პაკეტების უსაფრთხო მარშრუტიზაციის ალგორითმების შემუშავება კომპიუტერულ ქსელებში

მიხეილ დონაძე
კომპიუტერულ მეცნიერებათა დეპარტამენტის ასოცირებული პროფესორი
ელ-ფოსტა: mikheil.donadze@bsu.edu.ge

1. შესავალი. ინფორმაციული უსაფრთხოება ინტეგრირებული უსაფრთხოების ერთ-ერთი ყველაზე მნიშვნელოვანი ასპექტია, რა დონეზეც არ უნდა მივიჩნიოთ ეს უკანასკნელი: ეროვნული, ინდუსტრიული, კორპორატიული თუ პირადი [1], [2].

აქ მნიშვნელოვანია არა იმდენად ინდივიდუალური გადაწყვეტილებები (კანონები, სასწავლო კურსები, პროგრამული და აპარატურის პროდუქტები), რომლებიც პერიოდულად განიცდის განახლებას, არამედ ახალი გადაწყვეტილებების გენერირების მექანიზმები, რომლებიც საშუალებას გვაძლევს ვიცხოვროთ ტექნიკური პროგრესის ტემპით. ინფორმაციული უსაფრთხოება ახლა არა მხოლოდ უკიდურესად მნიშვნელოვანი, არამედ ძალიან მოდური და მომგებიანი საქმიანობის სფეროა. სავსებით ბუნებრივია, რომ აქ მრავალი დეპარტამენტის, კომპანიისა და პიროვნების ინტერესები ეჯახება, არის ბრძოლა გავლენის სფეროებისთვის, ზოგჯერ კი გადარჩენისთვის. ორგანიზაციის დაკავშირება გლობალურ ქსელთან, როგორიცაა ინტერნეტი, მნიშვნელოვნად ზრდის ორგანიზაციის ეფექტურობას და უხსნის მას ბევრ ახალ შესაძლებლობებს. ამავდროულად, ორგანიზაციამ უნდა იზრუნოს ინფორმაციული რესურსების დაცვის სისტემის შექმნაზე, რა თქმა უნდა ვისაც სურს მათი გამოყენება, შეცვლა ან გაუმჯობესება. მიუხედავად სპეციფიკისა, ორგანიზაციის უსაფრთხოების სისტემა გლობალურ ქსელებში მუშაობისას უნდა იყოს მიმართული ინფორმაციული რესურსების უსაფრთხოების უზრუნველყოფისკენ [2].

ასეთ სიტუაციაში ინფორმაციული უსაფრთხოების უზრუნველსაყოფად აუცილებელია ახალი მიდგომების ძიება. ერთ-ერთი ასეთი სფეროა საკომუნიკაციო ქსელში აბონენტებს შორის ინფორმაციის გაცვლის მარშრუტების მართვა [5].

TCP/IP სტეკი არ არის სრულიად უსაფრთხო და იძლევა მასზე სხვადასხვა ტიპის შეტევების საშუალებას. ასეთი შეტევების განსახორციელებლად, თავდამსხმელს უნდა ჰქონდეს წვდომა ინტერნეტთან დაკავშირებულ ერთ-ერთ სისტემაზე. ეს შესაძლებელია, მაგალითად, იმ შემთხვევაში, როდესაც თავდამსხმელმა „გატეხა“ რაიმე სისტემა ან იყენებს ინტერნეტ ქსელში ჩართულ კომპიუტერს [3].

TCP/IP-ზე თავდასხმები ზოგადად იყოფა ორ ტიპად: პასიური და აქტიური. პასიური შეტევების დროს TCP დონეზე თავდამსხმელის მოქმედება მთავრდება ხელმისაწვდომი მონაცემების ან კომუნიკაციის სესიების მონიტორინგით. მოსმენა მოიცავს ქსელის ნაკადის ჩაჭრას და მის ანალიზს [3], [4].

ვინაიდან TCP/IP ტრაფიკი, როგორც წესი, არ არის დაშიფრული, თავდამსხმელს შესაბამისი ხელსაწყოების გამოყენებით შეუძლია „გადაიჭიროს“ TCP/IP პაკეტების სესიები და ამოიღოს მომხმარებლის სახელები და პაროლები.

უნდა აღინიშნოს, რომ ამ ტიპის თავდასხმის მიგნება შეუძლებელია, რადგან ქსელის ნაკადი არ იცვლება. თავდამსხმელები ხშირად იყენებენ პასიურ სკანირებას, რათა გაარკვიონ თუ რომელ TCP პორტებში მუშაობენ დომენები, რომლებიც პასუხობენ ქსელის მოთხოვნებს. რეგულარული

სკანერის პროგრამა აჩვენებს კავშირებს სხვადასხვა პორტებთან დამოკიდებულებაში და შემტევს აცნობებს პორტის ნომრებს.

შეტყობინებების პაკეტების მარშრუტიზაციის არსებულ მეთოდებს აქვს მთელი რიგი უარყოფითი მხარეები, მათ შორის ქსელის სტრუქტურის ცვლილებებთან ადაპტაციის ნაკლებობა, კომუნიკაციის დაბალი უსაფრთხოება და მრავალი სხვა. გადაცემის მარშრუტის არჩევა ნიშნავს სატრანზიტო ქსელის კვანძების თანმიმდევრობის განსაზღვრას, რომლების მეშვეობითაც უნდა გადაიცეს შეტყობინებები ადრესატამდე. ამ შემთხვევაში, მარშრუტის არჩევა ხორციელდება პროვაიდერი ოპერატორების ქსელის კვანძებში. უსაფრთხოების დაბალი დონის მქონე ასეთი კვანძების არსებობა ქმნის ქსელში შემოჭრის წინაპირობებს, რაც იწვევს კომუნიკაციის უსაფრთხოების დაქვეითებას. სემინარზე შემუშავებული მიდგომები და წარმოდგენილი ალგორითმი მიზნად ისახავს კომუნიკაციის უსაფრთხოების გაზრდას ქსელის აბონენტებს შორის ინფორმაციის გაცვლის მარშრუტების მართვის გზით [2].

ტექნიკური არსით ყველაზე ახლოს სემინარზე წარმოდგენილ მოდელთან არის „როუტერში მიზნობრივად გამოსაყენებელი მარშრუტის არჩევის მეთოდი ქსელში თანაბარი კომუტაციისათვის“. მეთოდი შედგება მარშრუტების ხარისხის კრიტერიუმების შემცველი საწყისი მონაცემების წინასწარ დაყენებაში. ინფორმაცია საკომუნიკაციო ქსელის სტრუქტურის შესახებ ინახება როუტერში, მათ შორის ქსელის კვანძების მისამართები და მათ შორის კავშირები. იქმნება შესაძლო საკომუნიკაციო მარშრუტების ნაკრები. ქსელის სამიზნე მისამართისთვის შეტყობინების მიღების შემდეგ, წინასწარ განსაზღვრული მარშრუტის ხარისხის კრიტერიუმების მიხედვით ირჩევა ერთი მარშრუტი და შეტყობინებები გადაიცემა არჩეული მარშრუტის გასწვრივ [6].

თუმცა, ამ მეთოდის მინუსი არის კომუნიკაციის შედარებით დაბალი უსაფრთხოება საკომუნიკაციო ქსელში აბონენტების ინფორმაციის გაცვლის არჩეული მარშრუტის გამოყენებისას [7].

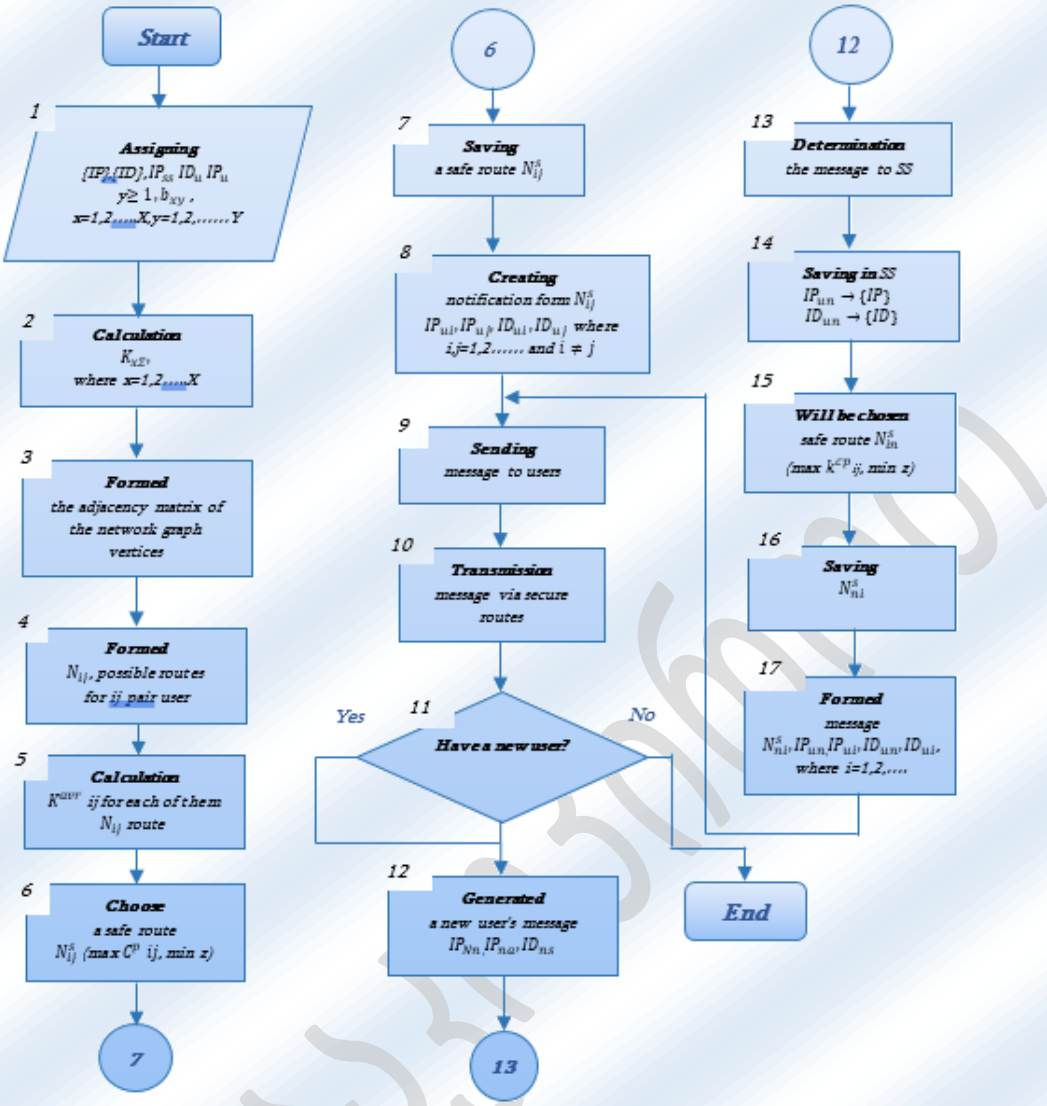
შეტყობინებების პაკეტების უსაფრთხო მარშრუტიზაციის ალგორითმი. საკომუნიკაციო ქსელში უსაფრთხო მარშრუტის არჩევის ალგორითმი წარმოდგენილია ორი ვერსიის სახით. პირველი ვერსია განიხილავს საკომუნიკაციო ქსელს, რომლის კვანძები ერთმანეთთან შეიცავს $X \geq 2$ კავშირებს. ქსელის კვანძებს წინასწარ ენიჭება საწყისი მონაცემები, და ჩაიწერება ინფორმაცია საკომუნიკაციო ქსელის სტრუქტურის შესახებ, ქსელის კვანძების IP_{Nn} მისამართების ჩათვლით და მათ შორის კავშირის არსებობის შესაძლებლობით. იქმნება N შესაძლო საკომუნიკაციო მარშრუტების ნაკრები, საიდანაც აირჩევა ერთი მარშრუტი, რომლითაც უსაფრთხოდ გადაიცემა შეტყობინებები.

N_{ij} რომელიც წარმოადგენს საკომუნიკაციო ქსელის გრაფის ხეს და ასახავს მარშრუტებს ქსელს i და j აბონენტებს შორის და გამოითვლება ფორმულით:

$$N_{ij} = B_0 * B_0^T,$$

სადაც $B_o = M * K$ - საკომუნიკაციო ქსელის ამსახველი გრაფის მეზობელი წვეროების მატრიცაა, ხოლო $M = M_p - 1$, K- შესაბამისად, მატრიცის სტრიქონების და სვეტების რაოდენობა, M_p - ორიგინალური მატრიცის მიმდებარე რიგების რაოდენობა და უდრის საკომუნიკაციო ქსელის კვანძების საერთო რაოდენობას; B_0^T -კი B_o ტრანსპონირებული მატრიცა.

ალგორითმის მეორე ვერსია განიხილავს საკომუნიკაციო ქსელს, რომლის კვანძები ერთმანეთთან შეიცავს $X \geq 2$ კავშირებს. ქსელის კვანძებს წინასწარ ენიჭება საწყისი მონაცემები და ჩაიწერება ინფორმაცია საკომუნიკაციო ქსელის სტრუქტურის შესახებ, ქსელის კვანძების IP_{Nn} მისამართების ჩათვლით და მათ შორის კავშირის არსებობის შესაძლებლობით. იქმნება N შესაძლო საკომუნიკაციო მარშრუტების ნაკრები, საიდანაც აირჩევა ერთი მარშრუტი, რომლითაც უსაფრთხოდ გადაიცემა შეტყობინებები.



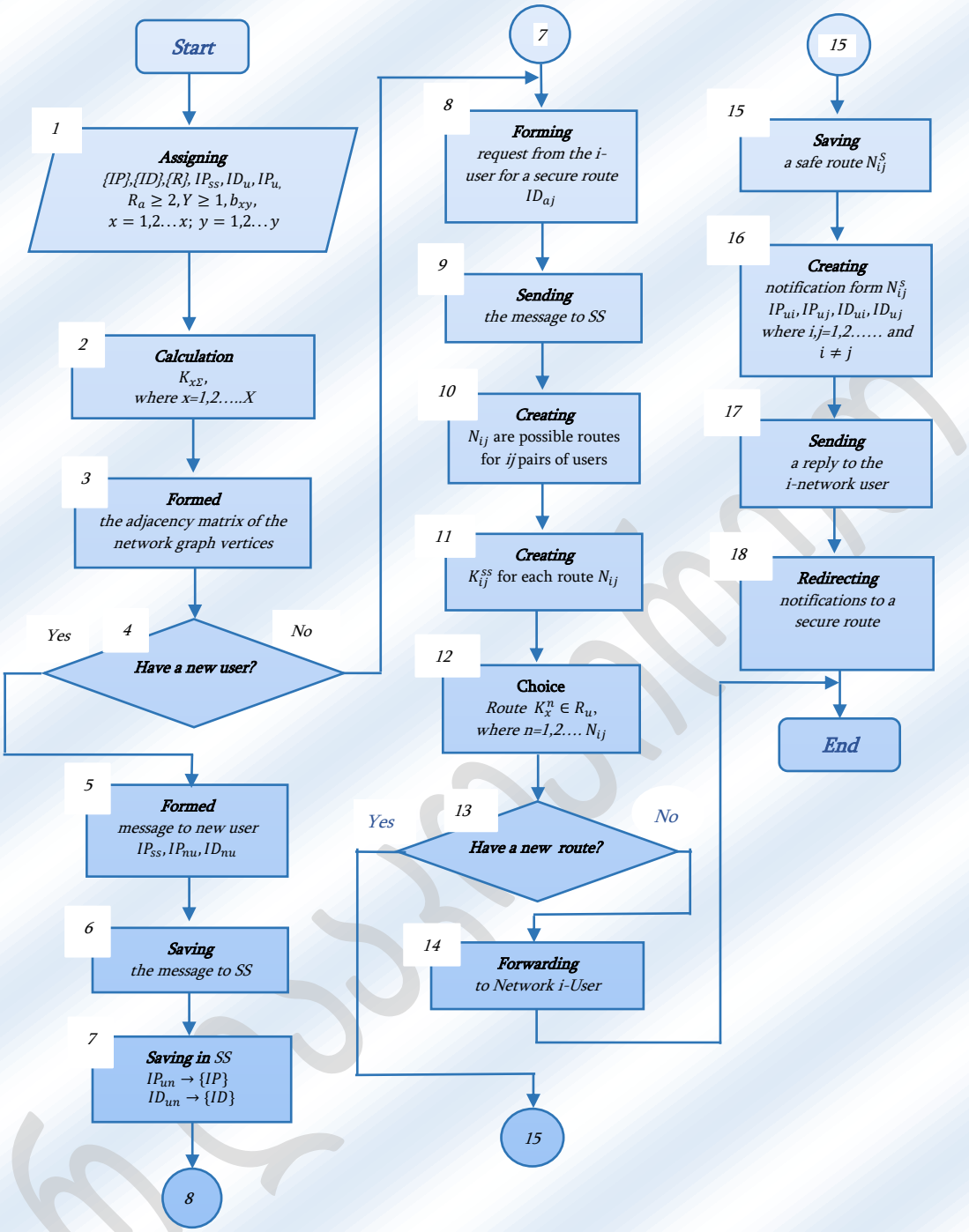
ნახ.1 შეტყობინებების პაკეტების უსაფრთხო მარშრუტიზაციის ალგორითმის პირველი ვერსიის ბლოკ-სქემა

წინა ალგორითმისგან განსხვავებით წინასწარ განსაზღვრულ საწყის მონაცემებში, ქსელის სტრუქტურულ და საიდენტიფიკაციო მასივებთან, დასაშვები მარშრუტის უსაფრთხოების ინდიკატორთან და უსაფრთხოების სერვერის IP_{Nn} მისამართთან ერთად დამატებით მითითებულია ქსელში გადასაცემი ინფორმაციის შესაბამისი რანგების R_{inf} და ქსელის კვანძების $k_{x\Sigma}$ კომპლექსური უსაფრთხოების ინდიკატორები.

ქსელის i და j აბონენტებს შორის საკომუნიკაციო ქსელის გრაფი მარშრუტების რაოდენობა N_{ij} გამოითვლება ფორმულით:

$$N_{ij} = |B_o \times B_o^T|$$

სადაც არის $B_o = M * K$ - საკომუნიკაციო ქსელის ამსახველი გრაფის მეზობელი წვეროების მატრიცა, ხოლო $M = M_p - 1$, K - შესაბამისად, მატრიცის სტრიქონების და სვეტების რაოდენობა, M_p - ორიგინალური მატრიცის მიმდებარე რიგების რაოდენობა და უდრის საკომუნიკაციო ქსელის კვანძების საერთო რაოდენობას; B_0^T -კი B_o-ს ტრანსპონირებული მატრიცას.



ნახ.2 შეტყობინებების პაკეტების უსაფრთხო მარშრუტიზაციის ალგორითმის მეორე ვერსიის ბლოკ-სქემა

უსაფრთხო მარშრუტიზაციის ალგორითმების მუშაობის პრინციპი. როგორც ცნობილია საკომუნიკაციო ქსელში აბონენტებს შორის ინფორმაციის გაცვლის უზრუნველსაყოფად, ქსელის აბონენტებს შორის შესაძლო მარშრუტების ნაკრებიდან უნდა მოხდეს ერთი უსაფრთხო საკომუნიკაციო მარშრუტის შერჩევა. შეტყობინებების გადაცემის მარშრუტის არჩევა ნიშნავს სატრანზიტო ქსელის კვანძების თანმიმდევრობის დადგენას, რომლის მეშვეობითაც უნდა მოხდეს შეტყობინებების გადაცემა. მარშრუტის განსაზღვრა რთული ამოცანაა, განსაკუთრებით მაშინ, როდესაც წყვილ აბონენტებს შორის ბევრი სავარაუდო მარშრუტია. მარშრუტების განსაზღვრის ამოცანა მოიცავს შესაძლო ნაკრებიდან ერთი ან რამდენიმე მარშრუტის არჩევას გარკვეული კრიტერიუმის მიხედვით. მარშრუტის შერჩევის არსებულ მეთოდებში, როგორც წესი, შერჩევის კრიტერიუმებია მაგალითად: ნომინალური გამტარუნარიანობა, საკომუნიკაციო

არხების გადატვირთულობა, არხების მიერ შემოტანილი შეფერხებები, ქსელის შუალედური სატრანზიტო კვანძების რაოდენობა, არხების და ქსელის სატრანზიტო კვანძების საიმედოობა. უმეტეს შემთხვევაში უსაფრთხო მარშრუტის არჩევის დროს არსებობს ერთგვარი წინააღმდეგობა კომუნიკაციის უსაფრთხოების უზრუნველყოფის მოთხოვნასა და არსებულ მეთოდებს შორის. შემოთავაზებული მეთოდი (ვარიანტები) მიზნად ისახავს ამ წინააღმდეგობის აღმოფხვრას. შესაბამისად წარმოდგენილი მეთოდის პირველი ვერსია რეალიზებულია შემდეგნაირად.

ზოგად შემთხვევაში, ნახ. 3 ნაჩვენები საკომუნიკაციო ქსელი წარმოადგენს 1. X ქსელის კვანძების, 2. უსაფრთხოების სერვერის, 3. ქსელის აბონენტების, 4. გაერთიანებული ფიზიკური საკომუნიკაციო ხაზების ერთობლიობას. ქსელის X კვანძების რაოდენობა ორზე მეტია ან ტოლია $R_a \geq 2$. ყველა ეს ელემენტი განისაზღვრება იდენტიფიკატორებით, რომლებიც გამოიყენება TCP/IP პროტოკოლების ყველაზე გავრცელებულ სტეკში, როგორც ქსელის IP მისამართები. აბონენტებისა და ქსელის კვანძების საკომუნიკაციო ქსელთან დამაკავშირებელი მისამართების ნაკრები არ იკვეთება. ქსელის აბონენტებს შორის შეტყობინებების გადაცემა ხორციელდება ქსელის კვანძების მეშვეობით და მათ შორის კავშირი შერჩეულია, როგორც ყველაზე უსაფრთხო ყველა შესაძლო საკომუნიკაციო მარშრუტიდან. ქსელის ელემენტებს შორის კავშირები ხასიათდება მხოლოდ ორი მნიშვნელობით, კავშირის არსებობა და მისი არარსებობა. საკომუნიკაციო ხაზების დარჩენილი პარამეტრები განიხილება, როგორც მუდმივი და მხედველობაში არ მიიღება, რადგან საკომუნიკაციო ქსელში ინფორმაციის გაცვლის უნებართვო თვალთვალის ყველაზე სავარაუდო და უფრო ადვილად განხორციელებული მეთოდი არის კავშირი მის კვანძებთან. ნახ.1. გვიჩვენებს მოქმედებების თანმიმდევრობის ბლოკ სქემას, რომელიც ხორციელდება შემუშავებული მეთოდის საკომუნიკაციო ქსელში უსაფრთხო მარშრუტის არჩევის პირველ ვარიანტში, სადაც შემოღებულია შემდეგი აღნიშვნები:

{IP} - სტრუქტურული მასივი;

{ID} - საიდენტიფიკაციო მასივი;

IP_{SS} - უსაფრთხოების სერვერის ქსელის მისამართი;

ID_b- აბონენტის ID; IP_b - აბონენტის ქსელის მისამართი;

Y - ქსელის კვანძების უსაფრთხოების განსახილველი პარამეტრების რაოდენობა;

b_{xy} - x ქსელის კვანძის უსაფრთხოების y პარამეტრის მნიშვნელობა, სადაც x = 1.2,…,X, y = 1.2,…,Y;

$K_{x\Sigma}$ - თითოეული x ქსელის კვანძის უსაფრთხოების კომპლექსური მაჩვენებელი;

N_{ij} - საკომუნიკაციო ქსელის გრაფიკის ხეების რაოდენობა, რომელიც შეესაბამება i და j ქსელის აბონენტებს შორის შესაძლო საკომუნიკაციო მარშრუტების სიმრავლეს, სადაც i = 1.2,…, j = 1,2,…, და $i \neq j$;

K_{ij}^{cp} - ქსელის i და j აბონენტებს შორის საკომუნიკაციო მარშრუტის უსაფრთხოების საშუალო მაჩვენებელი;

N_{ij}^{S} - უსაფრთხო საკომუნიკაციო მარშრუტი ქსელის i და j აბონენტებს შორის;

Z_n- n გრაფის ხის წვეროების რაოდენობა, სადაც n = 1,2,…, N_{ij}, შესაბამისი ქსელის კვანძების რაოდენობას;

SS - უსაფრთხოების სერვერი.

მეორე ვერსიაში ნახ.2. შემოღებულია შემდეგი დამატებითი აღნიშვნები:

{R} - შესაბამისობის მასივი აბონენტთა R_a რიგებსა და ქსელის კვანძების $k_{x\Sigma}$ უსაფრთხოების კომპლექსურ მაჩვენებლებს შორის და R_b - ქსელის აბონენტების რანგები.

საწყის ეტაპზე, უსაფრთხოების სერვერზე დაყენებულია საწყისი მონაცემები, მათ შორის

სტრუქტურული *{IP}* და საიდენტიფიკაციო *{ID}* მასივები, უსაფრთხოების სერვერის მისამართი IP_{ss}, იდენტიფიკატორები ID_a და საკომუნიკაციო ქსელში ჩართული აბონენტების IP_a მისამართები, ასევე უსაფრთხოების პარამეტრები თითოეული *X* ქსელის კვანძისთვის, სადაც $x = 1,2,\ldots,X$, $Y \geq 2$ და მათი მნიშვნელობა b_{xy}, სად $y = 1,2,\ldots,Y$, რომლებიც მოცემულია ცხრილში 1.

სტრუქტურული მასივი *{IP}* – ინახავს მონაცემებს IP_{SS} უსაფრთხოების სერვერის, IP_{Nn} კვანძების და IP_a ქსელის აბონენტების მისამართების, აგრეთვე ინფორმაციის მათ შორის კავშირის არსებობის შესახებ, (ცხრილი 5) რომელიც ხასიათდება, მხოლოდ ორი მნიშვნელობით, "1" - კავშირის არსებობა და "0" - მისი არარსებობა.

ცხრილი 1

y / x	1	2	...	Y
1	b_{11}	b_{12}		b_{1y}
2	b_{21}	b_{22}		b_{2y}
...				
X	b_{x1}	b_{x2}		b_{xy}

ცხრილი 2

	IP_{SS}	IP_{n1}	IP_{n2}	IP_{n3}	IP_{n4}	IP_{n5}	IP_{ni}	IP_{nj}	IP_{nn}
IP_{SS}		1	0	0	0	0	0	0	0
IP_{n1}	1		1	1	1	0	0	0	0
IP_{n2}	0	1		0	1	1	1	0	0
IP_{n3}	0	1	0		1	1	0	1	0
IP_{n4}	0	1	1	1		1	0	0	1
IP_{n5}	0	0	1	1	1		0	0	0
IP_{ni}	0	0	1		0	0		0	0
IP_{nj}	0	0	0	1	0	0	0		0
IP_{nn}	0	0	0	0	1	0	0	0	

საიდენტიფიკაციო მასივი *{ID}* - მასივი ინახავს მონაცემებს ID_{SS} უსაფრთხოების სერვერის იდენტიფიკატორების, საკომუნიკაციო ქსელის აბონენტების ID_a-ის და ქსელის აბონენტების შესაბამისი IP_a მისამართების და IP_{SS} უსაფრთხოების სერვერის მისამართების შესახებ (ცხრ. 3).

ცხრილი 3

ქსელში ჰოსტის მისამართი	ქსელში ჰოსტის იდენტიფიკატორი
IP_{SS}	$ID_{უს}$
IP_{ai}	ID_{ai}
IP_{aj}	ID_{aj}
. . .	. . .
IP_{an}	ID_{an}

ქსელის კვანძების უსაფრთხოების პარამეტრები განისაზღვრება, ISO/IEC JTC 1/SC 27 აღიარებული სტანდარტების საფუძველზე.

ქსელის b_{x1} კვანძების უსაფრთხოების $y = 1$ პარამეტრის მნიშვნელობები განისაზღვრება, ქსელის კვანძების მოწყობილობების მწარმოებლების მახასიათებლებით, რომელთა შესახებ ინფორმაცია შესაძლებელია მიიღოთ ფიზიკური მისამართებიდან. მაგალითად, ვთქვათ N_{n1} კვანძისთვის, რომლის ფიზიკური მისამართი პირობითად შეიძლება იყოს 00:01:e3:3F:D4:E1, პირველი სამი მნიშვნელობა

განსაზღვრავს მწარმოებელს, რომელიც შეესაბამება უსაფრთხოების პარამეტრის მნიშვნელობას b_{11} = 0.3. ანალოგიურად, განისაზღვრება უსაფრთხოების პარამეტრის b_{x1} მნიშვნელობები *Nn2- Nn5* ქსელის კვანძების $y = 1$, ისევე როგორც ყველა მოცემული $Y \geq 2$ უსაფრთხოების პარამეტრის b_{xy} მნიშვნელობები.

ქსელის თითოეული X კვანძისთვის, მისი უსაფრთხოების b_{xy} პარამეტრებზე დაყრდნობით გამოითვლება უსაფრთხოების კომპლექსური ინდექსის $k_{x\Sigma}$ მნიშვნელობები. გამოთვლილი მაჩვენებლები წარმოდგენილია ცხრილში 4.

ცხრილი 4

ქსელის კვანძი	k_Σ
1	$k_{1\Sigma}$
2	$k_{2\Sigma}$
x	$k_{x\Sigma}$
X	$K_{X\Sigma}$

უსაფრთხოების კომპლექსური ინდექსი $k_{x\Sigma}$ ქსელის თითოეული x კვანძისთვის გამოითვლება ან შეჯამებით $k_{x\Sigma} = \sum_{y=1}^{y} b_{xy}$ ან გამრავლებით $k_{x\Sigma} = \prod_{y=1}^{y} b_{xy}$ ან კვანძის b_{xy} უსაფრთხოების პარამეტრების საშუალო არითმეტიკულით $k_{x\Sigma} = (\sum_{y=1}^{y} b_{xy})/y$.

უსაფრთხოების კომპლექსური ინდექსის $k_{x\Sigma}$ გამოთვლის მეთოდი პრინციპულად არ მოქმედებს უსაფრთხო მარშრუტის არჩევის შედეგზე. უსაფრთხოების კომპლექსური ინდექსის $k_{x\Sigma}$ გამოთვლილი მნიშვნელობები საკომუნიკაციო ქსელის განხილული ვარიანტის თითოეული x კვანძისთვის, შესაბამისი უსაფრთხოების პარამეტრების b_{xy} მნიშვნელობების გათვალისწინებით მოცემულია ცხრილი.5-ში.

ცხრილი.5 b_{xy} კვანძების მოცემული მნიშვნელობები

ქსელის კვანძი X = 5	უსაფრთხოების მაჩვენებელი Y = 3				x-კვანძის უსაფრთხოების კომპლექსური მაჩვენებელი $k_{x\Sigma}$		
	y = 1	y = 2	y = 3		$\sum b_{xy}$	$\prod b_{xy}$	$(\sum b_{xy})/Y$
x = 1	0,3	0,13	0,4		0,83	0,0156	0,276666667
x = 2	0,3	0,16	0,4		0,86	0,0192	0,286666667
x = 3	0,2	0,1	0,34		0,64	0,0068	0,213333333
x = 4	0,5	0,2	0,25		0,95	0,025	0,316666667
x = 5	0,05	0,08	0,01		0,14	0,00004	0,046666667

შემდეგ, ხდება ქსელის გრაფის მეზობელი წვეროების მატრიცის ფორმირება, რომლისთვისაც ქსელის კვანძების *IPss* მისამართები და ქსელის აბონენტების IP_a მისამართები თავსდება სტრუქტურულ მასივში, ასევე ინფორმაცია კვანძებსა და ქსელს აბონენტებს შორის კომუნიკაციის (კავშირების) არსებობის შესახებ. ცნობილია გრაფის მეზობელი წვეროების მატრიცის გენერირების მეთოდები (იხ., მაგალითად, სასრული გრაფები და ქსელები. R. Basaker, T. Saaty, M, 1973, 368c.). განხილული საკომუნიკაციო ქსელის გრაფის მეზობელი წვეროების მატრიცას ექნება შემდეგი სახე:

ცხრილში 6

		$ქვ_1$	$ქვ_2$	$ქვ_3$	$ქვ_4$	$ქვ_5$
	$ქვ_1$	0	1	1	1	0
	$ქვ_2$	1	0	0	1	1
b=	$ქვ_3$	1	0	0	0	1
	$ქვ_4$	1	1	0	0	1
	$ქვ_5$	0	1	1	1	0

ამის შემდეგ, საიდენტიფიკაციო მასივში გროვდება ქსელის ID_a, *IDss* იდენტიფიკატორები და

შესაბამისად ქსელის აბონენტების და უსაფრთხოების სერვერის IP_a და IP_{SS} მისამართები.

საკომუნიკაციო გრაფის ყოველი n-ური ხე, სადაც $n = 1,2,\ldots, N_{ij}$, შედგება z_n წვეროებისგან, რომლებიც შეესაბამება ქსელის კვანძების რაოდენობას. ქსელის i და j აბონენტებს შორის საკომუნიკაციო ქსელის გრაფში ხეების მთლიანი რაოდენობა N_{ij} შეიძლება განისაზღვროს სხვადასხვა მეთოდით. წარმოდგენილ მეთოდში საკომუნიკაციო გრაფის ხეების მთლიანი რაოდენობის N_{ij}-ს ფორმირება ხდება მატრიცის მეზობელი წვეროების გამოყენებით.

B მატრიცის ნებისმიერი მწკრივის წაშლით, მივიღებთ B_0 საწყის და მასთან ტრანსპონირებულ B_0^T მატრიცას:

$$B_o = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}; B_o^T = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

N_{ij} ხეების რაოდენობის გამოთვლა საკომუნიკაციო ქსელის გრაფის i და j აბონენტებს შორის ხდება მიღებული B_0 და B_0^T მატრიცების გამრავლებით და შემდეგ მისი დეტერმინანტის მოძიებით.

$$N_{ij} = \left|B_o \times B_o^T\right| = \begin{pmatrix} 3 & 2 & 2 & 1 \\ 2 & 2 & 2 & 0 \\ 2 & 2 & 3 & 1 \\ 1 & 0 & 1 & 3 \end{pmatrix} = 5$$

საკომუნიკაციო ქსელის გრაფის ხეზე დაყრდნობით აბონენტებს შორის საკომუნიკაციო მარშრუტების აგება გულისხმობს ყველა შესაძლო საკომუნიკაციო მარშრუტის პოვნას, ე.ი. გამორიცხავს ჩაკეტილ მარშრუტებს, რომლებიც მიუღებელია შეტყობინების გადაცემისთვის.

შესაძლო უსაფრთხო საკომუნიკაციო მარშრუტის დასაბუთება და ობიექტურად არჩევა N_{ij}=5 ნაკრებიდან ქსელის i და j აბონენტებს შორის ხდება უსაფრთხოების საშუალო მაჩვენებლის k_{ij}^{SS} გამოთვლით. იგი მიიღება, როგორც ქსელის კვანძები უსაფრთხოების კომპლექსური მაჩვეენებლი, ანუ საშუალო არითმეტიკულის გამოთვლით k_{Σ}^{n}, და მოიცავს კავშირის n საკომუნიკაციო მარშრუტს $k_{ij}^{SS} = (\sum k_{\Sigma}^{x})/z_n$.

ქსელის კვანძების უსაფრთხოების კომპლექსური მაჩვენებლის სხვადასხვა გზით გამოთვლის შედეგად, გამოითვლება ქსელის i და j აბონენტებს შორის ფორმირებული საკომუნიკაციო მარშრუტები საშუალო უსაფრთხოების მაჩვენებელით k_{ij}^{SS}. შედეგები წარმოდგენილია ცხრილში 7.

ცხრილი 7. ქსელის კვანძების უსაფრთხოების კომპლექსური მაჩვენებლის მნიშვნელობები

მარშრუტი N_{ij} = 5	ქსელის კვანძები n-მარშრუტზე	Z_n ქსელის კვანძების რიცხვი n-ურ მარშრუტზე	n-ური მარშრუტის უსაფრთხოების საშუალო მაჩვენებელი		
n = 1	123	3	0,78	0,0139	0,26
n = 2	1234	4	0,82	0,0167	0,27
n = 3	12345	5	0,68	0,0133	0,23
n = 4	235	3	0,55	0,0087	0,18
n = 5	2345	4	0,65	0,0128	0,22

N_{ij}^{s} ქსელის i და j აბონენტებს შორის უსაფრთხო მარშრუტს არჩევა ხდება მისი უსაფრთხოების საშუალო მაჩვენებლის k_{ijn}^{SS} ყველაზე მაღალი მნიშვნელობის საფუძველზე. თუ მოიძებნა რამდენიმე მარშრუტი თანაბარი უსაფრთხოების საშუალო მაჩვენებლის თანაბარი მნიშვნელობით, ამ შემთხვევაში ნაპოვნი მარშრუტებიდან აირჩევა უმოკლესი მარშრუტი, ე.ი. მარშრუტი მასში Z_n კვანძების ყველაზე მცირე რაოდენობით. ამის შემდეგ ხდება არჩეული მარშრუტის დამახსოვრება. ცხრილში წარმოდგენილი

შედეგებიდან ჩანს, რომ გაანგარიშების ყველა მეთოდისთვის, მეორე $n = 2$ მარშრუტის აქვს უსაფრთხოების საშუალო ინდექსის ყველაზე მაღალი მნიშვნელობები k_{ij}^{cp}, რომლებიც შესაბამისად გამუქებულია. შეიძლება დავასკვნათ, რომ $k_{x\Sigma}$ გაანგარიშების მეთოდი, არ მოქმედებს უშუალოდ უსაფრთხო მარშრუტის არჩევის შედეგზე, ამ სახით ფორმირდება ქსელის ყველა აბონენტს შორის მარშრუტების ყველა შესაძლო ვარიანტების ნაკრები.

შედეგი, გენერირდება შეტყობინებებით, რომლებიც მოიცავს დამახსოვრებულ მარშრუტებს N_{ij}^{S} i და ყველა j აბონენტს შორის, ID_{aj} იდენტიფიკატორებს და ყველა j აბონენტის IP_{3j} მისამართებს. ამის შემდეგ გენერირებული შეტყობინებები ეგზავნება ქსელის ყველა i - აბონენტს. ამრიგად, ქსელის თითოეულ აბონენტს ეგზავნება შეტყობინება უსაფრთხო მარშრუტების შესახებ რომელის შესაძლებელია დამყარდეს ქსელის ყველა სხვა დანარჩენ აბონენტებს შორის.

აბონენტებს შორის შეტყობინებების გადასაცემად აბონენტ-მიმღების იდენტიფიკატორის მიხედვით შეტყობინების ID_a შეირჩევა მისი IP_a მისამართით და აბონენტამდე უსაფრთხო N_{ij}^{S} მარშრუტის მიხედვით, რის შემდეგაც შეტყობინება გადაეცემა მიმღებ აბონენტს. ცნობილი მარშრუტიზაციის პროტოკოლები, როგორიცაა RIP, OSPF, NLSP, BGP ემსახურება მომხმარებლის ინფორმაციის გადასცემს (source specified routing) მარშრუტიზაციის მეთოდით და უზრუნველყოფენ ინფორმაციის გაცვლას წყარო მიმღებიდან მოცემულ მარშრუტზე. ამრიგად, აბონენტებს აქვთ შესაძლებლობა, გაგზავნონ შეტყობინებები უშუალოდ მოცემული უსაფრთხო მარშრუტის მიხედვით. როდესაც ახალი აბონენტი უკავშირდება საკომუნიკაციო ქსელს, მისთვის გენერირდება შეტყობინება, რომელიც შეიცავს ქსელის N_{n4} კვანძის IP_{n4} მისამართს, მიმღების ID_{an} იდენტიფიკატორს და მიმღების IP_{an} მისამართს. გენერირებული შეტყობინება იგზავნება უსაფრთხოების სერვერზე, სადაც ის ინახება სტრუქტურულ და საიდენტიფიკაციო მასივებში, რითაც აახლებს ინფორმაციას საკომუნიკაციო ქსელის უსაფრთხოების სერვერში, ზემოთ აღწერილი მეთოდის მსგავსად, შეირჩევა და ინახება უსაფრთხო საკომუნიკაციო მარშრუტები ახალ აბონენტსა და ქსელის ყველა j აბონენტს შორის.

შემდეგ ეტაპზე ფორმირდება შეტყობინება, რომელიც მოიცავს ინფორმაცია, ქსელის სტრუქტურისა და აბონენტების შესახებ. გენერირდება შეტყობინებები, მათ შორის შენახული ინფორმაცია უსაფრთხო საკომუნიკაციო მარშრუტების შესახებ, ქსელის თითოეული j აბონენტიდან ახალ აბონენტამდე და იგზავნება ქსელის j აბონენტთან. ამრიგად, ქსელის ახალ აბონენტს ეცნობება უსაფრთხო მარშრუტების შესახებ ქსელის ყველა დანარჩენ აბონენტთან, ხოლო დანარჩენ აბონენტებს ეცნობება ქსელის ახალი აბონენტთან შესაძლებელი უსაფრთხო მარშრუტების შესახებ.

ამრიგად მეთოდის პირველ ვერსიაში, საკომუნიკაციო ქსელის სტრუქტურის შესახებ ინფორმაციის დაყენებით, საწყისი მონაცემებით ქსელის კვანძებისა და აბონენტების შესახებ და ქსელის კვანძების უსაფრთხოების კომპლექსური მაჩვენებლების გაანგარიშებით, ხდება უსაფრთხო მარშრუტების არჩევა. საკომუნიკაციო ქსელში აბონენტებს შორის კომუნიკაციის უსაფრთხოების გაზრდა მიიღწევა ინფორმაციის გაცვლის მარშრუტების მართვით.

მეთოდის მეორე ვარიანტსა და პირველს შორის განსხვავება შემდეგია. მეთოდის ამ ვერსიაში შემოტანილია ახალი ცნება ქსელის აბონენტების რანგები. ქსელის აბონენტებს შორის უსაფრთხო მარშრუტის არჩევა ხორციელდება მხოლოდ აბონენტის მოთხოვნით და ქსელის აბონენტთა წინასწარ განსაზღვრული რანგების შესაბამისად. უსაფრთხო საკომუნიკაციო მარშრუტის არარსებობის შემთხვევაში, აბონენტს ეცნობება ამის შესახებ.

ნახ. 2-ზე წარმოდგენილია მოქმედებების თანმიმდევრობის ბლოკ-სქემა, რომელიც ასახავს წარმოდგენილი მეთოდის, საკომუნიკაციო ქსელში უსაფრთხო მარშრუტის შერჩევის მეორე ვერსიას.

საწყის ეტაპზე, ანალოგიურად, როგორც მეთოდის პირველ ვარიანტში, საწყისი მონაცემები მითითებულია უსაფრთხოების სერვერზე.

საწყის მონაცემებში, მეთოდის პირველი ვარიანტისგან განსხვავებით, დასაშვები მარშრუტის უსაფრთხოების ინდექსი k^{perm} არ არის მითითებული. გარდა ამისა, მეთოდის მეორე ვარიანტთან შედარებით, შემოტანილია აბონენტების R_a რანგის {R} შესაბამისობის მასივი და ქსელის კვანძების $k_{x\Sigma}$ უსაფრთხოების კომპლექსური მაჩვენებლები. მასივი {R} შეიცავს ქსელის კვანძების $R_a \geq 2$ აბონენტის

რანგების და უსაფრთხოების კომპლექსური ინდიკატორების $k_{x\Sigma}$ შესაბამის მნიშვნელობებს. მაგალითად, აბონენტის რანგი $R_a = 1$ შეესაბამება ქსელის კვანძების უსაფრთხოების რთული ინდიკატორების $k_{x\Sigma}$ მნიშვნელობებს 0-დან 0.2-მდე. საწყისი მონაცემების დაყენების შემდეგ, ანალოგიურად, როგორც მეთოდის მესამე ვარიანტში, თითოეული x ქსელის კვანძისთვის, უსაფრთხოების კომპლექსური მაჩვენებელი $k_{x\Sigma}$ გამოითვლება მისი უსაფრთხოების პარამეტრების b_{xy} მნიშვნელობებიდან. გამოთვლილი ინდიკატორები მოცემულია ცხრილში.

შემდგომში, ისევე როგორც პირველ ვარიანტში, იქმნება ქსელის გრაფის წვეროების მიმდებარე მატრიცა. ახალი აბონენტის საკომუნიკაციო ქსელთან დაკავშირების შემთხვევაში, ისევე როგორც მეთოდის მესამე ვარიანტში, მისთვის გენერირდება შეტყობინება, რომელიც შეიცავს ქსელის კვანძის $NS4$ $IPns_4$ მისამართს, რომელზედაც ის არის დაკავშირებული და თავისივე იდენტიფიკატორების ID_{an} და IP_{an} მისამართებს. გენერირებული შეტყობინება იგზავნება უსაფრთხოების სერვერზე, სადაც ის ინახება სტრუქტურულ და საიდენტიფიკაციო მასივებში, რითაც ავსებს (ახლებს) ინფორმაციას საკომუნიკაციო ქსელის სტრუქტურისა და ქსელის აბონენტების შესახებ. შემდეგ ყალიბდება შეტყობინება, რომელიც შეიცავს აბონენტ-მიმღების იდენტიფიკატორს ID_a, ანალოგიურად, როგორც წარმოდგენილი მეთოდის მესამე ვარიანტში, შეირჩევა მისი მისამართი IP_a და უსაფრთხო მარშრუტი N_{ij}^s , რის შემდეგაც შეტყობინება გადაეცემა მიმღებ აბონენტს მოცემულ მარშრუტზე.

გარდა ამისა, რაც შემოთავაზებული იყო მეთოდის მესამე ვარიანტში სადაც, i და j ქსელის აბონენტებს შორის შესაძლო საკომუნიკაციო მარშრუტების ნაკრები იქმნება საკომუნიკაციო ქსელის გრაფის N_{ij} ხეების სახით. მეთოდის მესამე ვარიანტისგან განსხვავებით, უსაფრთხო კომუნიკაციის მარშრუტი N_{ij}^s ქსელის i- და j-აბონენტებს შორის, შეირჩევა ისეთ შემთხვევაში, თუ მასში შემავალი კვანძების უსაფრთხოების კომპლექსური ინდიკატორები $k_{nx\Sigma}$ შეესაბამება ქსელის i აბონენტის თანაბარ ან უფრო მაღალ რანგს R_{ai}. მაგალითად, i ქსელის აბონენტისთვის $R_{ai} = 1$, $k_{nx\Sigma}$ კვანძების უსაფრთხოების კომპლექსური მაჩვენებლები აკმაყოფილებს უსაფრთხო კომუნიკაციის შერჩეულ მარშრუტს N_{ij}^s და არის 0-დან 0.2-მდე მნიშვნელობების დიაპაზონში (ცხრილი 8).

ცხრილი 8

Rank of Network subscribers $R_a \geq 2$	$k_{x\Sigma}$
1	0…0,2
2	0,2…0,4
3	0,4...0,6
4	0,6...0,8
5	0,8...1

ამგვარად, უსაფრთხო საკომუნიკაციო მარშრუტი i და j აბონენტებს შორის ირჩევა ქსელის i აბონენტის მოთხოვნით და ქსელის აბონენტების წინასწარ განსაზღვრული რანჟირების შესაბამისად. გარდა ამისა, ისევე როგორც მეთოდის პირველ ვარიანტში, დაცულია უსაფრთხო მარშრუტი N_{ij}^s სარეზერვო მარშრუტის ჩათვლით შეტყობინების გენერირება N_{ij}^s და j აბონენტის მისამართი IP_{aj} და გენერირებული შეტყობინება ეგზავნება ქსელის i აბონენტს.

ქსელის i და j აბონენტებს შორის უსაფრთხო მარშრუტის არარსებობის შემთხვევაში, ე.ი. იმ შემთხვევაში, როდესაც აბონენტებს შორის შესაძლო საკომუნიკაციო მარშრუტებს შორის არ არის მარშრუტი, რომელშიც მასში შემავალი კვანძების უსაფრთხოების ინდიკატორები არ შეესაბამება აბონენტის რანგს, იქმნება პასუხი და ეგზავნება ქსელის i აბონენტს, ქსელის j აბონენტთან უსაფრთხო მარშრუტის არარსებობის შესახებ.

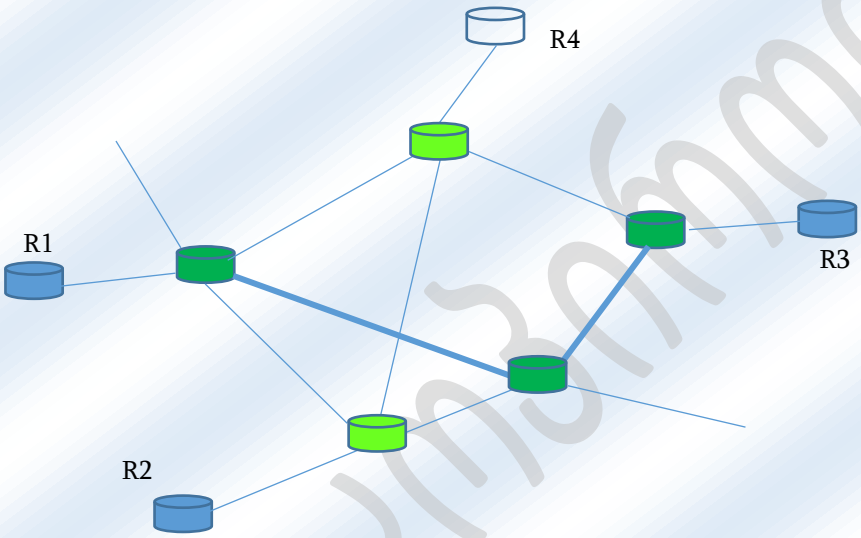
მეთოდის პირველი ვარიანტისგან განსხვავებით, უსაფრთხო კომუნიკაციის მარშრუტი N_{ij}^s ქსელის i- და j-აბონენტებს შორის, შეირჩევა ისეთ შემთხვევაში, თუ მასში შემავალი კვანძების უსაფრთხოების კომპლექსური ინდიკატორები $k_{nx\Sigma}$ შეესაბამება ქსელში გადასაცემი ინფორმაციის $R_{inf\,i}$ თანაბარ ან უფრო

მაღალ რანგს. მაგალითად ქსელის *i* აბონენტისთვის გადასაცემი ინფორმაცია $R_{inf\,i} = 1$, უსაფრთხო კომუნიკაციის შერჩეულ მარშრუტში N_{ij}^{s} და უსაფრთხოების კომპლექსური მაჩვენებელი $k_{nx\Sigma}$ არის 0-დან 0.2-მდე მნიშვნელობების დიაპაზონში.

გენერირებულ საკომუნიკაციო მარშრუტებში შემავალი კვანძების უსაფრთხოების კომპლექსური ინდიკატორები $k_{nx\Sigma}$ იძლევა ქსელის აბონენტებს შორის შერჩეული უსაფრთხო საკომუნიკაციო მარშრუტების ობიექტური შეფასების საფუძველს და საშუალებას გვაძლევს გათვალისწინებული იქნეს კომუნიკაციაში უსაფრთხო მარშრუტის არჩევისთვის აუცილებელი და საკმარისი პირობები.

ამრიგად, მეთოდის მეორე ალგორითმშიც მიღწეულია ჩამოყალიბებული ტექნიკური შედეგი - ქსელის აბონენტებს შორის კომუნიკაციის უსაფრთხოების გაზრდა.

ნახაზი (ნახ.3) გვიჩვენებს საკომუნიკაციო ქსელში უსაფრთხოების სერვერზე უსაფრთხო მარშრუტის არჩევის მაგალითს საკომუნიკაციო ქსელში *i* და *j* აბონენტებს შორის.



ნახ 3. საკომუნიკაციო ქსელში უსაფრთხოების სერვერზე უსაფრთხო მარშრუტის არჩევის მაგალითი

გამოთვლილია ქსელის საკომუნიკაციო კვანძების უსაფრთხოების კომპლექსური ინდიკატორების $k_{nx\Sigma}$ მაჩვენებლები და მათი უსაფრთხოების b_{xy} პარამეტრები, მნიშვნელობები წარმოდგენილია ცხრილში 3.

ცხრილი 8 საკომუნიკაციო კვანძების უსაფრთხოების კომპლექსური ინდიკატორების $k_{nx\Sigma}$ მაჩვენებლები

ქსელის კვანძი	ქსელის კვანძების უსაფრთხოების პარამეტრები b_{xy}			ქსელის კვანძის უსაფრთხოების მაჩვენებელი
	y=1	*y=2*	*y=3*	$k_{x\Sigma}$
ქკ = 1	0,3	0,13	0,4	*0,83*
ქკ = 2	0,3	0,16	0,4	0,86
ქკ = 3	0,2	0,1	0,34	0,64
ქკ = 4	0,5	0,2	0,25	0,95
ქკ = 5	0,5	0,08	0,01	0,14

წარმოდგენილი მაგალითიდან ჩანს, რომ უსაფრთხო მარშრუტის მეორე ვერსიის გამოყენებისას, მიიღწევა ქსელში უსაფრთხოების დაბალი დონის მქონე სატრანზიტო კვანძების გამორიცხვა, რომლებიც შესაძლებელია მაღალი ალბათობით ყოფილიყო ქსელში აბონენტების მიერ გადაცემულ შეტყობინებებზე არასანქცირებული წვდომის შესაძლებლობა. ამ მაგალითში როგორც გაანგარიშების ცხრილიდან ჩანს, N_{55}-ს აქვს ქსელის უსაფრთხოების ინდექსის $k_{5\Sigma}$ და აბონენტის უსაფრთხოების პარამეტრების b_{5y} მაღალი მნიშვნელობები, რომლებიც შესაბამისად გამუქებულია (ნახ. 3.).

ამრიგად, შერჩეული უსაფრთხო საკომუნიკაციო გზა, რომელიც გამოყოფილია მუქი ხაზებით, *i* და *j*

აბონენტებს შორის გადის ქსელის ტრანზიტულ კვანძებზე, რომლებსაც აქვთ უსაფრთხოების ყველაზე მაღალი მაჩვენებელი რაც ამცირებს დამრღვევების მიერ ალბათობას, ჩაერიოს ქსელის აბონენტების შორის ინფორმაციის გაცვლაში.

დასკვნა

მაგალითებიდან ჩანს, რომ უსაფრთხო მარშრუტის არჩევისას წარმოდგენილი მეთოდის გამოყენებისას მიიღწევა უსაფრთხოების დაბალი დონის მქონე სატრანზიტო ქსელის კვანძების გამორიცხვა, რადგან ისინი მიუთითებს გადაცემული შეტყობინებების არასანქცირებული ჩარევის მაღალ ალბათობაზე.

სემინარზე მიღებული შედეგების საფუძველზე შეიძლება დავასკვნათ, რომ წარმოდგენილ მეთოდში, უსაფრთხო მარშრუტის არჩევის ორივე ვარიანტის გამოყენებისას, კომუნიკაციის უსაფრთხოება იზრდება საკომუნიკაციო ქსელში აბონენტებს შორის ინფორმაციის გაცვლის მარშრუტების კონტროლის საფუძველზე. ალგორითმი გამოირჩევა უსაფრთხოების პრობლემის გადაჭრის თვისობრივად ახალი მიდგომით და მიმართულია კომპიუტერულ ქსელებში შეტყობინებების პაკეტების მარშრუტიზაციის არსებულ მეთოდებში არსებული მინუსების აღმოფხვრაზე.

გამოყენებული ლიტერატურა

1. J. Forshaw, Attacking Network Protocols, 2017, Publisher(s): No Starch Press
2. D. Medhi K. Ramasamy, Network Routing Algorithms, Protocols and Architectures, 2017
3. B. Halabi, Internet Routing Architectures, 2nd Edition, Cisco Press, 2001
4. A. Yu. Romanov, Development of routing algorithms in networks-on-chip based on ring circulant topologies, 2019
5. O. Bonaventure, Computer Networking: Principles, Protocols and Practice. Rel.0.25, 2011
6. E. Stack Computer Networking The Complete Guide, 2019
7. Junwei Jin. Sanghyun Ahn, A Multipath Routing Protocol Based on Bloom Filter for Multihop Wireless Networks / Mobile Information Systems Volume 2016, p. 1-10.
8. D. Vyas, R. Patel, A. Ganatra, Survey of Distributed Multipath Routing Protocols for Traffic, Management International Journal of Computer Applications (0975-8887), Volume 63-No.17, February 2013, p. 42-48.
9. Karthiga. S, Balamurugan, Traffic Engineering System Based on Adaptive Multipath
10. Routing / International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 2, February 2013, p. 659664.