1%	D.T.	S.D	N.H.	NCHRP 50	P.D.	G.	C.S.
3%	S.D.	D.T.	NCHRP 50	N.H.	P.D.	C.S.	G.
6%	NCHRP 50	S.D.	D.T.	P.D.	C.S.	G.	N.H.
10%	N.H.	NCHRP 50	S.D	D.T.	P.D.	C.S.	G.
20%	S.D.	D.T.	P.D.	NCHRP 50	G.	N.H.	C.S.
40%	S.D.	D.T.	C.S.	P.D.	NCHRP 50	G.	N.H.

Қарастырылған уақыт аралығындағы зерттеліп отырған өткелдерде болған апаттың болжамды бағалары мен нақты саны арасындағы осы әдістердің бірқатар кемшіліктері анықталды:

- әр түрлі факторлардың көп саны мен әр түрлі комбинациялары бар біртекті өткел топтарын болжау үшін қолданылатын құрылыстың күрделілігі;
- жазатайым оқиғалар туралы ақпараттың болмауына байланысты жаңадан құрылған немесе қалпына келтірілген өткелдерде алынған бағалар сенімділігінің төмендеуі;
- теміржол өткелінің жеке сипаттамаларының қозғалыс қауіпсіздігіне әсерін сандық бағалау мүмкін еместігі;
- осы оқиғалардан кейін болған төтенше жағдайлар туралы ақпарат алғаннан кейін ғана қозғалу кезінде қабылданған шаралардың тиімділігіне неғұрлым негізделген баға алу;
- жазатайым оқиғалар туралы статистикалық мәліметтерді алу үшін интервалда қозғалыс сипаттамалары өзгерген жағдайда әдісті қолдану мүмкін еместігі.

Алынған нәтижелердің сенімділігін арттыру үшін болжамдау кезінде қолданылатын математикалық әдістерді одан әрі жетілдіру қажет. Құрылған математикалық әдістер қозғалысқа тән жеке сипаттамалардың көпшілігінің қозғалыс қауіпсіздігіне әсерін, қозғалыс ағындарының өзгеруінің кездейсоқ сипатын және көлік құралдарының жүргізушілерінің мінез-құлқын ескеруі керек.

Қолданылған әдебиеттер тізімі

1. Абрамов В.М., Полоцкий В.Н., Баранов Л.А., Моисеев А.А. Расчет и оптимизация координатного сближения поездов метрополитена. //Вестник ВНИИЖТа.-М.:1992.-№6.- С. 24-28с.
2. Ададуров С.Е., Гапанович В.А., Лябах Н.Н., Шабельников А.Н. Железнодорожный транспорт: на пути к интеллектуальному управлению: монография.- Ростов-на-Дону: 2009.- 322с.
3. Ададуров С.Е., Шаров В.А., Разработка технологии перевозочного процесса, обеспечивающей системное повышение скорости и надежности доставки грузов на основе экономических критериев и создания интеллектуальных железнодорожных систем// Бюллетень объединенного ученого совета М.:2010.- № 3.- С. 3-12.
4. Андрейчиков А.В., Андрейчикова О.Н. Интеллектуальные информационные системы. М.: Финансы и статистика, 2004. - 424 с.

ОӘЖ 004

АҚПАРАТТЫ САҚТАУ ЖӘНЕ ТАСЫМАЛДАУДАҒЫ ҚАТЕЛІКТІ ЗЕРТТЕУ

Ахметов Уалихан Пернебайұлы

ahmetovuali@mail.ru

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің

Информатика және ақпараттық қауіпсіздік кафедрасының
магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – т.ғ.к.,доцент Сагиндыков К.М.

Бұл мақалада ақпаратты сақтау арнасындағы қателіктердің көздері мен түрлерін анықтау үшін АСТА моделінің дискілік операциялары деңгейінде магниттік ортадағы мәліметтерді жазу және оқу процесінде ақпаратты беру ерекшеліктері қарастырылады.

Диск операцияларын өңдеудегі қателерді техникалық сипаттамаларына сәйкес екі негізгі түрге бөлуге болады:

- Мәліметтерді оқудағы қателіктер;
- құрылғының жалпы қателіктері;

Бұл бөлу дискі контроллерімен қайтарылған жұмыс нәтижесіне (жүйенің қателік коды) сәйкес орындалады. Құрылғының жалпы қателіктері көп жағдайда бүкіл құрылғының істен шығуына әкеледі, бұл осы құрылғыда жазылған барлық ақпараттың жоғалуына тең келеді. Мұндай қателіктерді түзету әдістері аппараттық резервтік көшірме жасау принциптеріне негізделген және жұмыста ескерілмеген. Деректер қателеріне мыналар кіреді:

- CRC немесе ECC басқару қателері;
- Сектор тақырыбы мен жолдың зақымдалуына байланысты қателер;

Итерациялық кодтың параметрлерін анықтау үшін АСБТ дискінің жұмыс деңгейіндегі қателіктердің статистикалық сипаттамаларын талдауы қажет. Атап айтқанда, дискі секторынан ақпаратты оқу кезінде қателіктің болу ықтималдығын, бір ақпараттық блокта бірнеше нашар секторлардың пайда болу ықтималдығын және пайда болатын қателер жиынтығының құрылымын бағалау қажет. Мұндай талдау әдебиеттерде және интернет көздерінде ұсынылмаған, декларативті жоспардың әртүрлі өндірушілердің қатты дискілері үшін қалпына келтірілмейтін қателіктің ықтималдығы 10^{-12} кем емес, ал алынатын баспа құралдары үшін температураның, ылғалдылықтың сақталуы, соққы мен электромагниттік жүктемелер болмаған кезде -10^{-6}, -10^{-12} болуы мүмкін [1].

Қателіктердің пайда болуын және таралуын тудыратын факторларды талдаймыз және ықтималдықтардың шекаралық мәндерін дербес есептейміз. Контроллердің шығуында мәліметтерді түрлендірудің (декодтаудың) екі немесе одан да көп сатысының нәтижесі пайда болады:

- Бірінші қадам - тректің атауын табу және оқу. Егер контроллер тақырыпты оқып жатқанда оқылған қатені анықтаса, онда келесі әрекеттер тоқтатылады және тиісті қате коды қайтарылады («Бөлім табылмады» немесе «Трек табылмады»). Жолда сақталған деректер толығымен жоғалған кезде, ал буфер кездейсоқ ақпаратты қамтиды.
- Екінші қадам - сектор тақырыбын іздеу және оқу. Егер контроллер қате тапса, оқу тоқтайды, сұрауды бастаған дискі деңгейінің процедурасы алмасу буферінде кездейсоқ мәліметтерді алады, ол «Сектор табылмады» қате кодымен белгіленген.
- Секторлардың мәліметтер аймағын оқу. Оқып болғаннан кейін контроллер тексеру ведомосін тексереді, ал сәйкессіздіктер туындаған жағдайда деректерді жарамсыз деп белгілейді. Қате коды - «Деректерді оқу қатесі» немесе «CRC қатесі». Алмасу буферінде қалдық ақпарат, яғни қате бар сектордың мәліметтері болады.

Нәтижесінде аралық сақтағышта сектор бойынша оқылатын ақпараттар бар (4096 биттерден тұрады) және осы ақпараттың сенімділік дәрежесі туралы қосымша ақпарат қате коды болады. Кездейсоқ және пакеттелетін кішігірім қателер кластарына (қате коды - «Мәліметтерді оқу қатесі»), буферде секторға локализацияланған үлкен қателіктер пакеттері болуы мүмкін (қате коды «Сектор табылмады» немесе «Трек табылмады»). Жалпы жағдайда баған кодының декодері жол кодын декодтау нәтижесіне әсер ете алмайды және ол декодтау мәліметтерін білмейді. Осы себепті, дискідегі қателермен оқылған сектор, келесі декодтау қадамдары үшін 4096 биттік өшіру қателіктерінің пакеті болып табылады, және дискілерді басқару деңгейіндегі ақпаратты сақтау арнасы өшіру пакеті арнасы ретінде жіктеледі [2].

Бір битті оқу кезінде қателіктің ықтималдығы (BER, Bit Error Rate)р 10^{-5}-нен 10^{-7} болғанда, сектордың оқу қатесінің ықтималдығын бағалайық: стандартты диск жетектері үшін сектордың ұзындығы 4096 бит, тақырып аймағы - 80 бит және ауданы тексеру биттері -32 және одан да көп. Нәтижесінде N=4208 бит аламыз. Ықтималдық теориясы бойынша секторда кем дегенде бір қателіктің пайда болуы төмендегі формламен есептеледі.

$$P_{\text{sec}} = \sum_{i=1}^{N} C_N^i p^i (1-p)^{n-i} \quad (1)$$

Р ықтималдығына сандық мән беретін болсақ, $8 * 10^{-3}$–тен $4 * 10^{-4}$ -не дейін секторда кем дегенде бір қателіктің пайда болу ықтималдығын аламыз.

Сектор тақырыбына зақым келгендіктен салалық қателіктер пакетінің пайда болу ықтималдығын есептейік. Үстіңгі колоннаның ұзындығы 80 бит немесе сектор ұзындығының шамамен 1/50 құрайды. Аздап оқу кезінде қателіктің ықтималдығы сектордың қызмет көрсету бөлігінде және пайдаланушылардың деректерін өсіру үшін бірдей. Сектордың тақырып аймағындағы қателіктің ықтималдығы тек деректер аймағындағы қателіктің ықтималдығынан өзгеше болатын екі дәрежелі бұйрық болып табылады және $8 * 10^{-4}...8 * 10^{-6}$ диапазонында болады. Салаға қызмет көрсету аймағында қателер орын алуы мүмкін, бұл сектордағы деректердің толық жоғалуына әкеледі.

АССЖ кодының түзету қабілетінің шекарасын анықтау үшін P_{sec} секторында қателіктің есептелген ықтималдығы $6 * 10^{-3}$ –нен $4 * 10^{-4}$ -ке дейінгі 10 сектор тобын оқығанда екі немесе одан көп сектордағы қателіктердің ықтималдығын есептейміз. Формуланы қолданайық [3]:

$$P_2 = C_{10}^2 P_{\text{sec}}^2 (1-P_{\text{sec}})^{10-2} \quad (2)$$

(2) формуласындағы P_{sec} мәндерін алмастыра отырып, 2 сектордағы қателіктердің ықтималдығы $2 * 10^{-4}$-нен $7.2 * 10^{-6}$ дейін екенін анықтаймыз. Соңғы есептеу дискіден үлкен мәліметтер блогын оқу кезінде бір уақытта екі жаман секторды алу мүмкіндігі қаншалықты жоғары екенін көрсетеді.

(2) формуласының мәндерін санау арқылы сенімділіктің талап етілетін деңгейіне $P_i < 10^{-14}$ әр кодтың бір сектордың ұзындығынан кем дегенде үш өшіру пакетін түзету мүмкіндігімен қол жеткізілгендігін тексеруге болады Pscc-тің әрбір мәніне. Кодтар тобында үшеуден көп нашар секторлардың пайда болу ықтималдығы сомасы 10^{-14} шекті мәнінен төмен, сондықтан код параметрлерін таңдағанда үш сектордың жиынтық ұзындығына назар аудару ұсынылады.

Жұмыс жетек ақауларына қарсы тұру үшін екі өлшемді итеративті кодтарды қолдануға кеңес береді, өйткені бұл кодтар қателіктерді немесе түзетулерді тиімді түрде жояды және түзетеді және оларды кодтау және декодтау алгоритмдері оңай. Ұсынылған итеративті кодтың баған коды - ГСК (n_1, m_1, d_1) $d_{\min} \geq 3$. Баған кодының j-х код топтарының биттері итерациялық кодтың бір кодтық тобына біріктірілген секторлардың j-х биттерінен тұрады. Баған кодына арналған кодек бағдарламалық түрде орындалады. Сызық коды - ақпараттың тұтастығын басқарудың (CRC / ECC) аппараттық қамтамасыз етудің коды (n_2, m_2, d_2). Контроллер пайдаланатын код көбінесе с $d_{\min 2} \geq 4$ болатын Рид-Соломон коды болып табылады және жоғары анықтау қабілетіне ие [4].

АСТА дискілерінің жұмыс деңгейіне қатысты зерттелген қателіктердің статистикасына сәйкес АСБТ кодының параметрлерін таңдаймыз:

АСБТ кодын тексеру бөлігінің минималды мөлшерін пакеттегі жинақталатын эраздармен арнадағы төрт секторды түзету үшін анықтаймыз. Өрттің теоремасын өшіру пакеттерін түзететін жағдайлар жағдайында кеңейте отырып, қалаған кодтың тексеру бөлігінің ұзындығының төменде максималды түзетілетін өшіру пакетінің L ұзындығымен шектелгенін білеміз [5].

$$K_{\min} > L \quad (3)$$

Жалпы ұзындығы бірнеше (р) өшіру пакеттерін түзету кезінде L (бір код тобында екі өшіру пакетінің пайда болу ықтималдығы өте жоғары):

$$K_{\min} > L + p \quad (4)$$

L-ді төрт секторға (4 * 4208) тең деп, р төртке тең болса, $K_{\min} > 16836$ бит > 4 секторды аламыз. Осылайша, кодтар тобының артық бөлігі сынақ бөлігінің ұзындығының көптігін, сектор көлемін ескере отырып, кем дегенде 5 сектордан тұруы керек.

Айта кету керек, әр түрлі конфигурациялардың қателіктерінің теориялық есептеулері АССЖ тестілері кезінде алынған тәжірибелік мәліметтермен толық расталған. Дискпен жұмыс жасау деңгейіндегі қателіктер туралы статистикалық мәліметтерді жинау үшін бағдарламалар пакеті іске асырылды, қабылдау тесттері аясында іргелес бірнеше секторда сәтсіздіктердің пайда болуы бірнеше рет тіркелді.

Қолданылған әдебиеттер тізімі

1. Арбо-Соренсен Р. Сбои полупроводниковых запоминающих устройств при полетах спутников. // Москва: ВИНИТИ Надёжность и контроль качества №27. 2013.-С.25-28.
2. Алексеев В.Б., Сложность умножения матриц. // Кибернетический сборник. М: Мир, 2019. - №25 - С.72-89.
3. Амербаев В.М. под ред. Теория кодирования и оптимизация сложных систем. // М.: Наука, 2017. - 217с.
4. Ахо А., Хопкрофт Дж. Построение и анализ вычислительных алгоритмов. //М.: Мир, 2016.-420 с.
5. Ахо А.В., Хопкрофт Д. Э., Ульман Д.Д. Структуры данных и алгоритмы. // М.: Вильяме, 2018.-356 с.

ОӘЖ 003.26.09

ТӨМЕН РЕСУРСТЫ КРИПТОГРАФИЯ ӘДІСТЕРІН ҚОЛ ЖЕТІМДІ БАҚЫЛАУ ЖӘНЕ БАСҚАРУ ЖҮЙЕСІНДЕ ҚОЛДАНУ

Әбілбек Ақниет Мықтыбекқызы

akniet.abilbek@mail.ru

Л.Н.Гумилев атындағы Еуразия ұлттық университеті 7М06103 магистранты

Нұр-Сұлтан қ, Қазақстан

Ғылыми жетекішісі - А.А.Муханова

Л.Н.Гумилев атындағы Еуразия ұлттық университетінің ақпараттық жүйелер кафедрасының аға оқытушысы Оспанов Руслан Маратович

Нұр-Сұлтан қ, Қазақстан

Біздің дәстүрлі криптография әдістері, мысалы, AES (шифрлау), SHA-256 (хэширлеу) және RSA/эллиптикалық қисық (қолы) сияқты, ақылға қонымды есептеу қуаты мен жад мүмкіндігі бар жүйелерде жақсы жұмыс істейді, олар ендірілген жүйелер мен сенсорлық желілер бар әлемде нашар масштабталады. Осылайша, қарапайым криптографияның көптеген мәселелерін шешу үшін криптографияның оңай әдістері ұсынылады. Бұл физикалық өлшеммен, өңдеу талаптарымен, жадының шектелуімен және энергия шығынымен байланысты шектеулерді қамтиды.

AES және SHA компьютерлік жүйелерде жақсы жұмыс істейді. Дегенмен, ресурстары шектеулі құрылғылар үшін көптеген жеңіл криптографиялық примитивтер ұсынылды және қолданылды. Ұлттық (NIST) және халықаралық (ISO / IEC) ұйымдар жеңілдетілген криптография үшін қолдануға болатын және Internet of Things (IoT) және radio frequency identification (RFID) құрылғыларында пайдалы болуы мүмкін бірқатар әдістерді сипаттайды [1]. Олар құрылғы спектрін келесідей анықтайды:

- Әдеттегі криптография. Серверлер мен десктоптар; планшеттер мен смартфондар.
- Жеңіл криптография. Орнатылған жүйелер; RFID және сенсорлық желілер.