Çoxkanallı telekommunikasiya sistemlərində informasiyanın kriptomühafizəsinin bəzi aspektləri

Bayram İbrahimov[1], Tural Məmmədov[2]
[1]Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
[2]AR Silahlı Qüvvələrinin Hərbi Akademiyası, Bakı, Azərbaycan
[1]*i.bayram@mail.ru*

***Xülasə*— Məqalədə çoxkanallı telekommunikasiya sistemlərində abunəçi və şəbəkə rabitə xətlərinə icazəsiz qoşulmalardan mühafizə etmək üçün informasiyanın veriliş üsulları və kriptomühafizə vasitələri analiz edilir. Telekommunikasiya sistemlərində informasiya təhlükəsizliyinin bəzi aspektlərinə baxaraq, kriptoqrafik sistemlərdə parolların dayanıqlığının ehtimal-zaman xarakteristikalarının qiymətləndirilməsi üçün analitik ifadələr verilmişdir.**

Açar sözləri — telekommunikasiya sistemləri, icazəsiz qoşulma, ehtimal-zaman xarakteristikaları, kriptomühafizə, informasiyanın mühafizəsi, parol, kriptoqrafiya sistemləri

I. GİRİŞ

Müasir dövrdə perspektiv informasiya və kompüter texnologiyalarının imkanlarından səmərəli istifadə etməklə gələcək nəsil rabitə şəbəkələrinin arxitektur konsepsiyası bazasında qurulmuş telekommunikasiya sistemlərinin informasiya təhlükəsizliyinin təmin edilməsini tələb edir. Bu baxımdan dövlətin, idarələrin və kommersiya strukturalı müəssisələrin informasiya sirlərinin saxlanılması və mühafizəsi problemləri telekommunikasiya sistemlərində, rabitə kanallarında və xidmət sferalarında mühüm əhəmiyyət kəsb edir.

Çoxkanallı telekommunikasiya sistemlərində və şəbəkələrində məlumatların qəbulu, emalı və onların böyük tutumlu yaddaş sistemlərinə yığılması, rabitə kanalları vasitəsi ilə lazım olduqda ötürülməsi, veriliş traktının istənilən qov-şağına qoşulma prosesləri və qəbulu zamanı bütün tip məlumatların kriptomühafizəsi məsələləri böyük aktuallığa malik istiqamətlərdən hesab olunur [1].

Aparılmış uzunmüddətli tədqiqatlarda rabitə şəbəkələrinin abunəçi və şəbəkə traktına icazəsiz qoşulmaların təşkili və onların aşkar edilməsi məsələsinə baxılmış [1, 2, 3] və müəyyən edilmişdir ki, şəbəkənin bütün perimetri boyunca istənilən formada sistemə müdaxilə oluna bilər və məlumatın götürülməsi mümkündür [4].

Telekommunikasiya şəbəkələri və sistemlərində informasiyanın qorunması – kriptomühafizəsi, icazəsiz qoşulmaların təşkili, məlumatın sirlərinin aşkarlanması, təhlükəsizliyi məsələlərinə geniş baxılır [5]. Lakin çoxkanallı telekommunikasiya sistemlərində göstərilən istiqamətlərə nəzəri, texniki və texnoloji aspektdən baxılması və nəzəri cəhətdən əsaslandırmanın bəzi aspektlərinin təhlilinə yer ayrılmasına xüsusi önəm verilir.

Yuxarıda qeyd olunanları nəzərə alaraq, təqdim olunan iş çoxkanallı telekommunikasiya sistemlərində informasiyanın kriptomühafizəsinin bəzi aspektlərinə həsr edilmişdir.

II. ABUNƏÇİ VERİLİŞ TRAKTINA İCAZƏSİZ QOŞULMA ÜSULLARININ TƏHLİLİ

İlkin olaraq telekommunikasiya sistemləri nöqteyi-nəzərincə informasiya mənbəyindən – məlumat alana kimi çoxkanallı veriliş traktında abunəçi xəttinə icazəsiz qoşulma üsullarının təhlilini nəzərdən keçirək.

Telekommunikasiya sistemlərində abunəçi çoxkanallı veriliş traktına icazəsiz qoşulma üsulları aşağıdakılardır [1, 3]:

1. Abunəçi və şəbəkə terminallarına əlavə və gizli qoşulma üsulu;
2. Veriliş prosesi zamanı abunəçi veriliş xətlərinə əlavə olaraq paralel icazəsiz qoşulma üsulu;
3. Müdafiəsiz halda gizli olaraq (nəzarətsizlik olduğu hallarda, evlərdə, idarələrdə və s. yerlərdə) abunəçi terminalları və veriliş sistemlərini mənimsəmək üsulu;
4. Abunəçi taktında telefon xətlərinə və modemlərə əlavə olaraq gizli-pirat variantda veriliş prosesinə qoşulma üsulu;
5. Abunəçi veriliş traktına və rabitə kanallarına, naqilsiz və naqilli, dar- və genişzolaqlı icazəsiz qoşulma üsulları.

Yuxarıda göstərilmiş icazəsiz qoşulma üsulları telekommunikasiya sistemlərində məlumatların kriptomühafizəsi və müdafiəsi aspektlərini dəyişdirməyə vadar edir. Yəni icazəsiz qoşulma üsullarına uyğun olaraq, kriptomühafizə və müdafiə məsələləri də müxtəlif olurlar.

Qeyd edək ki, aparılmış təcrübələr göstərir ki, abunəçi veriliş traktına, kommutasiya sisteminə və rabitə kanallarına icazəsiz qoşulma üsulları məlumatın qorunması baxımından ən mühüm qovşaqlar və ya manqalar hesab edilir. Lakin bunlarla yanaşı, çoxkanallı veriliş sisteminə icazəsiz qoşulma üsullarında iki variant böyük əhəmiyyət kəsb edir:

a) Çoxkanallı telekommunikasiya sistemlərinin rabitə kanallarında kriptomühafizənin təşkili alqoritmi və vasitələri;

b) Mübadilə olunan məlumata əvvəldən-sona kimi traktında kriptomühafizənin təmin edilməsi.

Aparılmış təhlillər göstərir ki, telekommunikasiya sistemlərində abunəçi çoxkanallı veriliş traktına icazəsiz

DOI: 10.25045/NCInfoSec.2019.51

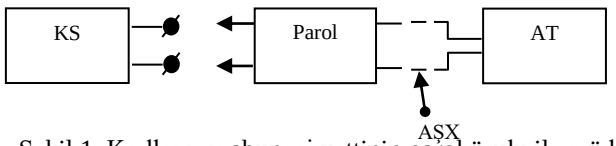
qoşulmaya qarşı müdafiənin səmərəliliyini yüksəltmək üçün elektrik rabitə sistemlərində kriptomühafizə üsulları və onların terminal vasitələrinin iş prinsipini öyrənmək vacib aspektlərdən hesab edilir.

III. TELEKOMMUNİKASİYA SİSTEMLƏRİNDƏ KRİPTOMÜHAFİZƏ ÜSULLARI VƏ ONLARIN TERMİNAL VASİTƏLƏRİ

Hal-hazırda şəhər telefon rabitəsinə yeni rəqəm tipli elektron kommutasiya sistemlərinin tətbiqində kpirtomühafizə məsələləri əvvəlki sistemlərlə müqayisədə çox sadələşdirilmişdir [4]. Buna səbəb isə rəqəm tipli elektron kommutasiya sistemlərinin idarəetmə məsələləri proqram üsulu ilə yerinə yetirilir və hər bir abunəçinin xətti uyğun olaraq kodlarla və proqram təminatı ilə daima nəzarətdə saxlanılır və mühafizə olunur.

Qeyd olunanlarla yanaşı, telekommunikasiya sistemlərində kriptoqrafiya məsələsi – abunəçi xətlərinin «parol» üsulu ilə müdafiəsi yerinə yetirilir. Bu üsulun bazasında zond terminalı yaradılmış və yerli, şəhərlərarası və beynəlxalq rabitənin təşkili zamanı bütün icazəsiz qoşulmalara nəzarət edilir və daima idarəetmə sistemləri ilə əlaqədə olaraq, nəzarətdə saxlanılır və şəbəkə üzrə monitorinqi aparılır.

Belə bir müdafiə üsulunda abunəçi xətlərin (AX) kodlanması – «parolu» böyük əhəmiyyət kəsb edir. Bu üsulun məğzi ondan ibarətdir ki, hər bir abunəçi xətti xüsusi 2 və 3 elementli kodlarla kodlanır və parolu tapılır. Əgər kod və parol düzgün olmadıqda abunəçi sistemi kommutasiya mərkəzindən bloklanır və qoşulmaya qadağa qoyulur. Abunəçi xəttinin müdafiəsi üçün «Parol» üsulunun sadə sxemi şəkil 1-də göstərilmişdir.



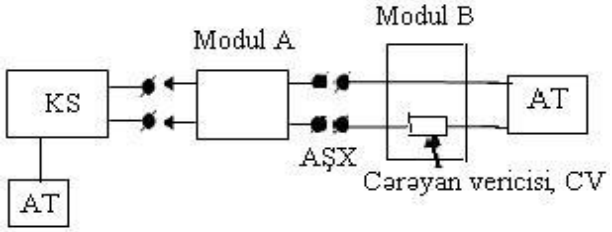
Şəkil 1. Kodlanmış abunəçi xəttinin parol üsulu ilə müdafiəsi sxemi

Müdafiə sxemi kommutasiya sistemindən (KS), abunəçi şleyf xəttindən (AŞX) və abunəçi terminaldan (AT) və ya istifadəçinin sadə telefon aparatından (TA) ibarətdir. Sistemdaxili rabitə zamanı KS-dən abunəçi xətinə məlum olmayan parametrli siqnallar daxil olmaqla «Parol» açılır və AT-a qoşulur. Bu zaman gərginlik U = 120 V, siqnalın tezliyi 25 Hs, gecikmə müddəti isə 50 msan olar. Qoşulma pauza müddətində yerinə yetirilir – abunəçi bunu hiss etmir. Əgər yenidən qoşulmaq istəsə, onda yenə də 2 və ya 3 elementli kodu yığmaqla, yenidən icazəsiz qoşula bilər.

Baxılan sadə hal üçün AŞX-sxemdə kriptomüdafiə elementi kimi istifadə olunur və (0,5-1,5) km məsafə üçün nəzərdə tutulur.

Belə sistemlərdə kriptomühafizəni yüksəltmək məqsədi ilə – «Parol» cərəyan vericisi (CV) tezlik üsulu ilə kodun ötürülməsi üsulundan istifadə olunur. Şəkil 2 abunəçi xəttinə «Parol-CV» üsulu ilə kriptomühafizə sxemi verilmişdir.

Sxemdə modul-A KS-də yerləşdirilmiş, modul – B isə abunəçi tərəfdə qoyulmuşdur və cərəyan vericisi ilə birlikdə fəaliyyət göstərir



Şəkil 2. Mühafizə kodun tezlik üsulu ilə ötürülməsində Parol-CV üsulunun sxemi

B-modulu avtomatik olaraq, A-moduluna tezlik impulslu kodlar ötürür. A-modulu daxil olmuş kodu tanıyaraq, stansiyanın cavab siqnalını, nömrənin yığılması və birləşməsini təşkil etməyə icazə verir. Belə sxemin köməyi ilə telekommunikasiyada yüksək səviyyədə kriptomühafizə əməliyyatı yerinə yetirilir.

İndi isə naqılsiz rabitə sisteminə və telefon aparatlarına icazəsiz qoşulma zamanı kriptomühafizə məsələsinə baxaq. Müxtəlif firma və şirkətlər tərəfindən, o cümlədən Panasonic, Premier, Motorola və s. abunəçi terminalın identifikasiya üçün sadə kodlardan istifadə olunur.

Baxılan hal üçün kriptoqrafiya sistemlərində istifadə olunan parol – rəqəm, söz, işarələrin gizli kombinasiyası olub, informasiya təhlükəsizliyində istifadəçinin autentifikasiyası üçün geniş istifadə edilir. Parol subyektin autentitifikatorudur, autentikasiyanın ən geniş yayılmış növüdür. Burada, autentifikasiya istifadəçinin sistemdə izlənməsi məqsədilə subyekt və ya obyektlərə daxilolma identifikatorunun verilməsi və ya təqdim edilmiş identifikatorun mövcud identifikatorlar siyahısı ilə müqayisəsi hesab olunur.

Çoxkanallı telekommunikasiya sistemlərində istifadə olunan N_p – parol əlifbasının gücü, yəni parolların tərtibi zamanı istifadə edilən ümumi işarələrin sayını nəzərə alsaq, parolun minimal uzunluğu L_p aşağıdakı bərabərsizliklə təyin edilir:

$$L_p \geq [\ell og_2 S / \ell og_2 N_p], \qquad (1)$$

burada S – kriptoqrafiya sistemlərində istifadə olunan parolların bütün mümkün sayıdır və parolun təhlükəsiz istifadə olunma müddətindən asılı olaraq belə ifadə olunur:

$$S = 2T_t / t_y, \qquad (2)$$

burada t_y – bir parolun yığılma müddətidir.

Sonuncu (1) və (2) ifadələri çoxkanallı telekommunikasiya sistemlərində istifadə olunan parolların tərtibi zamanı istifadə edilən ümumi işarələrin sayını və təhlükəsiz istifadə olunma müddətini qiymətləndirməyə imkan verən riyazi ifadələrdir.

Baxılan hallar üçün telekommunikasiya sistemlərində prosesin təkrar olunmaması üçün müxtəlif olmaqla kodların ümumi sayı 256-dan çox götürülür.

Müasir dövrdə kriptoqrafiya sistemləri üçün naqilsiz terminallarda parollarla idarə olunan nəzarət sxemlərindən istifadə etməklə tam etibarlı müdafiə sistemi təşkil olunmuşdur. Bu nəzarət sxemləri parolların düzgün seçilməsi hesabına efir üzrə abunəçi xətinin bütün növ qoşulmalardan müdafiə edir və məlumatların ötürülməsi zamanı təhlükəsizliyini lazımı səviyyədə təmin edir.

IV. KRİPTOQRAFİYA SİSTEMLƏRİNDƏ PAROLLARIN MÜHAFİZƏYƏ DAYANIQLIĞININ QİYMƏTLƏNDİRİLMƏSİ

Kriptoqrafiya sistemlərində müxtəlif məqsədlər üçün istifadə olunan parolların mühafizəsinin etibarını artırmağa imkan verən alqoritmləri, tədbirləri və alətləri nəzərə almaq vacib istiqamətlərdən biri hesab edilir. Bunun üçün ilk növbədə sistemdə audentifikasiya və identifikasiyasını nəzərə almaq mühüm əhəmiyyət kəsb edir.

Çoxkanallı telekommunikasiya sistemlərində autentifikasiya – sistemə daxil olmaq üçün təqdim etdiyi identifikatorun ona məxsusluğunun yoxlanması yolu ilə subyekt və ya obyektin əsilliyinin-həqiqiliyinin təsdiq olunmasıdır. Bu zaman daxil edilmiş parol və istifadəçi üçün əvvəlcədən təyin olunan parol müqayisə edilir. Onlar üst-üstə düşdükdə istifadəçinin həqiqiliyi təsdiqlənmiş sayılır.

Qeyd edək ki, parolların ən başlıca təhlükəsi onların elektron ələ keçirilməsidir. Bunun üçün ilk növbədə parol kiçik və baş hərflər, rəqəmlər və durğu işarələrinin qarışığından olmaqla, $L_p \geq L_{p.\max}$ maksimal uzunluqda tərtib edilib və tez-tez dəyişilməlidir.

Adətən, çoxkanallı telekommunikasiya sistemlərində parolların etibarlığı və fəaliyyət müddətinin idarə olunması üçün parolun əsas xarakteristikalarının qiymətləndirilməsi tələb olunur.

Fərz edək ki, sistemdə N – sayda əlifbadakı işarələrdən, yəni simvollardan istifadə olunmuşdur. Bəzən N – parol əlifbasının gücü də hesab olunur, bir sözlə N – parolların tərtibi zamanı əlifbada istifadə edilən simvolların sayıdır.

Tutaq ki, kriptoqrafiya sistemlərində N gücünə malik L_p uzunluqlu parollardan istifadə olunub. Bu zaman parolların bütün mümkün ola bilən sayı belə bir düsturla təyin oluna bilər [3]:

$$S = N^{L_p} \tag{3}$$

Fərz edək ki, mətnin daxiletmə sürəti V_m , onda L_p uzunluğuna malik olan bir parolun yığılma vaxtı aşağıdakı kimi qiymətləndirilə bilər:

$$t_y = \frac{L_p}{V_m} \tag{4}$$

Kriptoqrafiya sistemlərində N gücünə malik L_p uzunluqlu parolun fəaliyyət müddətini T_t ilə işarə edək. Belə olduğu halda istənilən parolun tapılma ehtimalı aşağıdakı ifadə ilə təyin olunur:

$$P = \frac{T_t}{N^{L_p} \cdot (L_p / V_m)} \tag{5}$$

(4) və (5) ifadələrini nəzərə alsaq, parolun təhlükəsiz istifadə müddətini aşağıdakı ifadə ilə qiymətləndirmək olar:

$$T_t = \frac{0{,}5 L_p \cdot N^{L_p}}{V_m} \tag{6}$$

Beləliklə, sonuncu ifadələr kriptoqrafiya sistemlərində parolların mühafizəyə dayanıqlığının qiymətləndirilməsi üçün alınmış analitik ifadələr hesab olunur və bir çox telekommunikasiya sistemlərində istifadə edilə bilər.

NƏTİCƏ

Çoxkanallı telekommunikasiya sistemlərində informasiyanın kriptomühafizəsinin bəzi aspektləri təhlil edilən zaman abunəçi veriliş traktina icazəsiz qoşulma üsullarına baxılmış və kriptoqrafiya sistemlərində parolların dayanıqlığının ehtimal-zaman xarakteristikalarının qiymətləndirmək üçün analitik ifadələr alınmışdır.

İSTİNADLAR

[1] İbrahimov B.Q. Elektrik rabitə nəzəriyyəsi. AzTU, Bakı, 2016. – 382 s.

[2] Ibrahimov B. G., Humbatov R.T., Ibrahimov R.F. "Analysis of information encryption methods in multichannel telecommunication systems," Proceedings of the 4-th International Scientific Conference on Actual multidisciplinary scientific-practical problem of informatıon security, pp. 18-21, 2018.

[3] Шаврин С.С. Защита информации в многоканальных телекоммуникационных систем. М.: МТУСИ. 2002. - 62 с.

[4] Тихонов, С.В. Универсальный метод защиты блочных шифров от побочных атак по цепям питания // Проблемы информационной безопасности. Компьютерные системы.– 2017. № 3.- с.48-55.

[5] Fragouli C, Soljanin E. Network coding. Foundations and Trends // Networking. V.2, No.1, 2007. -P.1–134.

SOME ASPECTS OF CRYPTOCURRENCY INFORMATION IN MULTICHANNEL TELECOMMUNICATION SYSTEMS

Bayram Ibrahimov[1], Tural Mammadov[2]

[1]Azerbaijan Technical University, Baku, Azerbaijan

[2]An associate of the Military Academy of the Republic of Azerbaijan, Baku, Azerbaijan

[1]*i.bayram@mail.ru*

Abstract: Multichannel telecommunication systems are reviewing data transmission and cryptocurrency analysis to protect subscribers and unauthorized access to network communication lines. Analyzes are given to evaluate the probability characteristics password persistence in cryptographic systems, while looking at some aspects information security in telecommunication systems.

Keywords: *telecommunications systems, unauthorized access, probability characteristics, cryptographic protection, information security, password, cryptographic systems.*