based network anomaly detection method," Entropy, vol. 17, no. 4, pp. 2367–2408, 2015.

(cc) BY