AXBOROTNI HIMOYA QILISH TIZIMLARINING ISHONCHLILIGI VA BARQARORLIGINI ANIQLASHDA STOXASTIK MODELLAR

Onarqulov Maqsad Karimberdiyevich

Farg‘ona davlat universiteti, Amaliy matematika va informatika kafedrasi dotsenti, O‘zbekiston

Ahadjonova Shahzoda Sharofiddin qizi

Farg‘ona davlat universiteti, Amaliy matematika mutaxassisligi 2-kurs magistranti, O‘zbekiston

Annotatsiya: Ushbu maqolada axborotni himoya qilish tizimlarining ishonchliligini va barqarorligini baholashda stoxastik modellardan foydalanish masalalari ko‘rib chiqiladi. Markov zanjirlari, Poisson jarayonlari, Weibull taqsimotlari va yashirin Markov modellari (HMM) asosida tizim xatarlarini miqdoriy tahlil qilish metodologiyasi ishlab chiqilgan. Raqamli modellashtirish natijalari va amaliy tavsiyalar keltirilgan.

Kalit so‘zlar: stoxastik jarayonlar, axborot xavfsizligi, ishonchlilik, Markov modeli, kibertahdidlar, mavjudlik ko‘rsatkichi, Weibull taqsimoti.

STOCHASTIC MODELS IN DETERMINING THE RELIABILITY AND STABILITY OF INFORMATION SECURITY SYSTEMS

Onarqulov Maqsad Karimberdiyevich

Fergana state university, Associate professor of the department of Applied mathematics and informatics, Uzbekistan

Ahadjonova Shahzoda Sharofiddin qizi

Fergana state university, 2nd year Master's student of the Applied mathematics, Uzbekistan

Abstract: This article examines the application of stochastic models for assessing the reliability and stability of information security systems. A methodology for quantitative risk analysis based on Markov chains, Poisson processes, Weibull distributions, and Hidden Markov Models (HMM) has been

developed. Numerical simulation results and practical recommendations are presented.

Keywords: stochastic processes, information security, reliability, Markov model, cyber threats, availability index, Weibull distribution.

KIRISH

Zamonaviy axborot texnologiyalari jadal rivojlanishi bilan birga kibertahdidlar ham tobora murakkablashib bormoqda. Davlat organlari, moliyaviy institutlar, sog‘liqni saqlash tizimi va boshqa muhim infrastruktura ob’ektlarida axborotni himoya qilish tizimlari (AXTS)ning uzluksiz va ishonchli ishlashi milliy xavfsizlikning ajralmas qismiga aylangan.

Biroq an’anaviy deterministik yondashuvlar real dunyo jarayonlarining tasodifiy tabiatini to‘liq aks ettira olmaydi. Nosozliklar, hujumlar va tiklash davrlari – barchasi tasodifiy hodisalar bo‘lib, ularni faqat ehtimollik nazariyasi va stoxastik jarayonlar vositalari orqali etarlicha to‘liq modellash mumkin.

Stoxastik modellashtirish – bu noaniqliklar mavjud bo‘lgan murakkab tizimlarning xatti-harakatini matematik jihatdan tavsiflovchi usullar majmuasi. AXTS ishonchliligini baholashda ushbu yondashuv quyidagilarga imkon beradi:

- ✓ nosozlik va tiklash jarayonlarining ehtimollik xarakteristikalarini hisoblash;
- ✓ tizimning turli holatlardagi vaqt ulushlarini aniqlash;
- ✓ kiberhujumlarning aniqlash va zararsizlantirish ehtimollarini modellashtirish;
- ✓ ma’lum xavfsizlik darajasini ta’minlash uchun zarur resurslarni optimallash.

STOXASTIK MODELLAR TASNIFI VA QIYOSIY TAHLILI

Asosiy modellar va ularning xususiyatlari

Axborot himoyasi sohasi uchun qo‘llaniladigan stoxastik modellar bir nechta asosiy sinfga bo‘linadi. Har bir model o‘ziga xos matematik apparatga ega bo‘lib, muayyan muammolar sinfini hal etishga mo‘ljallangan (1-jadval).

1-jadval

Stoxastik modellarning qiyosiy tavsifi

Model nomi	Parametrlar soni	Qo‘llanish sohasi	Asosiy cheklovlar
Markov zanjiri	2–5	Tizim holatlari	Eksponensial taqsimot
Erlang modeli	3–6	Navbat nazariyasi	Bir xil bosqichlar
Weibull taqsimoti	2	Ishonchlilik tahlili	Monoton xavf funksiyasi
NHPP model	2–4	Dasturiy nosozliklar	Stasionar bo‘lmagan jarayonlar
HMM modeli	4–8	Kriptografik tizimlar	Kuzatilmaydigan holatlar

Birinchi sinfga Markov zanjirlariga asoslangan modellar kiradi. Ular tizimning diskret yoki uzluksiz holatlar to‘plamida harakat qilishini tavsiflaydi, bunda kelajakdagi holat faqat hozirgi holatga bog‘liq (Markov xossasi). Bu xossa hisoblashlarni sezilarli darajada soddalashtiradi va katta o‘lchamli tizimlarni tahlil qilishga imkon beradi.

Weibull taqsimotiga asoslangan modellar asbob-uskunalar va komponentlarning eskirish jarayonlarini tavsiflashda keng qo‘llaniladi. $\beta < 1$ bo‘lganda – dastlabki nosozliklar dominantligi, $\beta = 1$ bo‘lganda – tasodifiy nosozliklar (eksponensial model), $\beta > 1$ bo‘lganda – eskirish effekti kuzatiladi.

Markov zanjirlari modeli: matematik asoslar

Uzluksiz vaqt bo‘yicha Markov zanjiri uchun tizim holatlari o‘rtasidagi o‘tish intensivliklari matritsasi Q tuziladi. Ikki holatli model (ishlamoqda / nosoz) uchun:

$$Q = \begin{vmatrix} -\lambda & \lambda \\ \mu & -\mu \end{vmatrix}$$

bu yerda λ – nosozlik intensivligi (muvaffaqiyatsizlik darajasi), μ – tiklash intensivligi. Tizimning statsionar mavjudligi (Availability) quyidagi formula orqali aniqlanadi:

$$A = \mu / (\lambda + \mu) = MTBF / (MTBF + MTTR)$$

bu yerda MTBF (Mean Time Between Failures) – nosozliklar orasidagi o‘rtacha vaqt, MTTR (Mean Time To Repair) – o‘rtacha tiklash vaqti. Ko‘p holatli

tizimlar uchun statsionar taqsimot $\pi = (\pi_0, \pi_1, ..., \pi_n)$ vektori quyidagi tenglamalar sistemasidan topiladi:

$$\pi \cdot Q = 0, \quad \Sigma \pi_i = 1$$

Ushbu sistem tizimning har qanday arxitekturasini – parallel, ketma-ket yoki aralash ulangan komponentlarni – modellashtirish imkonini beradi.

Kiber-tahdidlar modelida Poisson jarayonlari

Kiberhujumlar oqimini modellashtirish uchun norodnoqonun Poisson jarayoni (NHPP – Non-Homogeneous Poisson Process) qo‘llaniladi. Ushbu jarayonda intensivlik $\lambda(t)$ vaqtga bog‘liq bo‘ladi, bu esa hujumlar faolligining kunlik va mavsumiy o‘zgarishini aks ettiradi. [0, t] oralig‘ida kutilgan hujumlar soni:

$$\Lambda(t) = \int_0^t \lambda(s)\, ds$$

Amaliyotda ko‘pincha ikki parametrli model: $\lambda(t) = \lambda_0 \cdot e^{\wedge}(\alpha t)$ yoki sinusoidal model $\lambda(t) = \lambda_0 + A \cdot \sin(2\pi t/T)$ qo‘llaniladi. Hujumni vaqtida aniqlash ehtimoli esa quyidagicha baholanadi:

$$P(D) = 1 - exp(-\int_0^{\wedge}\tau\, \lambda\_det(s)\, ds)$$

bu yerda τ – aniqlash vaqti, λ_det(s) – aniqlash intensivligi funksiyasi.

RAQAMLI MODELLASHTIRISH NATIJALARI

Tizim mavjudligi va ishonchlilik ko‘rsatkichlari

Turli redundantlik arxitekturalariga ega tizimlar uchun mavjudlik koeffitsienti A va MTBF qiymatlari hisoblandi. Baza konfiguratsiya uchun $\lambda = 0.0012$ soat^{-1} va $\mu = 0.085$ soat^{-1} qiymatlari real axborot tizimlari statistikasidan olindi (2-jadval).

2-jadval

Turli arxitekturalardagi tizim ishonchlilik ko‘rsatkichlari

Ssenariy	λ (nosozlik darajasi)	μ (tiklash darajasi)	Mavjudlik A(%)	MTBF (soat)
Asosiy tizim	0.0012	0.085	98.62	833
Redundantlik 1:1	0.0000014	0.085	99.998	714 286
Qisman	0.00089	0.091	99.03	1123

redundantlik				
Dinamik zaxira	0.00041	0.110	99.63	2439
Gibrid arxitektura	0.000089	0.130	99.993	11 236

Natijalar shuni ko‘rsatadiki, 1:1 redundantlik bilan mavjudlik 98.62% dan 99.998% gacha oshadi, ya’ni yilik bo‘sh turish vaqti 127 soatdan atigi 10.5 daqiqaga tushadi. Gibrid arxitektura esa zarur resurslarning 2.3 barobar ko‘proq talab qilishiga qaramasdan, eng yuqori ishonchlilik ko‘rsatkichlarini ta’minlaydi.

Ikki komponentli parallel tizim uchun umumiy nosozlik intensivligi quyidagicha hisoblanadi: $\lambda\_sys = \lambda_1 \cdot \lambda_2 / (\lambda_1 + \lambda_2 + \mu_1 + \mu_2)$. Bu formula har ikkala komponent bir vaqtda nosoz bo‘lishi ehtimolini aks ettiradi.

Kiberhujumlar aniqlash tahlili

Axborot himoyasi tizimlarining barqarorligini baholashda nafaqat texnik nosozliklar, balki qasddan amalga oshiriladigan kiberhujumlar ham muhim rol o‘ynaydi. Turli turdagi hujumlar uchun stoxastik model parametrlari real hodisalar bazasidan olingan (3-jadval).

3-jadval

Kiberhujum turlari bo‘yicha stoxastik model parametrlari

Hujum turi	Aniqlash ehtimoli	Zararsizlantirish vaqti (s)	Tizim barqarorligiga ta’sir
DDoS	0.94	12–45	Sezilarli, lekin tiklanuvchi
SQL injection	0.88	3–8	Ma’lumotlar buzilishi xavfi
Man-in-the-Middle	0.79	20–90	Maxfiylik yo‘qolishi
APT hujumi	0.61	120–3600	Kritik, tizimli zarar
Zero-day exploit	0.34	Noma’lum	Juda yuqori xavf, modellashtirish murakkab

Jadvaldagi ma’lumotlardan ko‘rinib turibdiki, DDoS hujumlari eng yuqori aniqlash ehtimolliga (0.94) ega, chunki ular tarmoq trafikidagi keskin o‘zgarishlar orqali osongina aniqlanadi. Shu bilan birga, APT (Advanced Persistent Threat) va

zero-day hujumlari juda past aniqlash ehtimoli bilan tavsiflanadi va ular uchun stoxastik modellashtirish alohida murakkablik kasb etadi.

Birgalikdagi kibertahdid modeli uchun kumulyativ tavakkalchilik funksiyasi quyidagicha ifodalanadi:

$$R(t) = 1 - \prod_i [1 - F_i(t)]$$

bu yerda $F_i(t)$ – i-turdagi hujumning t vaqtgacha amalga oshirish ehtimoli, mahsulot esa barcha mustaqil tahdid manbalari bo‘yicha olinadi.

MUHOKAMA VA CHEKLOVLAR

Taklif etilgan stoxastik modellashtirish metodologiyasining quyidagi cheklovlari mavjud. Birinchidan, Markov xossasi ko‘plab real tizimlarda to‘liq bajarilmaydi – nosozlik intensivligi vaqtga bog‘liq bo‘lishi mumkin. Bu holda Weibull taqsimoti yoki yarim-Markov jarayonlari qo‘llanilishi kerak.

Ikkinchidan, model parametrlarini (λ, μ, o‘tish intensivliklari) aniqlash uchun etarli hajmdagi statistik ma’lumotlar talab etiladi. Yangi yoki noyob tizimlarda bu ma’lumotlar ko‘pincha mavjud emas yoki cheklangan.

Uchinchidan, zero-day hujumlar kabi yangi kibertahdidlar uchun oldindan parametrlash mumkin emas – bu holda Bayesian yangilanish metodlari yoki onlayn o‘rganish algoritmlari qo‘llaniladi. Shunga qaramasdan, stoxastik yondashuv deterministik baholashga nisbatan sezilarli ustunliklarni – miqdoriy aniqlik, noaniqlikni hisobga olish va optimallash imkoniyatlarini – ta’minlaydi.

XULOSA

Ushbu maqolada axborotni himoya qilish tizimlarining ishonchliligi va barqarorligini baholashda stoxastik modellarning keng doirasi ko‘rib chiqildi. Asosiy natijalarni quyidagicha umumlashtirish mumkin.

1. Markov zanjirlari tizim holatlari dinamikasini modellashtirish uchun eng universal vosita bo‘lib, ular yordamida mavjudlik koeffitsienti (A), MTBF va MTTR ko‘rsatkichlari aniq hisoblanadi.

2. Redundantlik arxitekturalari tahlili shuni ko‘rsatdiki, 1:1 zaxiralash mavjudlikni 98.62% dan 99.998% gacha oshiradi, ya’ni yilik operatsion yo‘qotishlarni taxminan 116 soatga kamaytiradi.

3. NHPP modeli kiberhujumlar oqimini o‘zgaruvchan intensivlik bilan reallistik modellash imkonini beradi va aniqlash ehtimolini aniqlash uchun integral formulalarni taqdim etadi.

4. HMM yashirin holatlarga ega murakkab kriptografik tizimlarni modellashtirish uchun mos bo‘lib, Baum-Welch algoritmi orqali real ma’lumotlardan o‘rganish imkoniyatiga ega.

5. Kompleks xatarlar matritsasi va optimallash usullarini qo‘llash orqali tizim loyihalashda xarajat va ishonchlilik o‘rtasida maqbul muvozanat topiladi.

Kelajakda ishni rivojlantirish yo‘nalishlari sifatida sun’iy intellekt algoritmlarini stoxastik modellar bilan birlashtirish, katta hajmdagi real vaqt ma’lumotlari asosida avtomatik parametr kalibrovkasi, hamda kvant hisoblash tahdidlariga nisbatan stoxastik modellashtirish ko‘rib chiqilishi maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. Trivedi K.S., Bobbio A. Reliability and Availability Engineering: Modeling, Analysis, and Applications. – Cambridge University Press, 2017. – 642 p.

2. Asmussen S., Glynn P.W. Stochastic Simulation: Algorithms and Analysis. – Springer, 2007. – 476 p.

3. Howard R.A. Dynamic Probabilistic Systems. Vol. I: Markov Models. – Dover Publications, 2007. – 608 p.

4. Rabiner L.R. A tutorial on hidden Markov models and selected applications in speech recognition // Proceedings of the IEEE. – 1989. – Vol. 77, No. 2. – P. 257–286.

5. Madan B.B. et al. A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems // Performance Evaluation. – 2004. – Vol. 56, No. 1–4. – P. 167–186.

6. Guo H., Yang X. Automatic creation of Markov reliability models for systems with complex configurations // Journal of Risk and Reliability. – 2008. – Vol. 222, No. 2. – P. 277–289.

7. Xing L., Amari S.V. Reliability of phased-mission systems // Handbook of Performability Engineering. – Springer, 2008. – P. 349–368.

8. O‘zbekiston Respublikasi Prezidentining 2022-yil 19-apreldagi PF-60-sonli Farmoni "Kiberhavfsizlik sohasini rivojlantirish strategiyasi to‘g‘risida".

9. NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. – National Institute of Standards and Technology, 2012. – 95 p.

10. Kharchenko V., Kolisnyk M., Piskachova H. Dependability of safety-critical systems and services: models, methods and case studies // IEEE Access. – 2021. – Vol. 9. – P. 47342–47356.