ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

დათუაშვილი ნაია

კვლევები ინტერნეტის მომავალ არქიტექტურაში

The Research On Future Internet Architectures

ინფორმაციული ტექნოლოგიები

ნაშრომი შესრულებულია **საინფორმაციო სისტემების მაგისტრის** აკადემიური ხარისხის მოსაპოვებლად

თბილისი 2013

სამაგისტრო ნაშრომის ხელმძღვანელი

ლელა მირცხულავა

დოქტორი, ასოცირებული პროფესორი

სარჩევი

ანოტაცია

დღესდღეობით არსებული ინტერნეტის წინაშე, რომელიც შეიქმნა 40 წლის წინ, დგას დგას უპრეცედენტო გამოწვევები მრავალი ასპექტით, განსაკუთრებით კომერციული კონტექსტში. რთულია წარმოქმნილი მოთხოვნების უზრუნველყოფა უსაფრთხოებაზე, მობილობაზე, კონთენთის გავრცელებაზე და ა.შ. სპეციალური პაჩების თანდათანდობითი ზრდით. მოსალოდნელია, წმინდა ახალი არქიტექტურა ახალი არქიტექტურული პრინციპების საფუძველზე, რომელიც იქნება ამ გამოწვევების გადაწყვეტილება. ამ თვალსაზრისით, მოცემულ სტატიაში განიხილება ინტერნეტის მომავალი არქიტექტურის თემა. გადმოცემულია მომავალი ინტერნეტ-არქიტექტურის კვლევების ზოგადი სურათი.

Annotation

The current Internet, which was designed over 40 years ago, is facing unprecedented challenges in many aspects, especially in the commercial context. The emerging demands for security, mobility, content distribution, etc. are hard to be met by incremental changes through ad-hoc patches. New clean-slate architecture designs based on new design principles are expected to address these challenges. In this survey article, we investigate the key research topics in the area of future Internet architecture. We aim to draw an overall picture of the current research progress on the future Internet architecture.

შესავალი

ძნელია ითქვას ზუსტად როდის დაიბადა ინტერნეტი ან ვინ იყო მისი შემოქმედი, ინტერეტი იყო პირველი თუ ARPA, ან ვინ ვინ წარმოშა, ფაქტი ერთია რომ ARPA–ს გარეშე არ შეიძლებოდა დაბადებულიყო ასეთი გლობალური ქსელი, მაგრამ ARPA–აც არ იქნებოდა ისეთი 1963 წელს სააგენტოს ინფორმაციის დამუშავების ბიუროს დირექტორის თანამდებობა რომ არ დაეჭირა ჯონ ლიკლაიდერს, რომლის სახელსაც უკავშირდება ქსელის შექმნა. გლობალური ქსელის შექმნაში მნიშვნელოვანი გავლენა იქონია RAND კორპორაციის მიერ ჩატარებულმა სამუშაოებმა. ასევე ლიკლაიდერს ეკუთვნის ნაშრომი „გალაქტიკის ქსელის“შესახებ, რომელშიც იწინასწარმეტყველა ადამიანებს შორის კომპიუტერით გლობალური კავშირის შესახებ.

ამგვარად დაიწყო ინტერეტის შექმნა, რომელსაც თამამად შეგვიძლია ვუწოდოთ კაცობრიობის ახალი ერა, და შემდგომში მისი სწრაფი განვითარება, რომელიც შემდეგნაირად განვითარდა:

- 1957 წლის 4 ოქტომბერს საბჭოთა კავშირმა გაუშვა დედამიწის პირველი ხელოვნური თანამგზავრი.
- 1961 წელს ლეონარდ კლეინროკმა დაამუშავა და პირველად 1964 წელს გამოაქვეყნა თეორია მონაცემების გადაცემისათვის პაკეტების კომუტაციის შესახებ.
- 1965 წელს კონფერენციის შემოწმებისათვის ლორენს რობერსმა და ტომას მერილმადაბალსიხშირიანი სატელეფონო ხაზით შეართეს კომპიუტერები TX-2 მასაჩუსეტსის შტატისა და Q-32 კალიფორნიაში. ამგვარად შექმნილ იქნა პატარა თუმცა პირველი ლოკალური კომპიუტერული ქსელი.
- 1972 წლის ოქტომბერში კომპიუტერული კომუნიკაციების კონფერენციაზე წარმატებით ორგანიზებულ იქნა ARPANET-ის ქსელის დემონსტრირება. ამ წელსვე გამოჩნდა ARPANET-ის პირველი ელექტრონული ფოსტა. რეი ტომლინსონმა BBN-დან ARPANET-ის მარტივი კოორდინაციის საშუალებიდან დაწერა ელექტრონული შეტყობინებების გადაგზავნის და წაკითხვის საბაზო პროგრამები, რომელსაც დაუმატა შეტყობინების სიის გაცემის შესაძლებლობა, ამორჩევითი წაკითხვა, ფაილში შენახვა, პასუხის გაგზავნა და მომზადება. ამის შემდეგ ელექტრონული ფოსტა გახდა მსხვილი ქსელური დამატება.
- 1974 წელს ინტერნეტის ქსელის სამუშაო ჯგუფმა, რომელსაც ხელმძღვანელობდა სერფი, წარმოადგინა გაერთიანებული ქსელების მონაცემების დაგაცემის უნივერსალური პროტოკოლი TCP/IP, რომელიც ძალზედ წარმატებული აღმოჩნდა.
- 1978 წელს აშშ-ს პრეზიდენტმა დ. ეიზენჰაუერმა გამოსცა განკარგულრბა ორი სამთვარობო ორგანოს ჩამოყალიბების შესახებ: NASA და ARPA.
- 1980 წელს კონსორციუმმა გამოუშვა დოკუმენტაცია Ethernet ქსელზე, შედეგად ლოკალური ქსელი წარმატებითიქნა გამოყენებული შემდეგი საჭიროებისთვის:

1. ფაილების ერთობლივი გამოყენება;
2. მომხმარებლის ერთმანეთთან კავშირი;
3. შორეული მართვა (ქსელური მართვა, პროგრამების შორეული, დისტანციური მართვა);

- 1983 წელს ARPANET-მა NCP-თან TCP/IP პროტოკოლზე საშუალება მისცა გაეყოთ ეს ქსელი ცალკე MILNET ქსელად, საკუთრივ სამხედრო მიზნებისთვის და ARPANET-ად, საკვლევი მიზნებისთვის. ამავე წელს პოლ მიკაპეტრისმა გამოიგონა დომენების სახელი სისტემა (DNS-Domain Name System), რამაც საშუალება მისცა შექმნილიყო მასშტაბირებული განაწილებული მექანიზმი კომპიუტერების იერარქიული სახელების გამოსახვისთვის ინტერნეტ-მისამართებში.
- 1985 წელს TCP/IP პროტოკოლის საფუძველზე დენ ლინჩმა ორგანიზება გაუკეთა კონფერენციას, რომელმაც მომდევნო ორ წლიანი თათბირისა და პრაქტიკული მეცადინეობის შედეგად TCP/IP პროტოკოლი მიწოდებული და დამუშავებული იქნა საუკეთესო პროვაიდერისთვის.
- 1986 წელს ARPANET-ის საფუძველზე შეიქმნა NSFNET (The National Science Foundation NETwork- ნაციონალური სამეცნიერო ფონდის ქსელი).
- 1987 წელს NSF-მა კომპანია Merit Network Ink. გადასცა კონტრაქტი, რომელთაც Merit IBM-ის და MCI-ის მონაწილეობით უნდა უზრუნველყო საბაზო NSFNET ქსელის მართვა, განეხორციელებინა გადასვლა უფრო მაღალსიჩქარიანი T-1 არხებზე და გაეგრძელებინა მისი განვითარება. განვითარებად საბაზო ქსელს ჰქონდა 10 კვანძზე მეტი.
- 1988 წლის ივლისში ქსელი შედგებოდა 13 კვანძისაგან, რომლებიც ერთმანეთთან შეერთებული იყვნენ 1536 კბტ/წმ სიჩქარიანი T-1 არხებით. მონაცემების კავშირი სწრაფად ავსებდა კავშირის ამარხებს. გადაცემული ინფორმაციის მოცულობა თვეში 20% სიჩქარით იზრდებოდა.
- 1990 წელს Merit-მა, IBM-მა და MCI-მა შექმნეს შვილობილი კომპანია ANS(Advnced Network & Servis), რომელსაც უნდა ემართა NSFNET საბაზო ქსელი და იმავდროულად აეგო ახალი საბაზო ქსელი T-3 არხებზე, სიჩქარით 45 მბტ/წმ, რომელიც შეცვლის მას.
  ამავე წელს მოხდა ინტერნეტის ნამდვილი „აყვავება“ როდესაც შეიქმნა WWW(World Wide Web საერთო რესურსებთან შეღწევის ტექნოლოგია), რომელიც ბირთვული ევროპული ორგნიზაციის მიერ იქნა შექმნილი, მან ძველ მსოფლიოს საშუალება მისცა ინტერნეტში შეღწევის.
- 1994 წელს შეიქმნა კონსორციუმი W3C, რომელმაც გააერთიანა სხვადასხვა უნივერსიტეტებისა და კომპანიების მეცნიერები, ამ კომიტეტმა დაიწყო ინტერნეტის სამყაროში არსებული ყველა სტანდარტზე მუშაობა.
- 1995 წელს ინტერნეტის ზრდის ტემპმა აჩვენა, რომ მიერთების და ფინანსირების საკითხების რეგულირება არ შეიძლებოდა ყოფილიყო ერთი, NSF-ს ხელში. ამიტომ მოხდა რეგიონალური ქსელებისათვის და ქსელების ნაციონალური მაგისტრალებისათვის მრავალრიცხოვანი მიერთების გადასახადის გადაცემა.

დღეს ინტერნეტზე მსჯელობისას წინა პლანზე გამოდის მისი ფუნქციონალურობის ორი მხარე: ტექნიკური და ჰუმანიტარული. ტექნიკური თვალსაზრისით ინტერნეტი არის ერთმანეთთან დაკავშირებული საკუთარი უნიკალური მისამართებისმქონე კომპიუტერების ფართო ქსელი. ეს კომპიუტერები შეერთებულია ერთმანეთთან მარშრუტიზატორებით. ჰუმანიტარული თვალსაზრისით ინტერნეტი არის კულტურის ახალი განზომილება, ცოდნის, ინფორმაციის შენახვისა და გავრცელების ხერხი, ამ კუთხით მას ასევე გააჩნია კომერციული და საინფორმაციო დატვირთვა. განვითარებულ ქვეყნებში ინტერნეტი ძირითადათ ორიენტირებულია კომერციაზე, მაშინ როდესაც განვითარებად ქვეყნებში ინტერნეტი ასრულებს საინფორმაციო ფუნცქიას.

ინტერნეტის ფენომენი თანამედროვე სამყაროში განსაკუთრებულია; ინტერნეტი, ეს არის: ბიბლიოთეკები და სამხატრო გალერიები, სტატიები და წიგნები, პოლიტიკა და ნებისმიერი სიახლე: მეცნიერების, ტექნიკის, ისტორიის, ეკონომიკის და ადამიანის მიღწევების ყველა სფეროში.

საქართველოში ინტერნეტის გავრცელება დაიწყო 90-იანი წლებიდან, როდესაც პრაქტიკულად ყველა პროვაიდერს კავშირი ჰქონდა რუსეთთან. ინტერნეტის პიონერი საქართველოში იყო კონპანია ხეთა და გუდვილიკომი, აგრეთვე ზოგიერთი სხვა პროვაიდერი, რომლის სააბონენტო თვეში შეადგენდა 300$, შემდგომ გამოჩნდენ სხვა პროვაიდერები და ფასი დაეცა 20$-მდე. პროვაიდერები იყენებდნენ თანამგზავრულ და საკაბელო შეღწევას. გაცემის სიჩქარე პირდაპირ არხში შეადგენდა 64 კბტ/წმ. შემდგომ საქართველოში გამოჩნდა ოპტიკურ-ბოჭკოვანი საკაბელო მაგისტრალების ქსელი. ინტერნეტის მომსახურების ფასები შემცირდა სიჩქარე გაიზარდა, ასევე ინტერეტი გავრცელდა საქართველოს სხვადასხვა ქალაქებში.

თავი I

კვლევები ინტერნეტის მომავალ არქიტექტურაში

არსებული ინტერნეტი, რომელიც შექმნილია 40 წლის წინ, დგას მრავალი გამოწვევების წინაშე. განსაკუთრებით კი კომერციულ კონტექსტში. მისი საწყისი მოთხოვნებია: დაცვა, მობილობა და ა.შ.ახალი clean-slate არქიტექტურის ძირითადი გეგმა, ახალ ესკიზებში, არის მისამართის მოსალოდნელი ცვლილებები. მრავალი მიმდინარე კვლევები არის წარმოდგენილი და განხილული რომლებიც ტარდება ამერიკის შეერთებული შტატებში, ევროპის კავშირში, ჩინეთში იაპონიაში და კიდევ მრავალ სხვა ქვეყნებში.

ინტერნეტი იქცა განუყრელ და სავალდებულო ნაწილად, როგორც ადამიანის ყოველდღიურ ცხოვრებისა, ასევე ეკონომიკური ოპერაციების შესასრულებლად და მთლიანად საზოგადოების ცხოვრების. მიუხედავად ამისა, მრავალი ტექნიკური თუ არატექნიკური გამოწვევები იქნა წამოჭრილი ამ პროცესების განმავლობაში, რომელიც ცნობილია როგორც ახალი ინტერნეტ არქიტექტურის შესაძლებლობები. უწყვეტი წარმატების ხელშემშლელ მიზეზად იქცა უსაფრთხოების ნაკლებობა თავდაპირველ არქიტექტურაში. აგრეთვე, IP-ის სუსტ წერტილად შეიძლება ჩავთვალოთ ისიც რომ მისი შიგთავსი არის ძნელად მოდიფიცირებადი, რის გამოც რთულია მასში სიახლის შეტანა. უფრო მეტიც, უკიდურესად რთული ხდება მისი დაცვა, ისეთ პირობებში როდესაც არსებობს უსაფრთოების მზარდი მოთხოვნა,მობილობა და სხვა მრავალი მოთხოვნები. შედეგად, შემოთავაზებული იქნა clean-slate არქიტექტურის ნიმუში, რომელიც კვლევების ყველა ესკიზში საერთოა, იგი შეეხება მომავალ ინტერნეტს.

უსაფთხოება უნდა იყოს განუყოფელი ნაწილი არქიტექტურის. აგრეთვე მნიშვნელოვანი მოთხოვნაა ტრანსფორმაცია ინტერნეტიდან მარტივ "ჰოსტი-ჰოსტთან" პაკეტებამდე მიმღები პარადიგმებიდან სხვა მრავალ პარადიგმებში, რომელიც ჩაშენებულნი არიან ბაზებში და იუზერებში მექანიზმის ნაცვლად. ყველა ეს ზემოთ ხსენებული ცვლილება არის წინამძღვარი იმ კვლევებისა რომელიც ხორციელდება ინტერნეტის მომავალ არქიტექტურაში.

ინტერნეტის მომავალი არქიტექტურა მიზნად არ ისახავს მხოლოდ რაიმე კონკრეტულ საგნის გაუმჯობესებას. კონკრეტული თემა Cleanslate-ის გადაჭრა პასუხისმგებელია არქიტექტურის სხვადასხვანაწილებზე, რომელიც იქნება მუდმივი და შეუცვლელი. ასე რომ,clean-slate განსხვავებული ასპექტების აწყობა არ იქნება საჭირო ინტერნეტის მომავალ არქიტექტურაში. ნაცვლად ამისა მას ექნება შესაძლებლობა მთელი არქიტექტურის რეკონსტრუქციის. მრავალი წინა clean-slate პროექტი ფოკუსირებული იყო ინდივიდუალურ ნაწილებზე. საერთო და ყოველმხრივი მიდგომით, საკითხების შესწავლით და კვლევების შედეგებით, ასევე ინდივიდუალური ძალიხმევით, შესაძლებელი გახდა მთლიანი ინტერნეტ არქიტექტურის მშენებლობა.

ინტერნეტ მომავალი არქიტექტურის სხვა მნიშვნელოვანი ასპექტია ახალი არქიტექტურის ექსპერიმენტიზაცია. არსებული ინტერნეტის მფლობელებს და დაინტერესებულ მხარეებს არ სურთ გამოამზეურონ და ყველასათვის თვლასაჩინო გახადონ მათი ინტერნეტის ექსპერიმენტები, რომლებიც შეიცავენ რისკებს. სხვა მიზეზი ინტერნეტ მომავალი არიტექტურის კვლევების არის ვირტუალური და მსხვილი მასშტაბების გახსნა მიმდინარე მომსახურების ხელშეუშლელად. ახალ არქიტექტორებს საშუალება ექნებათ გატესტონ, ლიცრნზირება გაუკეთონ და გააუმჯობესონ არსებული ინტერნეტიექსპერიმენტიზაციის პერიოდში, სანამ მათ შესაძლებლობა მიეცემათ გაშვებულ იქნან რეაულ სამყაროში.

არსებობს სამი თანმიმდევრული ნაბიჯი თუ როგორ უნდა იმუშავოს ინტერნეტის მომავალმა არქიტექტურამ, ესენია:

ნაბიჯი 1: ინოვაციები ინტერნეიტს სხვადასხვა ასპექტში.

ნაბიჯი 2: საერთო პროექტების ჩადება მრავალგზის ინოვაციებში.

ნაბიჯი 3: რეალურ მასშტაბიანიექსპერიმენტიზაცია.

მომავალი ინტერნეტის მთელი ძალისხმევა შესაძლებელია მიმართული იყოს მათ ტექნიკურ და გეოგრაფიულ მრვალაფეროვნების კლასიფიკაციაზე. სანამ ზოგიერთი პროექტის მიზანს წარმოადგენს კონკრეტული თემები, მთლიანი არქიტექტურის მიზანია შექმნას ურთერთთანამშრომლობა დამიაღწიოსერთობლივ ძალისხმევას ინდივიდუალურ პროექტებს შორის. კვლევების პროგრამის განსაკუთრებულ მიზანს წარმოადგენს მომავალი ინტერნეტის გამართვამთელ დედამიწაზე, მათ შორის ამერიკის შეერთებულ შტატებში, ევროპაში იაპონიასა და ჩინეთში.

ჩვენ განვიხილავთ კვლევების გასაღებებს და მომავალი ინტერნეტ არქიტექტურის მიზანს. კვლევის პროექტები დაწვრილებით და სათანადოდ არის განხილული ამერიკის შეერთებულ შტატებში, ევროპაში და აზიის ქვეყნებში.

კონტენტი და მონაცემებზე ორიენტირებული პარადიგმები: დღევანდელი ინტერნეტი აშენებულია IP–ის “narrow waist”-ის გარშემო. არსებული ინტერნეტი შეიცვალა host-to-host კავშირიდან შიგთავსის დისტრიბუციამდე, რომელიც ჯერ კიდევ გამოიყენება. სასურველია არქიტექტურის „narrow-Waist“-ის ცვლილებაIP–დან მონაცემებით ან დისტრიბუციის შიგთავსით. რამოდენიმე კვლევითი პროექტების ძირეულ იდეას სწორედ ეს წარმოადგენს. არსებობსასეთი კატეგორიის მაგალითების წარდგენის მცდელობა, მონაცემებში და დაცვის შიგთავსი, სახელებისმინიჭების მასშტაბები, და ა.შ.

ქსელის მობილობა და ყველგან წვდომადობა: ინტერნეტი განიცდის მნიშვნელოვან ცვლილებას PC-ს თავდაპირველი კომპიუტერიდან მოქნილ კომპიუტერამდე. მობილობა გახდა წამყვანი გასაღები მომავალი ინტერნეტისთვის. კონვერგენციული მოთხოვნების მზარდობა ჰეტეროგენულ(სხვადასხვაგვაროვანი) ინტერნეტისა (როგორიც არის ქსელერი IP) და უსადენო ad hoc ან მგრძნობიარე ქსელისა, განსხვავდებიან ტექნიკური სტანდარტებით და ბიზნეს მოდელით. მრავალი საზოგადო კვლევითი პროექტები აკადემიაში და საწარმოებაში არის განხორციელებული როგორც კვლევითი საგნები უზარმაზარი ინტერესებით.

FIA AND FIND

ეროვნული მეცნიერებათა ფონდის ინტერნეტ მომავალი არქიტექტურის პროგრამა არის აგებული წინა პროგრამაზე. ინტენეტის შემდგომი დიზაინი კონლოსიდირებულია მომავალი ინტერნეტის ყველა სახის ასპექტზე, რომელიც დაახლოებით 50 კვლევითი პროექტი ეძღნება. FIA არის მომავალი ფაზა არქიტექტურის, ჯგუფის იდეების და წინადადებების ერთობლიობისა. არსებობს რამოდენიმე საზოგადო ჯგუფი რომელიც გაერთიანებულია ამ პროექტის ქვეშ, ესენია:

Named Data Networking (NDN) - ამ პროექტის ხელმძღვანელნი არიან კალიფორნიის უნივერსიტეტი, ლოს ანჯელესის 10 უნივერსიტეტისა და კვლევითი ინსტიტუტების მონაწილეობით ამერიკაში. ძირითადი არგუმენტი ამ პროექტის მდგომარეობს იმაში, რომ არსებული ინეტენეტი შეიცვალა end-to-end პაკეტიდან მიმღებ content-centric მოდელით. NDN იყენებს განსხვავებულ მოდელებს რათა საშუალება მისცეს ქსელს რომ ფოკუსირება მოახდინოს არა „რა“-ზე (შინაარსზე) არამედ „სად“-ზე (მისამართზე). მონაცემები გახდა პირველი ორგანიზაცია NDN-ში. ნაცვლად იმისა, რომ ცდილობდეს გადამცემი არხის დაცვას, იგი ცდილობს დაიცვას მონაცემების შიგთავსი გაუმჯობესებული მეთოდის გავლით. NDN აქვს რამოდენიმე კვლევითი გასაღები,ესენია:

- მონაცემების ძებნა;
- მონაცემების დაცვა და ნდობის ხარისხი;
- NDN მასშტაბურობა;

საბოლოო ჯამში NDN ცდილობს მისამართები თავიდან ბოლომდე იყოს გადაწყვეტილი არხების მასშტაბურობით. მარშუტიზაციაში, იყოს დაცული და მოდელი იყოს სანდო, ჰქონდეს მონაცემების გავრცელებსა და მიღების სწრაფი უნარი. აგრეთვე მის უპირველეს მიზანს წარომადგენს შიგთავსის დაცულობა, პირადულობა და ყველა იმ თეორიის მხარდაჭარა რაც უკვე ავღნიშნეთ.

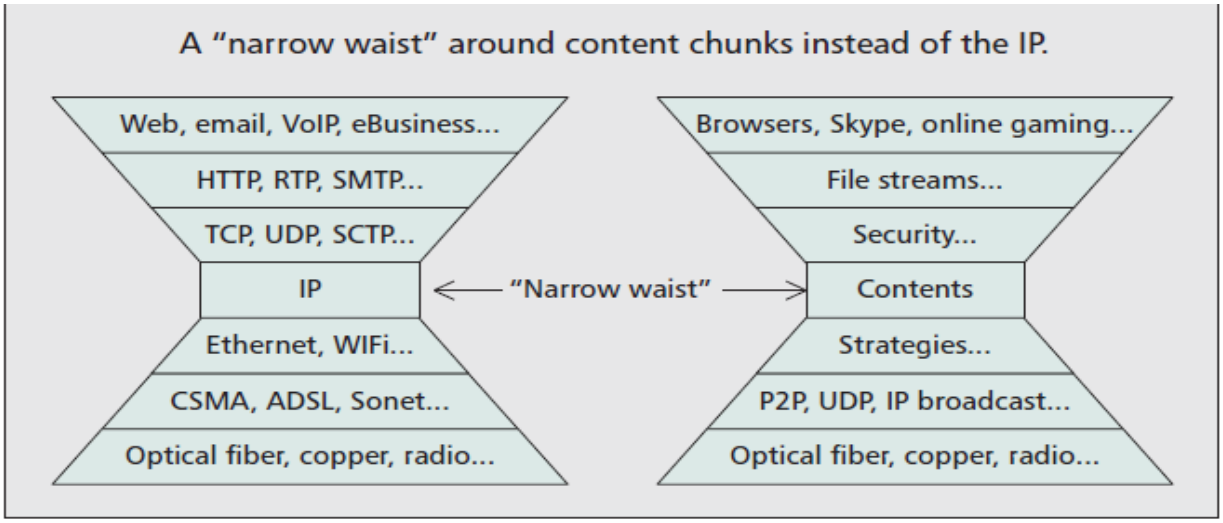

Figure 1. *The new "narrow waist" of NDN (right) compared to the current Internet (left).*

პირველი მობილობა (MobilityFirst)- ამ პროექტის ხელმძღვანელნი არიან რუთგერსის უნივერსიტეტი შვიდ სხვა უნივერსიტეტთან ერთად. პირველი ძირითადი მოტივაცია MobilityFirst არის არსებული ინტერნეტის დიზაინი, რომელიც უკავშირდება უცვლელ ბოლოწერტილებს. MobilityFirst-ისკიდევ ერთ-ერთი მიზანია მისამართების კონვერგენცია, რომელიც მოტივირებულია მობილურის უზარმაზარი პოპულაციით, იგი დაახლოებით 4 -5 ბილიონს აღწევს. სამომავლოდ, MobilityFirst აქვს ამბიცია დააკავშიროს მილიონობით მანქანა vehicle to vehicle (v2v) და vehicle to infrastructure (V2I) მოდელები, რომლებიც ჩართულნი იქნებიან ადგილობრივი სერვისით, გეოგრაფიული მარშუტით და საიდემო მულტიმაუწყებლობით.

MobilityFirst მისამართების ცვლილება შეიცავს უფრო ძლიერ დაცვას და სანდო მოთხოვნებს გახსნილი, უსადენო გასასვლელით და ა.შ. MobilityFirst აშენებულია "narrow waist" რამოდენიმე პროტოკოლის გარშემო, ესენია:

- საერთაშორისო სახელის რეზოლუცია და როუტინგ სერვისი;
- Storage-aware (DTN-like) როუტინგის პროტოკოლი;
- Hop-to-hop სეგმენტის გადამტანი;
- სერვისის და მენეჯმენტის აპლიკაციების პროგრამული ინტერფეისი (APIs);

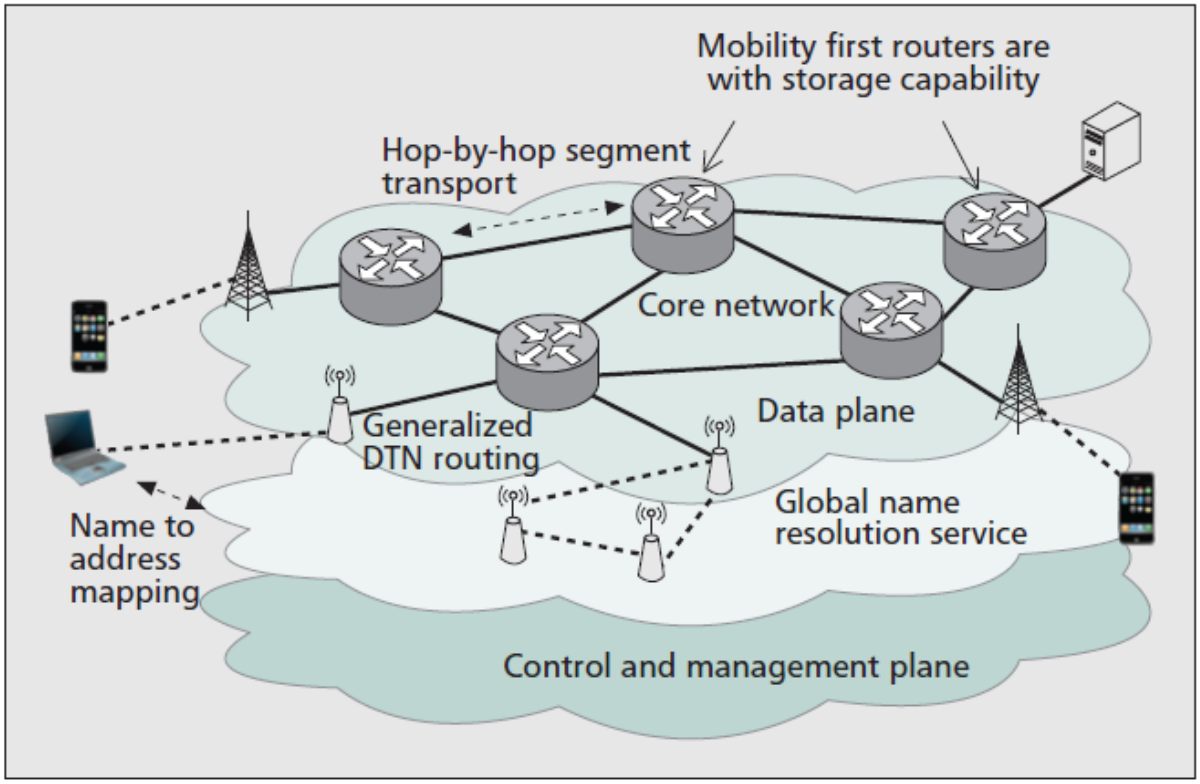

Figure 2. *MobilityFirst architecture.*

eXpressive Internet Architecture (XIA)- eXpressive Internet Architecture (XIA) არის NSF FIA-ს ერთ-ერთი პროექტი, იგი ინიცირებულია Carnegie Mellon უნივერსიტეტის კოლაბორაციის მიერ ორ სხვა უნივერსიტეტებთან ერთად. კვლევითი პროექტი ინტერნეტ მომავალ არქიტექტურაზე უნდა იყოს განხორციელებადი, ასევე მნიშვნელოვანიადაცვა და აგრეთვე მიზანშეზონილია სიფხრთილე მათ არქიტექტურაში, რათა თავიდან იქნას აცილებული თავდაპირველი ინტერნეტ დიზაინის გაბზარვა.

არსებობს რამოდენიმე გასაღების იდეა XIA-ს არქიტექტურაში, ესენია:

- განისაზღვროს ჩაშენებული ბლოკები ან კომუნიკაციების ორგანიზაციები, როგორც ქსელის პრინციპები, რომლებიც შეიცავენ ჰოსტებს, მომსახურეობას, შინაარსს და მომავალ დამატებით ორგანიზაციებს.
- შესაძლებლობა ჰქონდეს თანდაყოლილი დაცვის გამოყენებისა
- თვით-სერთიფიცირებული იდენთიფიკატორების ყველა პრონციპში, რომელიც შეიცავს ინტეგრირებულ დაანგარიშვალდებულ თვისებებს.
- შევსებადი “narrow waist” (შეუზღუდავი ჰოსტები, ძირითადი კომუნიკაციები, როგორც მიმდინარე ინტერნეტში) ყველა გასაღებ ფუნქციაში, მისაწვდომობის შემცველი პრინციპები.
- ურთიერთობა დაუინტერესებელ მხარეებს შორის.

XIA-ს კომპონენტები და მათი ურთიერთქმედება ნაჩვენებია ნახაზი 4-ზე.

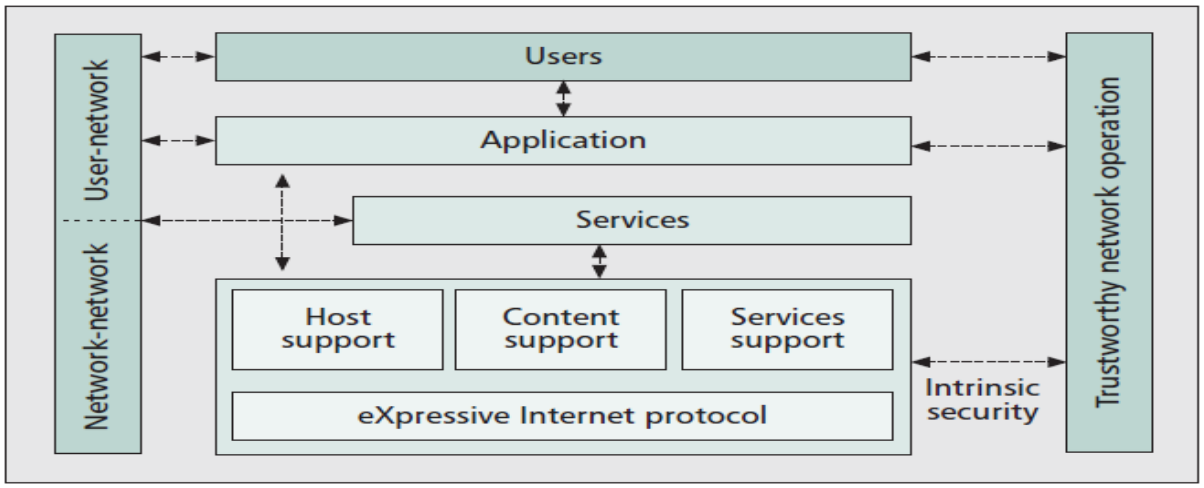

Figure 4. *XIA components and interactions.*

XIA ბირთვი არის გამოხატულება XIA -სა და სხვადასხვა ტიპის პრინციპებს შორის. XIA-ს სამი ძირითადი ტიპიურინიმუში არის შიგთავსი, ჰოსტი (აღწერილი როგორც „ვინ“) და მომსახურეობა (აღწერილი როგორც „რას აკეთებს“). თითოეული ტიპის პრინციპს აქვს narrow waist,რომელიც განსაზღვრავს მინიმალურ ფუნქციონალურ მოთხოვნებს ქსელის ურთიერთქმედების შესაძლებლობაში. XIA აგრეთვე სჭირდება სხვადასხვა სადნო მექანიზმები და პროვაიდერები ქსელის მისაწვდომელობისთვის, მაშინაც კი როდესაც ადგილი აქვს თავდასხმას. საბოლოოდ, XIA განსაზღვრავს ზუსტ ინტერფეისს ქსელის მსახიობსა და გახსვავებულ როლებსა და მიზეზებს შორის.

გლობალური გარემო ინტერნეტ ინოვაციებისთვის (GENI)

GENI არის საერთო პროგრამა მხარდაჭერილიNSF-ის მიერ. მისი განვითარება დაიწყო 2005 წელს, რომელიც დიდად იყო დაინტერესებული და ჩართული როგორც აკადემიაში ასევე მრეწველობაში. გარდა იმისა მან მხარი დაუჭირა არსებული პროექტს, როგორც ქსელის საფუძვლიანი ინფრასტრუქტურას. ასევე მისი ყურადება მიიქცია სხვა ინფრასტრუქტურულმა პლათფორმამ, როგორც ფედერაციებში მონაწილე-სქემის მართვის

ფრეიმორკმა. ამგვარად GENI არის განსხვავებული როგორც მომსახურებით ასევე მისი გამოყენებით.

GENI-ს იდეის გასაღები არის ჩაშენებადი უმცირესი საერთო ვირტუალური ნაწილი, რომელიც შეიცავს ორ გასაღებს. ესენია:

მატერიალურ ინტენეტ ნაწილაკი, რომელებიც არიან გაფარდოებადი ჩაშენებული ბლოკების კომპონენტებში.

გლობალური კონტროლი და მართვა ფრეიმვორკის, რომელიც ერთად შეკრებს ჩაშენებულ ბლოკებს და თანამიმდევრული მომსახურების.

არსებობს რამოდენივე ჯგუფი რომელიც კონცენტრირებულია განსხვავებულ მხარეებზე, როგორიცაა:

- კონტროლი ფრეიმვორკის მომუშავე ჯგუფების;
- GENI-ის ცდები შრომით პროცესებსა და მომუშავე ჯგუფებზე;
- ოპერაციების, მარვთის, ინტერგაციის და დაცვის ჯგუფები;
- აპარატურით აღმჭურველი და მენეჯმენტის ჯგუფები;

GENI-ს საერთო კონტროლის ფრეიმვორკი შედგება რამოდენიმე ქვესისტემისა და შესაბამისი ძირითადი ორგანიზაციებისგან:

- კომპონენტების გაერთიანება;
- საინფორმაციო ცენტრი;
- კვლევითი ორგანიზაციები, რომლებიც შედგენა მკვლევარებისა და ექსპერიმენტალური იარღებთ;
- ექსპერიმენტის დაცვის სერვისი;
- “Opt-in” ბოლო მომხმარებელი;
- GENI-ს დამუშავება და მართვა;

საინფორმაციო ცენტრები და განსხვავებული ორგანიზაციები შეიძლება დაუკავშირდნენ ერთმანეთს ფედერაციების გავლით.

GENI-ს კვლევები და რეალიზაციის გეგმა შედგება უწყვეტი სპირალებისგან. ამჟამად არსებობს 3 სპირალი. თითოეული მათგანი გრძელდება 12 თვე. 1 სპირალის დაინსტალირება მოხდა 2008 დან 2009-მდე, მეორე 2009-2010, ხოლო მესამე 2011-ში. პირველ სპირალში, ძირითად მიზანს წარმოადგენდა ერთი ან მეტი ადრეული პროტოტიპების დემონსტრაციაGENI-ს მართვად ფრეიმვორკში და წერტილ-წერტილ მუშაობა მრავალიცხოვანი ტექნოლოგიისა. არსებობს 5 GENI-ს მართვადი ფრეიმვორკი სახელად კლასტერი.

Categories	Project or cluster names (selected)
FIA	NDN, MobilityFirst, NEBULA, XIA, etc.
FIND	CABO, DAMS, Maestro, NetSerV, RNA, SISS, etc. (more than 47 total)
GENI	Spiral1: (5 clusters totally): DETER (1 project), PlanetLab (7 projects), ProtoGENI (5 projects), ORCA (4 projects), ORBIT (2 projects; 8 not classified; 2 analysis projects
	Spiral2: over 60 active projects as of 2009*
	Spiral3: about 100 active projects as of 2011*
* GENI design and prototyping projects can last for more than one spiral.	

Cluster Aიყო the Trial Integration Environment დაფუძნებული DETER-ზე, რომელის მართვას ფრეიმვორკს ფოკუსირებულს ფედერაციებზე, ნდობაზე და დაცვაზე. ის არის ერთი პროექტი დაფუძნებული DETER-ზე, რომელიც არის ინდივიდუალური "mini-GENI" საგამოცდო სტენდი,იგი დემოსტრირებულია, გაერთიანებულია და კოორდინირებულია ქსელის რეზერვუარში. მისი განსაკუთრებული მიზანია გამოყენებადობის უზრუნველყოფა საერთო თემების პარალელურად ფერედაციების გავლით. ის შეიქმნა ორ სხვა პროექტთან ერთდ, ესენია StarBED და ProtoGENI.

Cluster Bიყო მართვადი ფრეიმვორკი დაფუდნებული PlanetLab-ზე, რომელიც დანეგრილ იქნა Princeton University. სპირალი 2 შეიცავდა სულ მცირე 12 პროექტს სხვადასხვა უნივერსიტეტებიდან და კვლევითი ინსტიტუტებიდან. ამ პროექსტების შედეგი არის ინტეგრირებული PlanetLab გამოსაცდელი სტენდი. PlanetLab უზრუნველყოფდა "GENI-wrapper" კოდს AM-ის დამოუკიდებელი განვითარებისთვის და ინტერნეტ ორგანიზაციებისთვის. განსაკუთრებული „Lightweight"იყო წარმოდგენილი PlanetLab ინტერფეისსა და OpenFlow მოწყობილობებზე.

Cluster Cიყო ProtoGENI მართვადი ფრეიმვორკიUtah უნინერსიტეტისგან, რომელიც დაფუძნებულია Emulab-ზე, ქსელის მართაზე და მენეჯმენტზე. სპირალი 2-ის ბოლოს ის

შეიცავს სულ მცირე 20 პროექტს. ClusterC აკავშირებდა ამ არსებულ და ძირეულ სისტემას GENI ფუნქციეების მიწოდებულ გასაღებთან. ინტეგრაცია შეიცავს ოთხ კომპონენტს:

- დაფუძნების ძირითადი დებულება ინტერნეტ2-ზე;
- PCS და NetFPGAკარტები;
- subnets of wireless;
- wired edge clusters;

Cluster Dიყო ORCA (Open Resource Control Architecture) Duke-ის უნივერსიტეტიდან და RENCI-დან, რომელიც თავის მხრივ ფოკუსირებულია სენსორული ქსელის რესურსების განაწილებასა და ინტეგრაციაზე. სპირალი 2 შეიცავს 5 პროექტს. ORCAცდილობს ჩართოს ოპტიკური რესურსი არსებული Metro-Scale Optical-ს გამოსაცდელი სტენდიდან. განსხვავებით სხვა კლასტერებიდან, ORCAრეალიზაციას ახდენს ინტეგრირებული wireless/sensor პროტოტიპის ჩართვის საშუალებზე.

Cluster Eიყო Open-Access Research Testbed მომავალი თაობის უსადენო ქსელში რუთგერსის უნივერსიტეტისგან, რომელიც ფოკუსირებულია მობილობასა და უსადენო ქსელზე. იგი შეიცავს 3 პროექტს სპირალი 2-ის დასასრულს, ძირითადი ORBIT არ შეიცავს სრულ clearing-house-ის რეალიზაციას. Cluster E ცდილობს გამოიკვლიოს რამდენად ეფექტური იქნება მობილურის და უსადენო ქსელის ერთობლივი მუშაობა და მათი შერწყმა GENI-ის არქიტექტურასთან. ამ კლასტერის ერთ-ერთი პროტოტიპია WiMAX.

თავი II

მრავალი ექსპერტი თანხმდება იმაზე რომ საეჭვოა Wireless კომუნიკაციებმა სრულად ჩაანაცვლოს Wired კომუნიკაციაგარკვეული პერიოდის განმავლობაში. ის ნამდვილად ნაკლებად ღირებულია მრავალ პრაქტიკულ აპლიკაციებში, ეს არ არის მიჩნეული როგორც ნამდვილი საჭიროება. ფაქტობრივად, ავტომატური სისტემის ქარხანაში სადაც ხშირად საჭიროა დაუკავშირდნენ ერთმანეთს მცირე კომპონენტებით Wired კომუნიკაცია ვერ შეძლებს გავრცელებას (ადვილად და/ან საიმედოდ) კაბელის საშუალებით. ერთ–ერთი მაგალითი არის მგრძნობელობის აწევა მოძრავ/მბრუნავ მექანიზმზე რომელიც დაკავშირებულია Wired სეგმენტის მაკონტროლირებად ადგილებზე.

ამ მცირე პრობლემის გადაჭრა შეიძლება ადვილად,Wireless უზრუნველყოფით. Hybrid ქსელები არიანკონფიგურაციის შედეგები, რომელშიც ტიპიური Wireless სეგმენტი არის ლიმიტირებული გეოგრაფიულ მანძილზე (დაახლებით ათეული მეტრი) და უკავშირედება მხოლოდ მცირე ტერიტორიაზე. უფრო მეტიც, კონტორლერი არის ჩვეულებრივ დამკვირვებელიWired სეგმენტზე ამგვარ ქსელებში. ეს გულისხმობს, რომ Wireless ქსელები შეეძლებათ თანარსებობა უფრო მეტად ტრადიციულ Wired საკომუნიკაციო სისტემებთან ძალიან დიდი ხნის მანძილზე. ამგვარად, ინტეგრაცია Wireless და Wired კომუნიკაციების

სამეწარმეო სცენარებში გახდება თანააერსებობის მიზეზი რათა მიღწეულ იქნას შეთანხმება ეფექტურ და პერფორმანსულ მუშაობაში.

გარდა ამისა,Wireless შემსრულებლად შესაძლებელია განვიხილოთ Bluetooth ქსელი. ეს ქსელი, რომელიც იყო წარმომშობი დიზაინი როგორც არსებული კაბელის შემცვლელი სისტემა, რომელმაც ფართო გავრცელება ჰპოვა მომავალში და ამჟამად ისმუშაობს მრავალ ადგილას, სამეწარმეო ავტომატიზაციის ჩათვლით. მაგალითად, რეაული დროის Wireless სესნორული სისტემა დაფუძნებულია Bluetooth–ზე. ამ მეთოდს, რომელიც იყენებს წარმომშობი წვდომის კონროლის (MAC)პროტოკოლის მოდიფიცირებულ ვერსიას შთანერგილია და მათი კომპონენტები არიან ხელმისაწვდომი როგორც კომერციული პროდუქტი. თუმცა, მიუხედავად ამ ყველაფრისა ის საინტერესო მომავალია, რამოდენიმე პრაქტიკული მიზეზის გამო.

შესაბამისი სამეწარმეო ქსელები

Profibus DP და Profinet IO

Profibus და Profinet არიან ძირითადი საკონტაქტო გადაწყვეტილებებიProfibus და Profinet საერთაშორისო საზოგადოებისგან სამეწარმეო განვითარებისთვის.

Profibus DP არის ფართოდ გავცრელებული fieldbus ძირითადი master-slave მიმოხილვაზე, რომელიც ასრულებს მონაცემთა შეცვლას controller–სა და ფართო მექანიზმეს შორის, როგორიცაა სენსორები და actuators (slaves)რომლის მაქსიმალური სიჩქარე შეადგენს 12მგ/წმ.

როგორც ზუსტად განსაზღვრული სტანდარტი, არსებობს რამოდენიმე განსხვავებული ტიპები, რომლებიც შეიძლება დაუკავშირდნენ ქსელს მათთვის მნიშვნელოვანი IO კონტროლერით და IO მექანიზმით.

ძირითადათ, Profinet IO შექმნილია იმისთვის რომ გამოიყენებოდეს time division multiple access (TDMA) ტექნიკა და იმის გარანტიად რომ ტრანსმისია იქნება სწრაფი და ზუსტი. პრაქტიკაში, ტრაფიკის დაგეგმარება ნაჩვენებია ნახაზი–1–ზე.

FIGURE 1 – Profinet IO cycle.

სურათზე წრე დაყოფილია 4 ფაზად:

1. პირველი წითელი ფაზა არის მხოლოდ RT-CLASS 3 ტრაფიკისთვის (ძირითადათ კრიტიკული), რომელსაც შეუძლია აიღოს ადგილი და ზუსტად განსაზღვრული ფიზიკური ნაწილი რომელიც აიძულებს განსაკუთრებული სახის სვიჩებს წინასწარ განსაზღვროს Profinet IO.
2. აგურისფერ ფაზაში, მხოლოდ RT-CLASS 2 ფრეიმები არიან შეცვლილი.
3. მწვანე ფაზა არის სარეზერვო ორივე RT-CLASS 2 და RT-CLASS 1 ფრეიმებისთვის, ციკლურიც და არაციკლურიც. ამ ფაზაში, ფიზიკური წვდომის საშუალება არის რეგულირებული ფრეიმის პრიორიტეტების მიხედვით, IEEE 802.1Q შესაბამისად.
4. საბოლოო, ყვითელი ფაზა არის გამოყენებული არარეალური დროის ტრაფიკისთვის.

ამგვარად სხვა RTE ქსელები აღწერილია IEC 61784 სტანდატის მიხედვით, Profinet IO აპლიკაციის პროტოკოლის ფენა არის დაფუძნებული კომუნიკაციის ობიექტის სიზუსტეზე, რომ შეეძლოს შეცვლა I/O controllers-სა და I/O devices–ს შორის.

DeviceNet და Ethernet/IP

DeviceNet და Ethernet/IP (ControlNet და CompoNet–თან ერთად) ნამდვილად არიან კარგად წვდომადი ჩვეულებრივი სამეწარმეო პროტოკოლი (CIP)– ფორმალურად ცნობილი როგორც მართვადი და საინფორმაციო პროტოკოლები, რომელშიც ხელმისაწვდომია ფუნქციონალური თავსებადობის მაღალი ხარისხი ამდაგვარი სახის ქსელებში. ნახაზი 2–ზე გამოსახულია CIP.

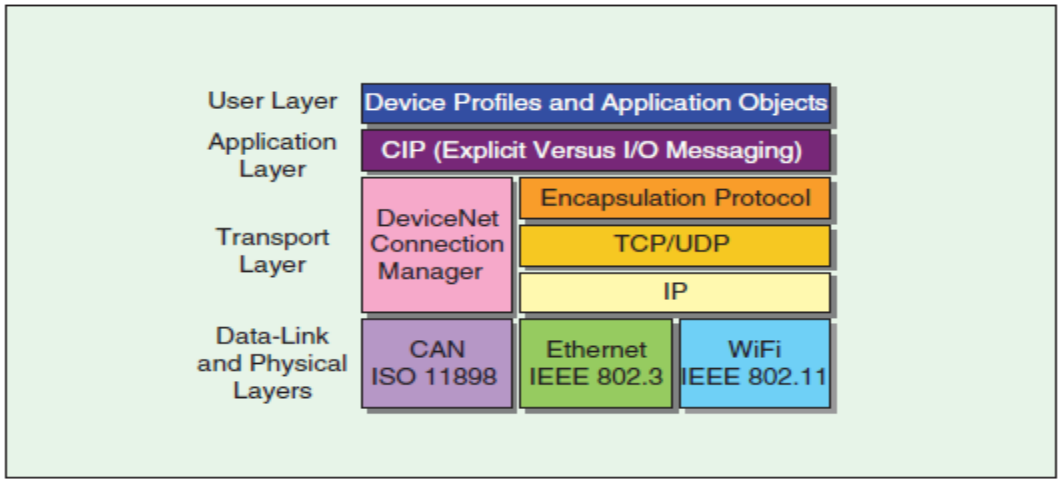

FIGURE 2 – Protocol stack of CIP-based networks.

Seamless bridging და როუტერი არიან დაცულნი ამ პროტოკოლის მიერ, რომელშიც ხელმისაწვდომია პარამეტრიზირებული ინფორმაცია და ბაზის მეთოდი, ის არის ადვილი შესაცვლელი ჰეტეროგენულ განაწილებად სისტემაში.

DeviceNet იღებს controller area network (CAN)პროტოკოლის დასტას, მიუხედავად ტოპოლოგიის bus–სა და დაბალი სიჩქარისა რომელიც არის 500კბ/წმ–ში.

ნაცვლად, Ethernet/IP არის ჩაფიქრებული რომელიცმინდობილია პირობითი Ethernet/IP ტრანსმისიებზე. თუმცა მკაცრად განსაზღვრული დეტერმინისტირებული ოპერატორები არ არიან ნაბოძები, Open DeviceNet Vendor Association (ODVA)აქვს დაწესებული რამოდენიმე სახის წესი. ძირითადად ისინი მოითხოვენ რომ სვიჩის მაღალ–სიჩქარიანი Ethernetიყოს aDOPTED და არასაშირო ქსელის ტრაფიკი იყოს შენახული როგორც დაბალი შესაძლებლობა.

IEEE 802.11

IEEE 802.11 შეიცავს რამოდენიმე სპეციფიკურ სტანდარტს ლოკალური Wireless ქსელისთვის. ყველა მოწყობილობა მაგალითად როგორიც არის family მუშაობს რადიო სპექტრის სპეციალურ ჯგუფში, ცენტრირებული გარშემო ან 2,54 GHz(802.11, 802.11b, 802.11g)და5 GHz (802.11a) შორის.

IEEE 802.11სპეციფიკური სტანდარტი სავალდებულო distributed coordination function (DCF) ხელმისაწვდომია ფიზიკურ გარემოში. გარდა ამისა, არასავალდებულო 802.11 გარშემორტყმულია აგრეთვე ცენტრალიზირებული MAC პროტოკოლით. ამ შემთხვევაში ქსელის წვდომა რეგულირდება სპეციალური პუნქტით. სახელდობრ წერტილოვანი კოორდინატორი, რომელიც ჩუქნის ექსკლუზიურ წვდომას ნებისმიერ Wireless სადგურს. თუმცა, PCF არ არის მიმდინარე დაცვა კომერციული Wifi საზღვრების ფართო უმრავლესობა.

ამ მეთოდში, ქსელის კოორდინატორი პრაქტიკულად ეყოფა superframes–ად, რომლებიც არიან დაყოფილნი ორ ნაწილად. პირველი ნაწილი, სახელად contention access period (CAP), იღებს დაუყონებლივ ადგილს სასიგნალო შუქურის შემდეგ და ძირითადათ მუშაობს განაწილებაზე CSMA/CA მექანიზმი წვმდომის არხის კონტროლისთვის. CAP–ს შემდეგ, ისინი შეიძლება შეიცავდნენ თავისუფალ პერიოდს (CFP).

ჰიბრიდული ქსელების განხორციელება

განსხვავებული ქსელების ურთიერთკავშირი მიღწევადია სპეციფიკური მოწყობილობების გავლით, რომელსაც ჰქვია შუალედური სისტემები (ISs). ამ მოწყობილობებს აქვთ განსხვავებული სტრუქტურა, ფუნქციონალობა და კომპლექსურობა.

ფიზიკური ფენის ურთიერთკავშირი

ISs–ს უმარტივესი ფორმა არის განმეორებადი. ისინი მოქმედებენ ფიზიკურ ფენებში და გამოიყენება subnetwork-ის ურთიერთკავშირისთვის, რომ გააზიარონ ზოგიერთი MAC მექანიზმი. ისინი ჩვეულებრივ ითვისებენ აღდგენილ სიგნალებს მიმდინარე გადამკვეთ განსხვავებულ ქსელის სეგმენტებს. Ethernet ქსელში, მაგალითად, ისინი მუშაობენ შესაბამის პრინციპთან რომელსაც სახელად ქვია 3-R: სიგნალის აღდგენა, retiming და გავრცელება. ამ შემთხვევაში შესაძლებელია იმ პრობლემის წინაშეც კი აღმოვჩნდეთ რომ სიგნალის გადაცემა დასუსტდეს კაბელის შემთხვევაშიც კი, როდესაც ქსელის სიგრძე ძალიან გაიზრდება.

გარდა ამისა მარტივი ორი არხის მექანიზმები, არსებობს სპეციალური სახის განმმეორებელი, რომელიც მარაგდება რამოდენიმე პორტით და რომლის შესრულება მიიღწევა ვარსკვლავური ქსელის ტოპოლოგიით. რადგან გაზრდილი საიმედოობა, hub–ები არია ძალიან ხელსაყრელი ქსელის ინფრასტრუქტურისთვის და აშენებული კაბელებისთვის.

MACმექანიზმი რეგულირდება მისაწვდომის გაზიარებით ტრანსმისიების საშუალებისთვის რომელიც არის მცირე მთლაინი ქსელისთვის. მრავალ შემთხვევაში, მაგალითად როგორიც არისEthernet, CAN ან Profibus ქსელები, ეს ლიდერობა შეზღუდულია.

ურთიერთკავშირი Data-Link ფენეს შორის

IS–ს მუშაობა Data-Link ფენებს შორის წოდებულია როგორც ხიდი. მისი ფუნქცია არის გადამტანი ფრეიმები სისტემებსა (რომელიც არ არინ ან არ შეუძლიათ იყვნენ დამუშავაბადი) და უფორმო საკომუნიკაციო მხარდამჭერ საშუალებებს შორის, რომელიც MAC დონის პროტოკოლია. ხიდი რომელიც არის აღჭურვილი ორზე მეტი პორტით არის ჩვეულებრივ გაგზავნილი როგორც სვიჩი.

მიუხედავად ამისა MAC მექანიზმს არ სჭირდება, მსგავსი subnetworks-დან დაკავშირებული ხიდი/სვიჩის გავლით, კომუნიკაციის მომსახურება.

ნახაზი 3-ზე ნაჩვენებია ურთიერთკავშირი ხიდსა და ჰიბრიდულ ქსელებს შორის.

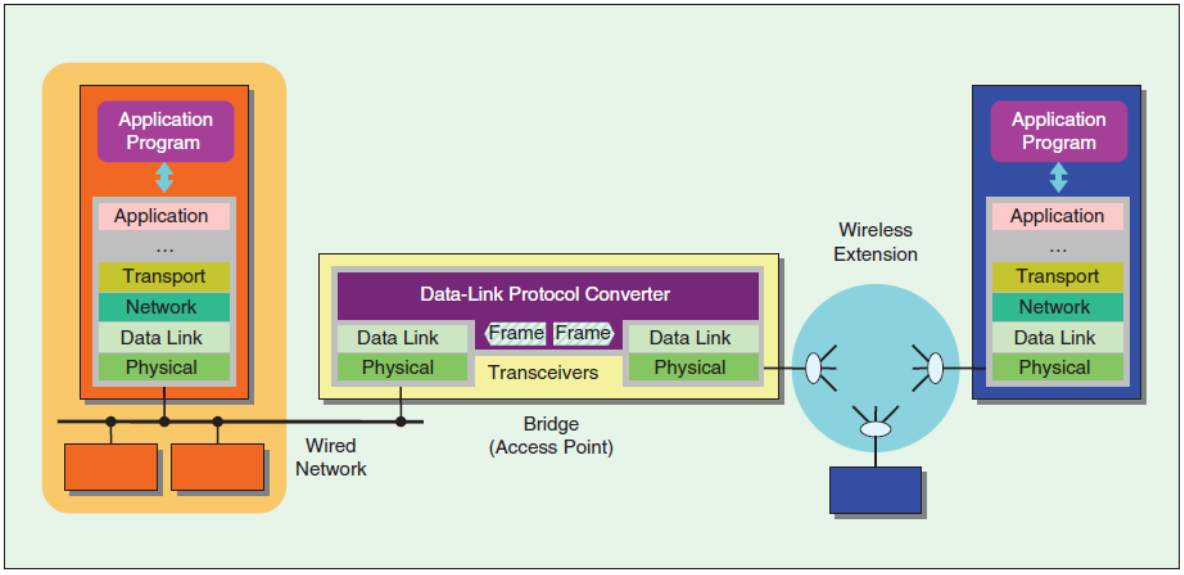

FIGURE 3 – Interconnection via a bridge.

უმაღლესი ფენების ურთიერთკავშირი

ISs მუშაობს ქსელურ ფენებთან ან უფრო ზევით, Gatewayსაერთო ვადა არის ხშირად მხარდაჭერილი. Gateway პასუხისმგებელია ტრანსფერულ პროტოკოლის მონაცემთა ერთეულებზე, ასევე ინფორმაციის საერთო ნაკადის, თხოვების სერვისების და ურთიერთკავშირის სისტემების თხოვების პროცესებს შორის, თარგმნის სავალდებულო პროტოკოლისგან. ჩვენების ძირითადი წერტილი, არ არის მთავარი შეზღუდვა ისეთისახის ქსელებზე რომლებსაც შეუძლიათ ურთიერთკავშირი Gateway–ს გავლით.

სხვა მხრივ, Gateway არის ჩვეულებრივ სამუშაოდ კომპლექსური, ძვირადღირებული მოწყობილობები.

ISs მუშაობს სპეციფიკურ ქსელურ ფენასთან,რომელიც ცნობილია როგორც როუტერი. ამ დონეზე, გამოიყენება მისამართების სქემის ფორმა და პროტოკოლი, იგი უზრუნველყოფილია მსოფლიო მასშტაბით, MAC მექანიზმების, და ურთიერთკავშირის Subnetwors-ის მონაცემთა–კავშირის მომსახურება.

როდესაც ურთიერთკავშირი აღებული იქნება აპლიკაციის ფენაზე, მინდობილობის ვადა ზოგჯერ არის შერჩეული. Proxy ნამდვილად მეტია ვიდრე აპლიკაციის ფენის gateway.ის ჩვეულებრივ წარმოგვიდგენს ქსელის ნაწილს თუ ისინი იყვნენ ერთადერთი კვანძი, შესაძლებელია დამალვა ქვემოთ განლაგებული სტრუქტურის დაცვისთვის ან შესრულებად შედეგებსა.

Wireless გავრცელების შთანერგვა აპლიკაციის ფენაში ნაჩვენებია ნახატი 4–ზე.

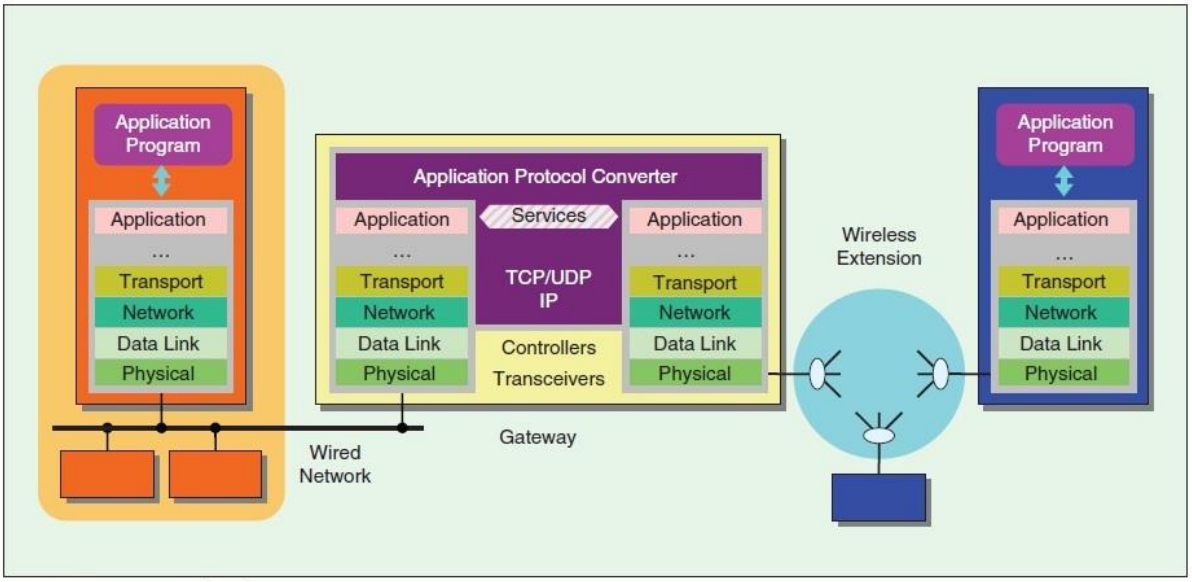

FIGURE 4 – Interconnection via a gateway.

საზოგადოებრივი ქსელები არიან მომავალი ინტერნეტის დამწყები და წარმატებული მოდელი ევროპასა და კიდევ სხვა მრავალ მხარეს. CONFINE პროექტი დამატებულია არსებული FIRE (Future Internet Research and Experimentation- მომავალი ინტერნეტ კვლევები და ექსპერიმენტები) ინფრასტრუქტურები საზოგადოებრივი-ლაბორატორიის დაარსებისგან, ახალი სინამდვილე ექსპერიმენტალური წამყვანი კვლევების აშებენის არის ფედერაცია არსებული საზოგადოებრივი IP ქსელების დანიშვნა 20 000-ზე მეტ კვანძებად და კავშირის 20 000 კმ .

თავი III

ბოლო რამოდენიმე წლის განმავლობაში, ციფრული საზოგადოებისთვის მისაწვდომი გახდა ინტერნეტ წვდომის გასაღები და ზომები, ინტერნეტის ზრდა და თვალსაწიერი დააყენა სტრესის ქვეშ თავისმაარქიტექტურამ და პროტოკოლმა. მზარდი ინტერნეტ შეღწევა სახლებში, სკოლებში, სამუშაო ადგილებზე და ნებისმიერ საზოგადოებრ თუ დაცულ ორგანიზაციებში, მაღალი მოთხოვნადობის დანერგვა და Qos-მგრძნობიარე აპლიკაციები როგორიც არის დიდი ფაილების დისტრიბიცა, ინტერაქტიული მულტიმედია, რეალურ დროის აუდიო და ვიდეო შედეგი .

თუმცა, საინვესტიციო საჭიროებების მახასიათებლები, საკუთრების ღირებულება და მოსალოდნელი ინვესტიციების დაბრუნება გარე ტრადიციულ სატელეკომუნიკაციო ბაზარზე სოფლებში არ ქალაქებში დაბალი შემოსავლის ინდივიდუალურ ან სპეციალურ საჭიროებებზე არ ვრცელდება სტანდარტული ტელეკომის პროვაიდერებისგან.

იგი გამოიწვევს ამ სტრატეგიული ტექნოლოგიების მითვისებას თავიანთი თემების მიერ, ასევე თვით უზრუნველყოფას, მესაკუთრეობას და ოპერაციას. ამ არამომსახურებად ადგილებს აქვთ აღებული კავშირის საჭიროება თავიანთ საკუთარ ველში, აქედან გამომდინარე, ისინი ჩამოყალიბდნენ როგორც „საზოგადოებრივი ქსელები“.

საზოგადოებრივი ქსელი (ასევე ცნობილი როგორც ქვედა–ზედა ქსელები) არის განვითარებადი მოდელი მომავლის ინტერნეტ მასშტაბით ევროპასა და მის გარეთ, სადაც მოქალაქეთა ერთობა მოქმედებეს და აქვთ საკუთარი ღია IP–ზე დაფუზნებული ქსელები, ასევე გასაღებების ინფრასტრუქტურა, როგორც ინდივიდუალური და კოლექტიური ციფრული მოწყობილობები.

ზემოთ აღნიშნული „საზოგადოებრივი ქსელი“ არის ინტერნეტის ნაწილი, მაგრამ არსებობს განსხვავება რამოდენიმე ძირითადი ასპექტებში რომლის მიზეზს წარმოადგენს ბუნება, ესენია:

- ისინი არიან ღია და გამჭირვალე, როგორც მონაწილეობის არარსებული ბარიერი;
- მმართველობა და ცოდნა არის ღია, საჯარო დოკუმენტაციისთვის როგორც ტექნიკურ ისე არა–ტექნიკურ ასპექტებში;

ისინი არიან საკუთრებაში არსებული როგორც საზოგადოებრივი წევრები მათი ქსელების, თვითმართვადი დისტრიბუციისთვის და არაწყვილი სტრუქტურისთვის, რომელსაც შესაძლებლობა ექნება გახსნან საზოგადოებრივი წევრის მონაწილეობა. თვითმარდობა ტოპოლოგიაში და შესაძლებლობებში, ეყრდნობა არამარტო დაგეგვმას არამედ უშუალო მოთხოვნებს, როგორც საზოგადოების წევრი შესაძლებლობა ექნებათ ისწავლონ და გადაწყვიტონ ქსელის გაფართოება მიაღწიონ ახალი წევრის ან პროვაიდერის უფრო მეტ ტევადობას. ამგავრად, ეს ქსელები არ არიან უბრალო გზა, რომ მიაღწიონ გარე ინტერნეტს, მაგრამ ქსელი თვითონ აგრძელებს გლობალურ ინტერნეტს, შიდა სერვერზე და მომსახურეობაზე და ტრაფიკზე.

საზოგადოებრივი ლაბორატორია არის testbed–ი, რომელიც მხარდაჭერილია CONFINE ევროპის ინტეგრირებული პროექტის მიერ. ეს testbed მხარს უჭერს ექსპერიმენტალურ-ორიენტირებულ კვლევას საზოგადოებრივი საკუთრებში არსებული ღია ლოკალური IP ქსელებში. იგი აერთიანებს და ვრცელდება სამ არსებულ საზოგადოებრივ ქსელებს, ესენია:

- Guifi.net (კატალონია, ესპანეთი);
- FunkFeuer (ვენა, ავსტრია);
- AWMN (ათენი, საბერძნეთი);

თითოეული მათგანი არის 500-20 000 კავნძების რიგში, კავშირების დიდი რაოდენობა და საბოლოო მომხმარებელიც კი. ეს ქსელები არიან ექსტრემალურად დინამიური და მრავალფეროვანი. ისინი წარმატებით აერთიანებენ განსხვავებულ wireless და wired ტექნოლოგიებს, სტატისტიკურ, დინამიურ და adhoc მარშუტიზაციის და ასევე მართვის

სქემებს. ისინი აწარმოებენ მრავალ თვითმომმარაგებად, ექსპერიმენტალურ და კომერციულ მომსახურეობებს და პროგრამებს. Testbed უზრუნველყოფს მკვლევართა შეშვებას ამ განვითარებად საზოგადოებრივ ქსელებში, მხარს უჭერს ნებისმიერ დაინტერესებულ მხარეს, რომელიც არის ექსპერიმენტალური სისტემების განვითარების და ტესტირების პროცესში, ასევე ტექნოლოგიებს, რომელიც არის ღია და შიდა მოქმედი ქსელის ინფრასტრუქტურა.

უმთავრესი მოტივაცია არის deployment,როგორიცაა კვლევითი ინფრასტრუქტურა რათა ხელი შეუწყოს საზოგადოებრივი სქელის ზრდას იმ თვალსაზრისით რომ მათი მასშტაბი და მდგრადობა უზრუნველყოფილი იქნება ჩაატაროს ექსპერიმენტალური კვლევები. იმ იმედით, რომ ეს კვლევები პირდაპირ აისახება ხარისხზე, რათა საზოგადოებრივი ქსელები გაუმჯობესდეს და მოამზადოს ნიადაგი მდგარი მოდელის შესაქმნელად.

ამჟამად არსებობს რამოდენიმე გამოწვევა და კვლელების ხაზი, რომელიც მიზნად ისახავს არსებული საზოგადოებრივი ქსელის გაზრდას. მათ შორის, CNs ყურადღებით უნდა განიხილოს გავლენა თავიანთ წევრების კონფიდენციალურობაზე, მისცენ მათ გახსნილობა და ხარისხის დეცენტრალიზაცია. დისტრიბუციის შემცველობა უნდა იყოს ეფექტური, მაგალითად როგორიც არის მარშრუტიზაციის და crosslayer პროტოკოლის ოპტიმიზაცია. კრიტიკულ საკითხს წარმოადგენს კვანძების სიმძლავრე ქსელში (მაგალითად ავტომატური რეკონფიგურაცია, დანერგვა და ნაკლოვანებების დამუშავება და ა.შ.) რადგან შეიძლება ისინი ისხდნენ დისტანციურად, ამიტომ არ არის ადვილი ყოველდღიური საფუძვნლიანი ხელმისაწვდომობა როგორც საზოგადოების ისევე მფლობელებისთვის. ამგვარად, CNs-ის მიზანს წარმოადგენს გაუმკლავდეს მთელ რიგ ჰეტეროგენულ ფიზიკურ ქსელებს დაწყებული უსადენო კავშირიდან დამთავრებული ბოჭკოვანი ინტერნეტით.

თუმცა, ეს გამოწვევები არიან დამისამართებულნი გარკვეული მიმართულებით, რაც გულისხმობს რომ ისინი მუშავდება სიმულაციების მეშვეობით ან ძალიან პატარა კონტროლირებად ლაბორატორიულ გარემოში. რადგან არ არსებობს რეალური testbed ექსპერიმენტები, რომელსაც შეუძლია თარგმნოს მძიმე შედეგებიანი რეალური სცენარი საზოგადოებრივი ლაბორატორია testbed.

დაკავშირებული მუშაობა და გამოცდილება

არსებობს რამოდენიმე ინიციატივაევროპასა და მის გარეთ,CNs მონაწილეობს 3 საწყის ეტაპზე, ესენია:

- testbed –guifi.net (კატალონია, ესპანეთი);
- FunkFeuer (ვენა, ავსტრია);
- AWMN (ათენი, საბერძნეთ);

ბერლინის RoofNet პროექტი არის ექსპერიმენტალური ქსელის ბადე ბერლინში, რომელიც შედგება დაახლოებით 50 შიდა კვანძებისგან, ის უზრუნველყოფს ინტერნეტის ხელმისაწვდომობას სტუდენტებისთვის, ასევე არსებობს VoIP. ამერიკაში, რომელსაც გააჩნია მსგავსი ინიციატივები ისეთ ქალაქებში, როგორიცაა ნიუ იურკი, სიეტლი, ვაშინგტონი ან

ოსტონი, ითანამშრომლეს საჯარო და არამომგებიან ორგანიზაციებთან რათა განევითარებინათ და გაეუმჯობესებინათ უფასო უსადენო ინტერნეტი, hot-spots თავიანთ ქალაქებში, მოქალაქეების ხელმისაწვდომიბის მიზნით. გარდა ამისა, MIT Roofnet პროექტი არის ქსელის ბადე რომელიც შედგება დაახლოებით 50 კვანძისაგან და მოიცავს დაახლოებით ოთხი კვარტალური კილომეტრის ფართობს, რომელიც შესაძლებეს ხდის მცირე და კონტროლირებადი ექსპერიმენტის წყალობით Click Modular როუტერი ინტეგრირებული იყოს მათ სამართავ პულტში.

თუმცა ყველაზე მეტად უსადენო ქსელის განლაგების მიზანია უზრუნველყოს მომსახურეობა (ძირითადად ინტერნეტ დაკავშირება) , რათა არ გახდეს აუცილებელი მკვლევარებისგან შეასრულონ ექსპერიმეტები მათზე. დაუსახლებელი ადგილები განკუთვნილია იმისთვის რომ გაიხსნას testbed ობიექტისათვის განკუთვნილი კვლევითი ობიექტები.

პირველი ინიციატივით რომ ჩატარებულიყო ფართომასშტაბიანი testbed კვლევა წინადადება წარადგინა PlanetLab. ისინი ამჟამად პლანეტის მასშტაბით მართავენ ექსპერიმენტალურ testbed, რომელიც შედგება ათასობით კვანძებისგან, რათა განალაგოს და შეაფასოს განაწილებული აპლიკაციები და მომსახურება რეალურ გარემოში. გასაღები ამ testbed მახასიათებლისა არის რესურსის გაზიარების ცნება განსხვავებულ მკველარევბს შორის ვირტუალიზაციის მეშვეობით. PlanetLab-მა წარადგინა ძირითადი აბსტრაქცია რომელსაც უწოდა ნაწილი, ის საშუალებას იძლება იზოლაცია გაუკეთოს სხვადასხვა ექსპერიმენტებს. ნაწილი არის testbed-ის ორფოგონალური ნაწილი, ან სხვა სიტყვებით რომ ვთქვათ, კვანძების ნაკრები, რომელშიც განაცხადები არის მინიჭებული რესურსების ნაწილის მეშვეობით ისეთი სახის ვირტუალური მანქანგან რომელიც წოდებულია როგორც sliver. ნაწილის ცნება განვითარდა დროთა განმავლობაში ასვეე ქსელის იზოლაციის ანგარიშში და სხვა სახის რესურსებში.

თუ შევხედავთ უსადენო კვლევით სივრცეს, არსებობს რამოდენიმე ინიციატივა თუ როგორ უნდა ჩატარდეს testbed ექსპერიმენტალური კვლევა, მაგრამ არც ერთი მათგანს აქვს აღნიშნული პრობლემის მაღალი მასშტაბის განლაგება და არც რესურსების გაზიარება-ორი ძირითადი პრინციპის საზოგადოებრივი ლაბორატორიის მიღმა. მაგალითად, IBBT w-iLab ფლარდიაში (ბელგია) შედგება ძირითადად 200 დახურული ადგილებისგან რომელიც ვრცელდება სამ ოფისში სართულებზე და ძირთადად შედგება ქსელის კონტროლისგან. საბერძნეთში, NITOS testbed საშუალებას აძლევს მკვლევარებს მთლიანად აკონტროლონ პროგრამული უზრუნველყოფის testbed კვანძები, რომელიც უარყოფს ერთდროულად რამოდენიმე მომხრამებლის არსებობას. გარდა ამისა, იგი შედგება 400 WiFi კვანძებისგან, რომელიც მხოლოდ მცირე ექსპერიმენტების საშუალებას იძლევა. და ბოლოს, ორბიტაზე testbed არის დიდ დახურულ ორგანზომილებიან ქსელში დაახლოებით 400 802.11 რადიო კვანძი, რომელიც შეიძლება დინამიურად ერთამენთთან შევიდეს მითითებულ ტოპოლოგიებში, რაც ყველაზე დიდი დახურული უსადენო ლაბორატორიაა.

გამოწვევები და მოთხოვნები

განლაგება, მართვა და გამოყენების სფერო არსებული CN ობიექტის, სადაც საკუთრების და ადმინისტრაციის ქსელის ინფრასტრუქტურა იყოფა მრავალ პირზე, აკისრებს ახალი გამოწვევებისა და მოთხოვნების ფეხის აყოლას და დიზაინის არქიტექტურის შეწყობას. შერჩევა არის ყველაზე მნიშვნელოვანი მოთხოვნა რომელიც მოკლედ არის განხილული ქვედა განყოფილებებში.

A. სიმსუბუქე დაბალი ღირებულება, თავისუფლება და ღია რესურსი

ამ მიზნის მისაღწევად არსებობს CN-ის ფართოდ გავრცელებული კვანძების მხარდამჭერი საზოგადოებრივი ლაბორატორია testbed, არსებული დანადგარები უნდა გავრცელდეს არა კომპანიებსთვის, რომელიც შეუძლია დამატებითი ტექნიკის შეძენა და ღირებულების შენარჩუნება (მაგალითად გაზრდილი ენერგიის მომხარება) არამედ კვანძის მფლობელებისთვის. აქედან გამომდინარე, ძალზედ მნიშვნელოვანია სიმსუბუქე და დაბალი ღირებულება რათა შესაძლებლობის ფარგლებში შენარჩუნებული იქნეს დაბალი ხარჯები.

ჩვეულებრივ საყოველთაოდ აღიარებული მიდგომების მეორედ გამოყენება, თავისუფლება და პროგრამული ხელისაწვდომობის ღია წყარო არის სავალდებულო განხილვისა და ნდობისათვის, ასევე ერთ-ერთ ძირითად მიზანს წარმოადგენს დატვირთვის შემცირება, მდგრადობა და ქსელის უფასო მიღება თემებში. ამავე მიზნებით CONFINE პროექტი სთავაზობს პროგრამულ და საჭირო დოკუმენტაციას რომ შექმნას სხვა testbeds , როგორც უფასო/ღია პროგრამა.

B. სისტემის სტაბილურობა

ექსპერიმენტების მომზადებისა და შესრულების გაადვილება, მკვლევარების უზრუნველყოფს სათანადო გარემოთი, რომელიც მათ საშუალებას მისცემს უკვე არსებული წარმოების მრავალჯერად გამოყენებას, სწორედ ასეთ გარემოს სთავაზობს Linux OS ძირეულ ნებართვასთან ერთად, რომელიც განვითარდა როგორც დე-ფაქტო სტანდარტის გარემოს ქსელის ექსპერიმენტი.

მეორე მხრივ, უშიშორების თვალსაზრისით, უნდა უზრუნველყონ, რომ ექსპერიმენტს საშუალება მისცენ ძირეული ნებართვის, რათა გავლენა ვერ მოახდინოს ზოგადად CONFINE კვანძის სისტემაზე, რომელიც გამოყენებულია საზოგადოებრივი ლაბორატორიის მიერ. ამის მიღწევა შესაძლებელია ექსპერიმენტის იზოლაციით სპეციალური ან ვირტუალიზაციის ტექნიკის გამოყენებით. მაგრამ მიუხედავად ამ ყველაფრისა არსებობს UNIX სისტემები, რამოდენიმე მათგანი წარმატებით არის დაპორტირებული და ჩაშენებული ტექნიკაში, რომელიც ჩვეულებრივ გამოყენებულია CNs კვანძებში.

C. ქსელის სიმტკიცე

მას შემდეგ რაც საზოგადოებრივი ლაბორატორიის testbed-ის მიზანია საშუალება მისცეს საზოგადოებას ინტეგრირებადი ქსელის ექსპერიმენტიზაციის, ურთიერთქმედების ზოგიერთი დონე ექსპერიმენტსა და მთავარ CN შორის უნდა იქნეს შესაძლებელი. მეორე მხრივ უნდა იყოს უზრუნველყოფილი რომ ექსპერიმენტები არ ჩაერევიან ერთმანეთის საქმიანობაში და არც წარმოების ქსელში. ექსპერიმენტის პოტენციური ზიანი შეიძლება კლასიფიცირებულ იქნეს ორ ტიპად:

- რესურსების მოხმარება: თითოეული ექსპერიმენტი უნდა იღებდეს შეზღუდულ მაგრამ სამართლაინ წილს. მოძრაობის ჩამოყალიბება და განაწილების შეფასება უნდა იქნეს შეზღუდულად გამოყენებული;
- კონფლიქტური პროტოკოლის ქცევა: ექსპერიმენტი მთავარი ქსელის (საშუალო დაშვების კონტროლი, მარშრუტიზაცია, DNS) და სხვა პროტოკოლის რესურსებისთვის (მისამართი, პორტი, არხის დავალებები) უნდა იყოს იზოლირებული ან მკაცრად კონტროლირებადი. Firewall ან პროგრამულად განსაზღვრული ქსელის ტექნიკის (როგორიცაVLAN ჭდეები) ან თუნდაც კავშირის რესურსის სრული ფიზიკური იზოლაცია დამოკიდებულია ყველაზე დაბალი ხელმისაწვდომი ქსელის ფენის ექსპერიმენტის დონეზე.

D. CN წევრების კონფიდენციალურობა

მკვლევარებმა გონივრულად უნდა მისცენ საშუალება მომხმარებლებს და ქსელის მონაცემებს (სტატისტიკური მონაცემებისთვის ან როგორც რეალური დროის კავშირის პროტოკოლი) კონფიდენციალური რეგლამენტის შესაბამისი CNლიზეცნზიების მინიჭებაზე და peering ხელშეკრულებებზე. სწორედ ამიტომ CONFINE სისტემის გამოყენება საზოგადოებრივი ლაბორატორიის მიერ უნდა იყო უზრუნველყოფილი და მოსახერხებელი მექანიზმის ტრაფიკის ფილტრაციისთვის და ქსელის მონაცემთა ანონიმურობისთვის.

E. მართვის ძალა

ერთი საინტერესო მაჩვენებლის მიხედვით კვლევების სინამდვილში CNs არის სხვადასხვა რგოლის შექმნა და გამძლეობა, რომელიც წარმოიქმნება CN ინფრასტრუქტურის განაწილებული მართვის გამო და ობიექტის კავშირის უზრუნველყოფით მიუხედავად იმისა რა მანძილითაც არ უნდა იყვნენ ისინი დაშორებულნი, ასევე ერთ-ერთ მიზანს წარმოადგენს დაბალი ფასები. ხშირად არსებობს მიტოვებული ადგილები კომერციული ISPs მიერ, რადგან განლაგება წარმოადგენს დაბრკოლებას და შემოსავლის პერსპექტივები თითქმის არ არსებობს. აქედან გამომდინარე, სისტემა (რომელიც პასუხისმგებელია მართვის განაწილებაზე CONFINE ექსპერიმენტებში სადაც ჩართულია ისეთი კვანძები, როგორიც არის თემის ლაბორატორია) მზად უნდა იყოს გაუმკლავდეს კავშირის არასტაბილურობას, სპონტანურ გარემოებას და კავშირის და კვანძების მოცდენას.

F. IP მისამართების უზრუნველყოფა

არსებული CN ინფრასტრუქტურის მიზანია დაუშვას აქტიური ექსპერიმენტები საკუთარ თავზე, აგრეთვე ურთიერთმქმედების დამყარება მომხმარებლებისთვის რომელიც ითხოვს CN საჯარო IP მისამართების რეზერვაციას ექსპერიმენტიზაციის პერიოდში.

თუმცა, იმის გამო რომ, ზოგადად IPv4მისამართების სივრცე არის მცირე, უნიკალური მისამართების გამოყოფის ექსპერიმენტი რთულია. გარდა ამისა, ზოგიერთი CNs იყენებს საკუთარ მისამართს გაყოფის სქემაზე დაყრდნობით შეზღუდულ კერძო მისამართებს სპექტრზე შიდა მარშრუტიზაციის და ბოლო მომხმარებლისთვის.

IPv4 მისამართების არასამეწარმეო კოორდინირებული გაყოფა არის გაზრდილი სხვა გამოწვევებსთვის, რომელიც წარმოადეგენს გრძელვადიან მიზანს, რათა შესაძლებელი გახდეს CONFINE testbeds (როგორც საზოგადოებრივი ლაბორატორია) ფედერაციის განლაგება სხვადასხვა CNs-ზე.

IPv6-ზე დაყრდნობით ჩანს ამ გამოწვევის ბუნებრივი გამოსავალი, მაგრამ ჩვენ უნდა გავითვალისწინოთ ის ფაქტი, რომ მხოლოდ რამოდენიმე არსებული CNs ჯერ-ჯერობით სრულად ვერ დაუჭერს მხარს მშობლიურ IPv6 მარშრუტს.

G. თავსებადობა

ახალი CONFINE კვანძები (რომელიც დაარსდა როგორც ექსპერიმენტული ობიექტი) უნდა იყოს თანდათანობით ინტეგრირებადი CN ინფრასტრუქტურის გამოყენებით. ამიტომ, CONFINE კვანძების და არსებული საზოგადოებრივი კვანძების (საზოგადოებრივი მოწლყობილობების) თავსებადობა ყოველთვის უნდა იყოს უზრუნველყოფილი. რადგან CNs-ში კვანძებს ფლობენ და კონფიგურაციას უკეთებენ ინდივიდუალურად და იგი შეიძლება დაფუძნებული იყოს საკუთრებაზე და დახურულ პროგრამულ სისტემაზე, არამოდიფიცირებადი წარმომშობი საზოგადოებრივი კვანძის სამართავი პულტი უნდა იყოს მოთხოვნადი და მხოლოდ რამოდენიმე ვარაუდს უნდა გაუკეთდეს მახასიათებლების და პროტოკოლების მხარდაჭერა ან წარმომშობი საზოგადოებრივი კვანძების კონკრეტული განხორციელება.

H. სპეციფიკური APIs-ს როლი და გამოყენებადობა

Testbed-ის ოპერაცია, დანერგვა და გამოყენება ინტეგრირებულია არსებულ CNs-თან, რომელიც მოიცავს სხვადასხვა როლს. კერძოდ, testbedმენეჯერის როლი, კვანძის მფლობელები და მკვლევარები არიან იდენტიფიცირებულნი.

გამარტივების მიზნით დაკავშირებული ოპერაციების ყოველი რიგი თავიდან ააცილებს კონფიგურაციას იმ მიზეზით რომ გადაფაროს ან დაკარგოს მოვალეობები, APIs სპეციალური როლი და დაშვების კონტროლი უნდა განხორციელდეს.

და ბოლოს, ინსტრუმენტები და APIs უზრუნველყოფა მართვისთვის და CONFINE testbed-თვის როგორიცაა საზოგადოებრივი ლაბორატორია უნდა იყოს როგორც მარტივი და ინტუიციური ასევე შესაძლებელი (თითოეული მონაწილის როლისთვის მიუხედავად შიდა სირთულისა).

საზოგადოებრივი ლაბორატორიის არქიტექტურა

CONFINE testbed, როგორიცაა საზოგადოებრივი ლაბორატორია შედგება სულ მცირე ერთი CONFINE სერვერისგან (ან კონტროლერისგან) და Confine ნაკრები ჩართულია კვანძების გავრცელების პროცესში საზოგადოებრივი ქსელის არსებულ კვანძებში.

კონტროლერი არის ნორმალური კომპიუტერი, რომელშიც უნდა იყოს უშუალოდ მიუწვდომელი CN–ის შიგნიდან (CN Ips გავლით) და ჩვეულებრივ ინტერნეტიდან. კვანძები არიან გაყოფილნი CN ნაწილებად და ჩამოყალიბებული რეაული ქსელის ინფრასტრუქტურად.

CONFINE testbed კვანძები ახორციელებს დამატებითი დაშვების კონტროლს, რესურსების იზოლაციას და მართვის შესაძლებლობებს ობიექტურობისთვის, რათა მიანიჭოს გარე მკვლევარებს/წევრებს კვანძის დამუშავების და ქსელის რესურსების გახსნა.

დიზაინი აღწერილია ამ მონაკვეთში, რათა ხელი შეუწყოს testbed კვანძების დამატებას CN–ის ნებისმიერი მდებარეობაში დამაკავშირებელი დამატებითი მოწყობილობების დახმარებით არსებული CN კვანძებთან ერთად, რათა სპეციფიკური testbed ცვლილებები და მათი კონფიგურაცია მინიმუმამდე იქნეს დაყვანილი.

ამავე დროს ის უზრუნველყოფს მკვლევარების უკვე კარგად ცნობილი Linux გარემოს, მათ შორის:

- მარტივი NAT ხელმისაწვდომობა (როგორც სახლში არსებული ყველა კომპიუტერი);
- საჯარო CN მისამართები (მომსახურეობა შემომავალი კავშირებისა);
- სრული L2 დაშვება VLAN-tagged ქსელში (მარშრუტიზაციის ექსპერიმენტის განხორციელება);
- CN ტრაფიკი (ანომიმურობისთვის);
- Raw L1 მისაწვდომობა (გარკვეულ პირობებში);

A. გრძელვადიანი ხედვა

როგორც ნაჩვენებია ნახაზი 1-ზე, CONFINE კვანძი შედგენა ორი ან სამი მოწყობილობისგან:

- საზოგადოებრივი მაუწყებლობა (CD);
- კვლევის მოწყობილობები (RD);
- აღმდგენი მოწყობილობები;

ასეთი დაყოფა ემსახურება იმ მიზანს რომ შენარჩუნებული იქნას CD-ს სტაბილურობა, რომელიც ყველაზე მეტად თავსებადია ნებისმიერ სამართავ პულტთან. ყველა მოწყობილობა უკავშირდება სახაზო ადგილობრივ ქსელს (LN), ასევე შესაძლებელია გაზიარებულ იქნეს სხვა არა-testbed მოწყობილობებისთვის, როგორც CN კლიენტები იყენებენ CD როგორც gateway-ს.

1. **თემის მოწყობილობა** : CD არის სრულიად ნორმალური საზოგადოებრივი ქსელის მოწყობილობა მინიმუმ ორ სხვადასხვა ქსელის ინტერფეისისთვის: wired ან wireless ერთი დაკავშრება CN და wired ერთი LN. კვანძი არის გამოყენებული testbed სერვერების მიერ, ადმინისტრატორების და მკვლევარებისCD-ის საზოგადოებრივი ინტერფეისის მეშვეობით, თუმცა ადმინისტარციის კვანძი იშვიათად გრძელდება LN-ის გავლით.
2. **კვლევების მოწყობილობა:**RD არის შედარებით ძლიერი მოწყობილობა რომელიც გაშვებულია მორგებული OpenWrt firmware მიერ წობებული როგორც CONFINE, იგი საშუალებას იძლევა ერთდროულად რამოდენიმე slivers შესრულების როგორც Linux კონტეინერი. Slivers აქვს მოწყობილობების რესურსის შეზღუდული ხელმისაწვდომობა, რაც უზრუნველყოფს ქსელის იზოლირებას. ეს გარანტირებულია RD კონტროლის პროგრამის მეშვეობით ისეთი იარაღების გავლით როგორიცაა ebtables, arptables, iptables, tc, Open vSwitch...

   RDახორციელებს შიდა ხიდის შიდა დამისამართებას , ეს არის ზოგიერთი მთელ testbed კვანძებში, რომელიც ეკუთვნის პირად ქსელს სადაც CN ან LN მისამართები არ ეჯახებიან ერთმანეთს. RD მომხმარებელს სთავაზობს ძირითად sliver მომსახურებას შიდა დამისამართებაზე, მათ შორის NATgateway ხელმისაწვდომობას CN-თვის.

   RD ასევე ასრულებს ლოკალური ხიდის როლს, რომელიც უკავშირდება LN-ს wired ინფრასტრუქტურის მეშვეობით. ხიდი გამოიყენება მარტივი ქსელის ფენის ხელმისაწვდომობისთვის CN მეშვეობით და RD ლოკალური მისამართით, რომელშიც გამოიყენება testbed მართისა და დისტანციური მართვის ადმინისტრირება. ადვილი RD კონფიგურაციისთვის და ადმინისტრირებისთვის, ლოკალური ინტერფეისი შეიძლება აგრეთვე აღდგენილი იქნეს მისამართის მეშვეობით, რომელიც ადვილი პროგნოზირებადია. გამართვის დამისამართება, რომელიც აგრეთვე ადვილი განსაჭვრეტია შეიძლება იყოს გამოყენებული რათა შეამოწმონ სხვადასხვაRDs იმავე ლოკალური ქსელის გამართვის მიზნით. RD შეიძლება ჰქონდეს დამატებითი ინტერფეისი, რომელშიც თითოეული მათგანი დაკავშირებული იქნება პირდაპირი ხიდის მეშვეობით. ეს ინტერფეისი შეიძლება

დაკავშირებული იყოს CN ბმულის ფენით და გამოიყენება ექსპერიმეტისთვის ქსელის ქვედა დონეზე.
ყოველი ხიდი იმართება პროგრამული კონტროლის საშუალებით რათა უზრუნველყოს ქსელის იზოლაცია ნაწილს შორის.

3. **მოწყობილობების აღდგენა:** კვანძი შეიძლება შეიცავდეს ზოგიერთ მარტივ აღმდგენ მოწყობილობას, რომლის მიზანია აიძულოს RD-ს გადატვირთვა იმ შემთხვევაში როცა არასწორი მუშაობის შედეგად გამოიყენება ზოგიერთი აპარატურული მექანიზმი (როგორც GPIO პორტი უკავშრედება RD-ს ელექტროენერგიის მიწოდებას), რითაც თავიდან აიცილებს ფიზიკური rebooting მოწყობილობების საჭირეობას, სადაც რთული მისადგომლობაა.
აღმდგენმა მოწყობილობებმა შეიძლება მიიღონ ინსტრუქციები CN-დან ან განსხვავებული სენსორებისგან. მას ასევე შუძლია მიიღოს heartbeat სიგნალი, რომელიც დაცულია კონტროლის პროგრამის მეშვეობით ზოგიერთი პირდაპირი კავშირის გავლით როგორც ხაზის სერია, როცა მოწყობილობის აღდგენში იკარგება heartbeats-ს რიცხვი, სწორედ ეს გადატვირთავს RD-ს. ამ ვერსიის წინა ვერსია შეიძლება დაეხმაროს RD ჩატვირთვაში რომელიღაც აღმდგენ გარემოში (მაგალითად PXE მეშვეობით) ან ზოგიერთი ტექნიკის თანამშრომლობით რათა მოწყობილობების განახლება და აღდგენა იყოს უსაფრთხო.

4. **Node და sliver კავშირი:** კვლევებს და აღმდგენ მოწყობილობებს აქვს მუდმივი მისამართი LN-ში და მათ სჭირდებათ არამარშრუტიზირებადი პროგრამული პროტოკოლი CN მისაღწევად: ისინი უბრალოდ იყენებენ CD's gateway მისამართს, როგორც განულისხმევი gateway. სტატიკური კონფიგურაცია ან DHCP საკმარისია რადგან მისამართები არის მუდმივი.
ამის საპირისპიროდ, sliver-ს კავშრი განისაზღვრება ქსელური ინტრფეისის მეშვეობით, რომელიც არიან მოთხოვნილნი მკვლევარების მიერ sliver დროის განმარტებებში და ინტერფეისზე დამოკიდებულო RD მიერ გათვალისწინებული. სტანდარტული routing კონფიგირაციის არსებობა პირდაპირ კონტროლირდება მკველვარების მეშევობით, რათა თავიდან იქნეს აცილებული ტრაფიკის მოულოდნელი ცვალებადობა არასასურველი ინტერფეისის გავლით.

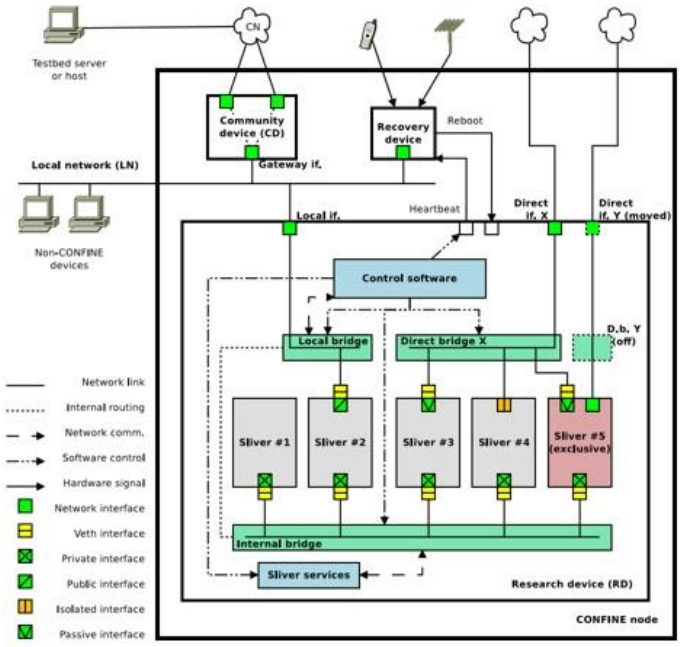

Fig. 1. The architecture of a Community-Lab node.

- ყველა sliver აქვს დაცული ინტერფეისი და მისამართი, რომლის ჰოსტის მხარის veth ინტერფეისი არის მოთავსებული შიდა ხიდში. მისამართები ავტომატურად არის გამოყოფილი RD კერძო ქსელში. მკვლევარმა შეიძლება გამოყენოს აღნიშნული მისამართი როგორც სტანდარტული gateway, ამ შემთხვევაში traffic არის routedRD მეშვეობითლოკალური ხიდის გავლით CD's gateway-ის მისამართი მას შემდეგ რაც NAT იქნება შესრულებული. ეს საშუალებას აძლევს კლიენტს CN-ს ხელმისაწვდომობას მაგრამ არა კავშირების მხრიდან.
  Sliver კონტეინერი-1 ნახაზი 1-ზე წარმოადგენს კერძო ინტერფეისის შიდა ხიდს.
- თუ RD აქვს გამოყოფილი ზოგიერთი საჯარო მისამართი, მკვლევარმა შეიძლება მოითხოვოს საჯარო ინტერფეისი და მისამართი, რომლის host side veth ინტერფეისი განთავსებული იქნება ადგილობრივ ხიდზე, რომელიც საშუალებას მისცემს დაშვებული იქნეს LN-ზე. მისამართი არის ავტომატურად გამოყოფილი საჯარო მისამართების RD's pool-დან , მკვლევარმა შეიძლება გამოიყენოს CD's gateway მისამართი, როგორც სტანდარტული gateway.
  Sliver კონტეინერი-2 ნახაზი 1-ზე წარმოადგენს საჯარო ინტერფეისის ადგილობრივ ხიდს.
- თუ RD აქვს პირდაპირი მისამართი, მკვლევარმა შეიძლება მოითხოვოს პასიური ინტერფეისი, რომლის host side veth ინტრფეისი მოთავსებულია ასოცირებულ პირდაპირ ხიდთან, რითაც საშუალება აქვს CN პირდაპირი წვდომის.
  Sliver კონტეინერი-3 აქვს პასიური ინტერფეისის პირდაპირი X ხიდი.

- თუ RD აქვს პირდაპირი ინტერფეისი, მკვლევარმა შეიძლება მოითხოვოს იზოლირებული ინტერფეისი. ე.ი. VLAN ინტერფეისი დაკავშირებულია პირდაპირ ხიდთან VLAN tags გამოყენებით. ნებისმიერი სახის ტრაფიკი შეიძელბა იყოს გადაცემული და რეგისტრირებული.
  Sliver კონტეინერი-4 აქვს იზოლირებული ინტერფეისის პირდაპირი X ხიდი.

- თუ RD აქვს პირდაპირი ინტერფეისი, მკვლევარმა შეიძლება მოითხოვოს დაუმუშავებელი ინტერფეისი ქსელის მოწყობილობებზე ხელმისაწვდომობისთვის. დაუმუშავებელი ინტერფეისი მოძრაობს sliver კონტეინერსა და მასთან დაკავშირებულ პირდაპირ ხიდს შორის. მას შემდეგ რაც sliver აქვს სრული ფიზიკური კავშირი ქსელის მოწყობილობებზე, ქსელის იზოლაცია ვერ იქნება გარანტირებული, ასე რომ მოხოლოდ ნებადართულია sliver ურთიერთქმედება.
  Sliver კონტეინერი-5 ნახაზი 1-ზე ფლობს RD პირდაპირ Y ინტერფეისს.

5. **Sliver მომსახურეობა:** RD სთავაზობს თავის შიდა მისამართის ზოგიერთ ძირითად მომსახურეობას, რომელიც გახდება ხელმისაწვდომი Sliver-სთვი თავიანთი პირადი ინტერფეისის გავლით. იგი აპირებს გაათავისუფლოს მკვლევარები კონფიგურაციის მომსახურებისგან, ხოლო უზრუნველყოს გარკვეული თვისებები რომელიც მორგებული იქნბა Sliver.
   ფაქტორინგი მომსახურების Sliver გარეთ რომელიც ინახავს რესურსებს და მინიმუმამდე ცვლის დაზიანების რისკს. მაგალითად:
   - DNS: RD მოქმედებს, როგორც სერვერის სახელი, შესაძლებელია ადრინდელი testbed ან ნაწილი-wide დომენების მორგება;
   - SMTP: RD მოქმედებს, როგორც gateway მეილი;
   - NAT gateway სჭირდება slivers ძირითდი კლიენტის კავშირი ქსელში;
   - DHCP მომსახურეობა, რომელიც შეიძლება იქნას გამოყენებული sliver მეშვეობით;
   - DLEP სთავაზობს ხარისხის და სიჩქარის ინფორმაციის კავშირს ქსელის slivers მოწყობილობებისგან;

6. **Slivers ხელმისაწვდომობა:** მიუხედავად იმისა რომ ნაწილს აქვს ნებისმიერი ხელმისაწვდომობა, მკვლევარმა ვერ უნდა შეძლოს წვდომა ნებისმიერი sliversRD-ს ლოკალური მისამართის გავლით მსგავსად PlanetLab, რომელიც დისტანციურს ხდის ბრძანების აღსრულებას და ფაილის გადაცემას ექსპერიმენტების შედეგების შეგროვებისთვის.
7. **საზოგადოებრივი კონტეინერი:** ეს არქიტექტურა საშუალებას იძლევა საზოგადოებრივი ლაბორატორიის კვანძის უფრო იაფი ვერსიის, სადაც CD გადის ვირტუალურ შიდა RD-ს, როგორც საზოგადოებრივი კონტეინერი (CC), ეს ყველაფერი უზრუნველყოფს აპარატურის სტაბილურ ფასს. ასეთ შემთხვევაში თითოეული საზოგადოებრივი ინტერფეისი ითვლება პირდაპირ ინტერფეისად RD-ში, ხოლო CC აქვს veth ინტერფეისი რომელიც მოთავსებულია მასთან

დაკავშირებულ ხიდში. CC-ს Gateway ინტერფეისი არის veth ინტერფეისი განთავსებული ადგილობრივ ხიდში. RD ლოკალური ინტერფეისი შეიძლება შენახული იყოს wired კვანძში და სხვა არა-testbed მოწყობილობებში. CC აქვს რამოდენიმე შეზღუდვები ლოკალურ და პირდაპირ ინტერფეისზე, მაშინ როდესაც slivers ჯერ კიდევ შეუძლია შეღწევა პასიური ან იზოლირებული ინტერფეისის გავლით. სწორედ ამ გზით CC შეიძლება მართოს რამოდენიმე პირდაპირი ინტერფეისი.

B. მდგრადობა

CNS აგებულია მომავალ „რეგულირების დამოკიდებულება“-ზე. ძირითადად გადაწყდა , რომ OpenWrt-ს მიმდინარე დეველოპერი იყოს ვაჭრობასა და მოთხოვნის უზრუნველყოფას შორის.

ეს განხორციელება ითვალისწინებს APIs-ს სპეციფიკურ როლს და CN არსებობას კვანძების მფლობელიბის კონტროლის ქვეშ.

Testbed და nodespecific მცირე ნაკრები (კვაძი,ID, საჯარო გასაღები..) უნდა იყოს გაცვლილი კვანძის მფობელსა და testbed ოპერატორს შორის ცენტრალური ვებპორტალის მეშვეობით და გამოიყენებოდეს RD-ს კონფიგურაციის დასრულებისთვის. კვანძის მართვის ფუნქციაა confine_node_enable/disable, რომელიც შეიძლება გამოყენებულ იქნას ნებისმიერ დროს, RD-ს მონაწილეობით აქტივაციასა ან დეაქტივაციიაში testbed-ში.

Sliver აბსტრაქტული ცნება ხორციელდება ვირტუალიზაციის მეშვეობით, რომელიც მკვლევარებს უზრუნველყოფს საერთო ექსპერიმენტალური გარემოს მეშვეობით, ამიტომ გადაწყვიტეს გამოეყენებინათ Linux კონტეინერი, როგორც ძალიან მსუბუქი ვირტუალიზაციის გადაწყვეტა. ეს საშუალებას იძლევა მკვლევარებს მიენიჭოს root ხელმისაწვდომობა OpenWrt ან Debianguest სისტემებში (sliver), მაგრამ გაშვებამდე მთლიანად აკონტროლებს CONFINE RD ფოსტ სისტემას. LXCმომხმარებლის სივრცის ხელსაწყოები იქნა პორტირებული როგორც ახალი პაკეტი და გამოიყენება CNS კონტროლისთვის LXC კონტეინერს შიგნით.

IPv6 overlay

Testbeds შეიქმნა რადგან რამოდენიმე საზოგადოებრივი ქსელი მკვეთრად შეფერხდა IPv6 მხრდაჭერის ნაკლოვანების გამო . ისინი ჩვეულებრივ იყენებენ კერძო Ipv4 მისამართს, რომ მთელი CNs აღარ არის საკმარისი. CN მოწყობილობების გამოყენება IPv4 ნიშნავს რომ კვლევის მოწყობილობა შეიძლება იყოს NAT ყუთის უკან ან firewalls დანამატი.

IPv4 სივცრის მისამართი ასევე ინარჩუნებს testbed-ს რომ გამოიყენებოდეს სუფთა და ერთგვაროვანი მისამართების სქემისთვის.

IPv6 მიგრაციის გადაწყვეტილება როგორც 6to4, 6in4, ან Teredo რომელსაც არც პრობლემები აქვს 41-ე პროტოკოლთან NAT ყუთში ან firewalls გადატანისდ და არც გამოიყენება IPv4 ძირეული მისამართების ჰოსტად, რომელიც შეიძლება ასევე clash და CNs შორის.

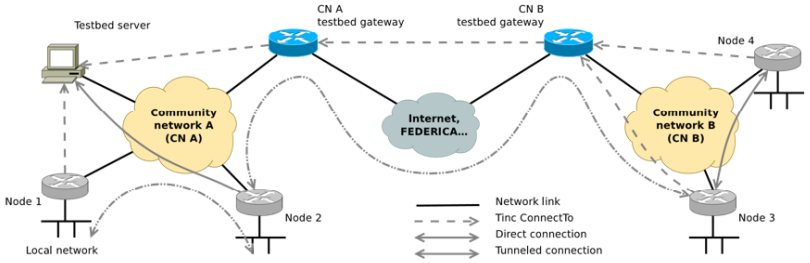

Fig. 2. The IPv6 overlay spanning two community networks.

CONFINE testbed როგორიცაა საზოგადოებრივი ლაბორატორია მუშაობს ამ პრობლემის გარშემო. Tinc ნებას რთავს mesh ქსელის შექმნის, სადაც მონაცემები გაიცვლება პირდაპირ წერტილსა (VPN პროგრამული ზრუნვა ტრაფიკის მარშრუტიზაციაზე) და გასამრავლებელ საბოლოო წერტილს შორის, რომელისაც სჭირდება მინიმალური კონფიგურაცია.

ნახაზი 2-ზე ნაჩვენებია tinc დომენი testbed კვანძში რომელიც უკავშირდება მხოლოდtestbed სერვერს ან CN testbed gateway. Gateways უკავშირდება ერთმანეთს სხვა ქსელის გავლით როგორიცაა ინტერნეტი. ისინი ერთად ქმნიან routed IPv6 ქსელს, სადაც ინდივიდულური ჰოსტი (სერვერი, კლიენტი და gateways) და subnetworks (კვანძი, მოწყობილობა და slivers) გადხა ერთმანეთისთვის ხელმისაწვდომი.

C. საზოგადოებრივი ლაბორატორის ინტეგრაცია არსებულ საზოგადოებრივ ქსელთან

რას აკეთებს საზოგადოებრივი ლაბორატორია testbed განსხვავებულს უკვე არსებულისგან? ეს არის ინტეგრაცია აქტუალურ საზოგადოებრივ ქსელთან (CNs). კვანძის კუთვნილი testbed დგას საზოგადოებრივი ქსელს შორის რომელსაც შეუძლია შეასრულოს ექსპერიმენტი რეალურ გარემოში რეალური მომხმარებლისთვის. ეს ქსელი არის მართლაც საწარმო ქსელი, მაგრამ ექსპერიმენტს უნდა ჰქონდეს გარკვეული შეზღუდვები ან გარკვეული დაცვა საზოგადოებრივი ქსელის მფლობელებისგან.

საზოგადოებრივი ქსელს ყავს რამოდენიმე მფლობელი, რაც ნიშნავს რომ ყოველი მომხმარებელი არის მფლობელი საკუთარი მოწყობილობის. ქალაქში, სადაც ხალხი ცხოვრობს კორპუსიში მომხარებლს ჩვეულებრივ აქვს ერთი მოწყობილობა განთავსებული სახურავზე-ეს კარგი პრაქტიკაა მაგრამ ყოველთვის არ არის შესაძლებელი.

ტიპიური საზოგადოებრივი ქსელს განლაგება ნაჩვენებია ნაზახი 3a-ზე. მწვანე ხაზები წარმოადგენს WiFi კავშირს. ყველაზე მეტად ეს ქსელია გამოყენებული რადგან იაფი, მარტივი და ადვილად მოპოვებადი. თუმცა ეს შეიძლება იყოს სხვა ტიპის მოწყობილობები, როგორიცაა WiMax, Ethernet ან Optical Fiber რომელიც დამოკიდებულია მესაკუთრეზე.

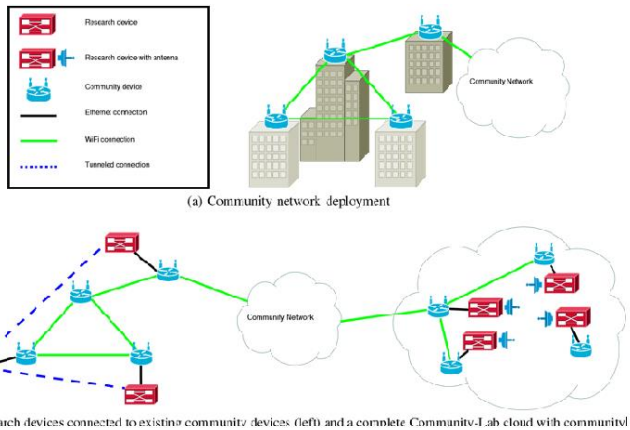

Fig. 3. Community-Lab integration with existing community networks.

საზოგადოებრივი ლაბორატორიის მოწყობილობების ინტეგრაცია შიგნით არსებულ CN მოითხოვს მინიმუმ ერთი საზოგადოების ნაწილის თანამშრომლობას. იმისთვის რომ ეს შესაძლებელი იყოს CONFINE პროექტი უზრუნველყოფს რესურსების დამატებას ზოგიერთი ხარჯის დაფარვის ნაცვლად, არსებობს სამი სხვადასხვა ინტეგრაცია:

1. **ერთი კვლევის მოწყობილობების დაკავშირება არსებულ კვანძთან:**როგორც ნაჩვენებია ნახაზი 3b-ზე (მარცხენა მხარეს) კვლევის მოწყობილობა ანტენის გარეშე მტკიცდება საზოგადოების მომხმარებლის მეშვეობით. RD დაკავშირებული იქნება საზოგადოებრივ მოწყობილობებთან Ethernet კავშირის გავლით.
   ამ შემთხვევაში CONFINE პროექტს სჭირდება მხოლოდ ინსტალაცია ერთი მოწყობილობის (RD) რადგან ის იყენებს არსებულ CD კუთვნილ მომხმარებელს.
2. **კვანძების გაგრძელება მიმდინარე ქსელში:**CONFINE პროექტის ერთი აშკარა მიზანი არის ხელი შეუწყოს განაწილებული ქონების ქსელის მოდელის ზრდას და გამოყენებას. ზოგიერთ შემთხვევაში, როდესაცსაზოგადოებრივ კავშირს სჭირდება ერთ ან მეტი კვანძი გასაფართოვებლად ან ხელმისაწვდომად, პროექტი ხელს შეუწყობს უზრუნველყოს დამატებითი რესურსი. ეს რესურსები განაწილებული იქნება ზოგიერთი საზოგადოებრივი წევრის ადგილმდებარეობაზე, სწორედ ასეთ კვლევით მოწყობილობებზე იქნება მოთხოვნა. ამ შემთხვევაში CONFINE პროექტს დაემატება ახალი CD და საერთო RD.
3. **მრავალჯერადი კვანძების განლაგება სფეციფიკურ სცენარში:** ზოგიერთი სფეციფიკური სცენარი კონტროლდება CONFINE პარტნიორის მიერ. როგორც ნახაზი 3b -ზე (მარჯვნივ) არის ნაჩვენები ეს ნიშნავს რამოდენიმე კვანძის ინსტალაციას. CD უნდა იყოს თავსებადი კვანძი არსებულ CN-თვის სადაც ის შეძლებს დაკავშირებას. RDშეიძლება შეიცავდეს ერთ ან რამოდენიმე WiFi ანტენას და რადიო მოწყობილობებს.
   ამ შემთხვევაში CONFINE პროექტი დამატებული იქნება ახალი CD, საერთო RD და ნებისმიერი სხვა მოწყობილობა საჭიროებისამებრ.

დასკვნა

მოცემულ სამაგისტრო ნაშრომში გადმოცემულია ინტერნეტის მომავალი არქიტექტურის მნიშვნელოვანი ასპექტები ახალი არქიტექტურის ექსპერიმენტიზაციის საფუძველზე. აღწერილია სამი თანმიმდევრული ნაბიჯი თუ როგორ უნდა იმუშავოს ინტერნეტის მომავალმა არქიტექტურამ, ესენია:

1) ინოვაციები ინტერნეიტს სხვადასხვა ასპექტში;

2) საერთო პროექტების ჩადება მრავალგზის ინოვაციებში;

3) რეალურ მასშტაბიანი ექსპერიმენტიზაცია.

მობილობა გახდა წამყვანი გასაღები მომავალი ინტერნეტისთვის. კონვერგენციული მოთხოვნების მზარდობა ჰეტეროგენულ (სხვადასხვაგვაროვანი) ინტერნეტისა (როგორიც არის ქულერი IP) და უსადენო ad hoc ან მგრძნობიარე ქსელისა, განსხვავდებიან ტექნიკური სტანდარტებით და ბიზნეს მოდელით. აქედან გამომდინარე დიდი ყურადღება ეთმობა ჰიბრიდული სადენიანი/უსადენო ქსელის არქიტექტურას მოცემულ ნაშრომში.