

მარშუტიზაციის პროტოკოლების ანალიზი სამხედრო ქსელებში

თ.გ.დ. ნანი არაბული
დავით აღმაშენებლის სახელობის
ეროვნული თავდაცვის აკადემია.
ასოცირებული პროფესორი

ფ.ა.გ.დ. რობეო ბაღდავა
დავით აღმაშენებლის სახელობის
ეროვნული თავდაცვის აკადემია.
ასოცირებული პროფესორი

აბსტრაქტი

მობილური ad-hoc უკაბელო ქსელები გვადლევს საშუალებას შევქმნათ დამოუკიდებელი და დროებითი ქსელები, ყოველგვარი ცენტრალური მენეჯმენტის ან ინფრასტრუქტურის გარეშე. შუალედურ კვანძებს, მიუხედავად მათი არასტაბილური ტოპოლოგიისა, უნდა შეეძლოთ გაგზავნონ და მიიღონ მონაცემები ნებისმიერ დროსა და ნებისმიერ ადგილას, თუმცა ხშირია კვანძებს შორის კავშირის წყვეტა. ამიტომ, ნებისმიერი უსადენო დიზაინის სტრატეგიები დამოუკიდებელია მარშუტიზაციის პროტოკოლის შერჩევაზე. ნაშრომში შეფასებულია DSDV, AODV და DSR მარშუტიზაციის პროტოკოლების საშუალებით პაკეტების მიწოდების კოეფიციენტის ეფექტი.

საკვანძო სიტყვები: მარშუტიზაციის პროტოკოლი, Ad-hoc ქსელი, AODV, DSR, DSDV.

Analysis of routing protocols in military networks

Nani Arabuli

David Agmashenebeli National Defense Academy.
Associate Professor. Doctor of Technical Sciences

Romeo Galdava

Associate Professor. PhD in Mathematics

Abstract

Mobile ad-hoc wireless networks allow us to create independent and temporary networks without any central management or infrastructure. Intermediate nodes, regardless of their unstable topology, should be able to send and receive data anytime and anywhere, however, the connection between the nodes is often broken. Therefore, any wireless design strategies depend on the selection of the routing protocol. The paper evaluates the effect of packet delivery rate through DSDV, AODV and DSR routing protocols.

Keywords: Routing protocol, Ad-hoc Networks, AODV, DSR, DSDV.

შესავალი

სამხედრო ქსელებს აქვთ უნიკალური მახასიათებლები, რადგან ისინი უზრუნველყოფილი უნდა იყვნენ უსაფრთხოების მაღალი მოთხოვნებით და აუცილებლობით, რომ ადაპტირდნენ ცვალებად გარემოებებთან და ლანდშაფტთან. სამხედრო ოპერაციების მოგება ძირითადად დამოკიდებულია დინამიური და ზუსტი გადანაცვლებების მიღებაზე, რომელიც დაფუძნებულია რეალურ დროში კრიტიკულ ინფორმაციაზე წვდომაზე. ეს ინფორმაცია შეიძლება მოდიოდეს თანამგზავრიდან, ბრძოლის ველის სენსორიდან ან სხვა სასაზღვრო მონაცემებიდან. მებრძოლები მიიღებენ ნამდვილ უპირატესობას მხოლოდ იმ შემთხვევაში, თუ ინფორმაციის გადასაცემად გამოყენებული ქსელის ინფრასტრუქტურას ექნება გამართული პროგრამული უზრუნველყოფა, იქნება დინამიური და უსაფრთხო.

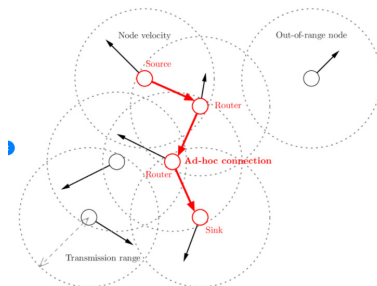
მობილური ქსელის მახასიათებლები, როგორცაა მობილურობა, ქსელის ზომა და მომსახურების ხარისხი, განუყოფელი ფაქტორებია კონკრეტული სცენარისთვის ქსელის დემონსტრაციის ფარგლებში. სამხედრო სცენარები, რომლებშიც გამოყენებულია უსადენო ქსელები, უზრუნველყოფს ისეთ გარემოს, რომელიც აფართოვებს ქსელურ ჩართულობას და დაცულობას. დაცული მობილური უსადენო ქსელი შესაძლებელია შეიქმნას საიმედო, ადაპტირებადი მარშრუტიზაციით.

მობილურობა აუცილებელი საჭიროებაა სამხედრო ოპერაციებისათვის. ქვედანაყოფებს გადაადგილებისას ესაჭიროებათ ხმოვანი, საინფორმაციო და შესაძლოა, ვიდეო კავშირითაც უზრუნველყოფა. ყოველივე ამის გამო, მობილურობა ძირითადი საკითხია სამხედრო ქსელის დაგეგმარებისას. ქსელი უნდა იყოს ავტონომიური, თვითფორმირებადი, თვითაღდგენადი და მისი გამოყენება უნდა იყოს შესაძლებელი ნებისმიერ ადგილას ინფრასტრუქტურის მონაცემის გარეშე. ასე რომ, ქსელი უნდა იყოს მობილური და სიტუაციური.

ქსელის ზომა (დაფარვა) განისაზღვრება კვანძების რაოდენობით, დაფარვის არეალით ან ორივეთი ერთად. დაფარვის დიაპაზონი განისაზღვრება როგორც წრიული დაფარვის რადიუსი ან როგორც მაქსიმალური მანძილი, სადამდეც შეუძლია სიგნალს რომ მიაღწიოს დანაკარგების გარეშე. დიაპაზონიც და დაფარვაც განისაზღვრება როგორც საზომი ერთეულები, საკმარისი სიგნალის სიძლიერისა სხვადასხვა გარემოსა და რელიეფზე. დიდი რაოდენობის კვანძებმა შეიძლება თავი მოიყაროს მართვის ცენტრთან ახლოს, ანდა მიმოიფანტოს მართვის ცენტრიდან შორს. ორივე შემთხვევაში ქსელის ზომა (კვანძების რაოდენობა და დაშორება) ქსელის პროექტირების მთავარი ფაქტორია. თუ ქსელი გადატვირთულია აქტიური კვანძებით, გენერირებული ტრაფიკი ზღუდავს ქსელის ხელმისაწვდომობას ქსელის მოცულობის გადაჭარბებით, ხოლო თუ ქსელი განიცდის აქტიური კვანძების სიმცირეს, შესაძლებელია მეტად დაშორებული კვანძი დარჩეს რადიო დაფარვის გარეშე, სიგნალის არასაკმარისი სიმძლავრის გამო.

ქსელის მომსახურების ხარისხი (QoS) არის უმნიშვნელოვანესი და ისაზღვრება გარკვეული პარამეტრებით. მომსახურების ხარისხი მოიცავს: შეფერხებას, მოცულობას, დაფარვასა და ბიტური ცდომილების სიხშირეს (BER). შეფერხების დიდი ნაწილი დამოკიდებულია უსადენო ქსელის დამუშავების სიმძლავრეზე და გამტარობაზე. მოცულობა ხდება პრობლემატური როდესაც დიდი რაოდენობის კვანძები ითხოვს ერთდროულად წვდომას შეზღუდული რაოდენობის რესურსებზე.

სწორედ ამიტომ საჭირო გახდა მობილური Ad-hoc ქსელის შექმნა. მობილური ad-hoc ქსელები არის უკაბელო ad-hoc ქსელის ქვეკლასი, რომელსაც აქვს დინამიური ქსელის ტოპოლოგიისა და მოძრავი კვანძების არაჩვეულებრივი თვისებები და განკუთვნილია პორტაბელურობის მხარდასაჭერად. მობილური ქსელები შეიცავს თვითნებურად მოძრავ კვანძებს. ყველა მოძრავი და სტაციონარული კვანძს შეუძლია დაუკავშირდეს ერთმანეთს უკაბელო ქსელით. ნაკლები ინფრასტრუქტურის გამო, ამ ავტონომიურ კვანძებს შეუძლიათ შეუერთდნენ ან დატოვონ ქსელი ნებისმიერ დროს (სურათი 1).

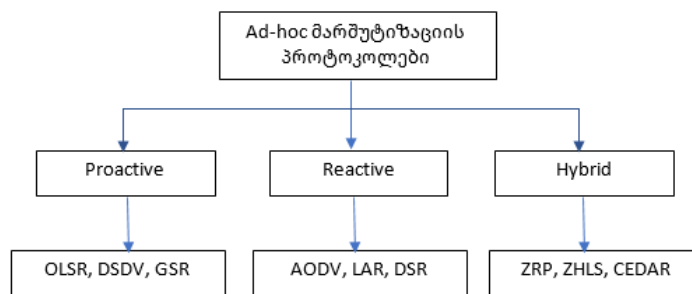


სურ 1. მობილური ad-hoc ქსელის მაგალითი: შავი ისრები - კვანძების სიჩქარე, წითელი ისრები - ad-hoc გადაცემა.

მობილურ ქსელს აქვს რამდენიმე უნიკალური მახასიათებელი: არაფიქსირებული ინფრასტრუქტურა; დინამიური ტოპოლოგია; ღია მედია; ცენტრალური კოორდინატორის ნაკლებობა; შეზღუდული გამტარუნარიანობა; შეზღუდული ენერგო სიმძლავრე და ა.შ. ასეთ ქსელებში უსადენო კავშირები ძალზედ მგრძობიარეა და უმეტეს შემთხვევაში შეიძლება ჩავარდეს კვანძების გადაადგილების ან დაბრკოლებების გამო. აქედან გამომდინარე, მარშრუტიზაცია ad-hoc ქსელებში ძალზედ მნიშვნელოვანია.

ძირითადი ნაწილი

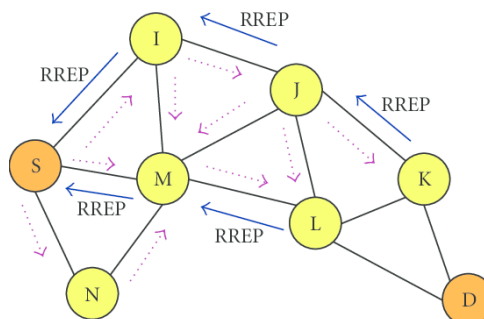
მარშრუტიზება არის მეთოდი, რომელიც მოიცავს მონაცემთა გაცვლას ქსელის ერთი კვანძიდან მეორე კვანძამდე. უკაბელო ქსელებში მარშრუტიზაციის პროტოკოლები ძირითადად კლასიფიცირდება ქსელის სტრუქტურის, კომუნიკაციის მოდელის, მარშრუტიზაციის სტრატეგიის მიხედვით ¹. მარშრუტიზაციის სტრატეგიიდან გამომდინარე, მარშრუტიზაციის პროტოკოლები შეიძლება დაიყოს Proactive, Reactive და Hybrid მარშრუტიზაციის პროტოკოლებად (სურათი 2.)



სურ.2. მარშრუტიზაციის პროტოკოლების კლასიფიკაცია.

პროაქტიულ მარშრუტიზაციის პროტოკოლებში კვანძებს აქვთ მარშრუტიზაციის ცხრილი, სადაც კვანძები ქმნიან მარშრუტებს, სანამ ისინი იქნება საჭირო. აქედან გამომდინარე, მარშრუტის აღმოჩენა ხორციელდება ბევრად უფრო სწრაფად, ვიდრე რეაქტიულ პროტოკოლებში, სადაც კვანძები რეაქტიულ პროტოკოლებში ქმნიან მარშრუტებს ზუსტად მაშინ, როდესაც ის არის საჭირო. ხოლო ჰიბრიდულ პროტოკოლებში კვანძები აერთიანებს როგორც რეაქტიულ, ისე პროაქტიულ სტრატეგიებს.

Ad-hoc On-demand Distance Vector (AODV) არის რეაქტიული პროტოკოლი. მისი მეთოდოლოგიაა hop-to-hop მარშრუტიზაცია. კვანძი ადგენს მარშრუტის მოთხოვნას (RREQ), თუ მას სურს იცოდეს მარშრუტი კონკრეტულ დანიშნულებამდე. შემდეგ შუალედური კვანძები აგზავნიან მარშრუტის მოთხოვნას და ამავე დროს, ეს შუალედური კვანძები ქმნიან საპირისპირო მარშრუტს დანიშნულების ადგილამდე². როდესაც კვანძი იღებს მოთხოვნას, რომელსაც აქვს მარშრუტი დანიშნულების ადგილამდე, ის ადგენს მარშრუტის პასუხს (RREP), რომელიც მოიცავს გადასვლების (hop) რაოდენობას, რომლებიც საჭიროა დანიშნულების ადგილზე მისასვლელად. თითოეული კვანძი, რომელიც მონაწილეობს წყაროს კვანძზე პასუხის დაბრუნებაში, ის ქმნის პირდაპირ მარშრუტს დანიშნულების ადგილამდე. სურათი 2 გვიჩვენებს RREQ და RREP-ის მარშრუტიზაციას AODV პროტოკოლში.



სურ. 3. გადაცემა AODV პროტოკოლის მაგალითზე

¹ G. Wang, N. Alamas, and M. Anggraeni, The use of internet of things and big data to improve customer data in insurance company, International Journal of Emerging Trends in Engineering Research, vol. 7, no. 12, pp. 756–761, 2019.

² D. O. Akande et al., "A Network Lifetime Extension-Aware Cooperative MAC Protocol for MANETs With Optimized Power Control," IEEE Access, vol. 7, pp. 546–557, 2019.

Dynamic Source Routing (DSR) წარმოადგენს რეაქტიულ მარშრუტიზაციის პროტოკოლს. ეს პროტოკოლი შექმნილია უსადენო ქსელებში საკონტროლო პაკეტების მეშვეობით დახარჯული გამტარუნარიანობის შესამცირებლად და პერიოდული ცხრილის განახლების შეტყობინებების წაშლით. DSR პროტოკოლში არ არის საჭირო ქსელის ინფრასტრუქტურა ან ადმინისტრირება, რადგან ეს ქსელები სრულიად თვითკონფიგურირებული და ორგანიზებულია. წყაროს მარშრუტიზება არის მეთოდი, რომლის მიხედვითაც წყაროს პაკეტი განსაზღვრავს კვანძების სრულ თანმიმდევრობას, რომლის მეშვეობითაც ხდება მონაცემთა პაკეტების გადაგზავნა. წყაროს მარშრუტიზაციას არ სჭირდება მარშრუტის ინფორმაციის შენახვა.

Destination Sequenced Distance Vector (DSDV) წარმოადგენს ერთ-ერთ ფართოდ გავრცელებულ პროაქტიულ მარშრუტიზაციის პროტოკოლს მობილურ ქსელებში. აღნიშნული პროტოკოლის ალგორითმი დამოკიდებულია დანიშნულების კვანძთან მისასვლელი ჰოპების რაოდენობაზე. ქსელის კვანძებს შორის მონაცემთა პაკეტების გადასაცემად, DSDV პროტოკოლი იყენებს მარშრუტიზაციის ცხრილებს, რომლებიც ინახება ყველა კვანძში. DSDV პროტოკოლს აქვს სამი ძირითადი მახასიათებელი: მაღალი მარშრუტიზაციის ზედნადების შემცირება, „Count to infinity“ პრობლემის და მარყუჟების აცილება. თითოეული მობილური კვანძი შეიცავს მარშრუტიზაციის ინფორმაციის ცხრილს, რომელიც მოიცავს ყველა მარშრუტს დანიშნულების ადგილამდე.

ერთ-ერთი მნიშვნელოვანი ფაქტორი მარშრუტიზაციის პროტოკოლის მუშაობის გასაზომად ნებისმიერ ქსელში არის პაკეტის მიწოდების კოეფიციენტი (Packet Delivery Ratio). პროტოკოლის შესრულება დამოკიდებულია სიმულაციისთვის არჩეულ სხვადასხვა პარამეტრებზე. ძირითადი პარამეტრებია პაკეტის ზომა, კვანძების რაოდენობა, გადაცემის დიაპაზონი და ქსელის სტრუქტურა. პაკეტის მიწოდების კოეფიციენტი არის დანიშნულების ადგილზე მიღებული პაკეტების რაოდენობის თანაფარდობა წყაროდან გაგზავნილი პაკეტების რაოდენობასთან (მათ შორის განმეორებითი გადაცემა). შესრულება უკეთესია, როდესაც პაკეტის მიწოდების კოეფიციენტი მაღალია. მათემატიკურად PDR გამოითვლება შემდეგნაირად:

$$PDR = \frac{\sum NPR}{\sum NPS}$$

ამ კვლევაში ჩვენ გამოვიყენეთ ქსელის სიჭულატოლი NS2. ძვედარეთ და შეაფასეთ DSDV, DSR, AODV მარშრუტიზაციის პროტოკოლების მოქმედება სამხედრო MANET ქსელებში. სიმულაცია გამოიყენებოდა სხვადასხვა რაოდენობის კვანძებისთვის. კვანძების რაოდენობა არის 20, 40, 60, 80, 100 და ისინი მოძრაობენ შემთხვევითად. გადაცემის დიაპაზონი ყველა კვანძში არის 250მ. სიმულაციური ფართობია 1000მ x 1000მ, სიმულაციის დრო 160წმ. პაკეტის ზომა 512 ბაიტი. ცხრილი 1 გვიჩვენებს სიმულაციის პარამეტრებს.

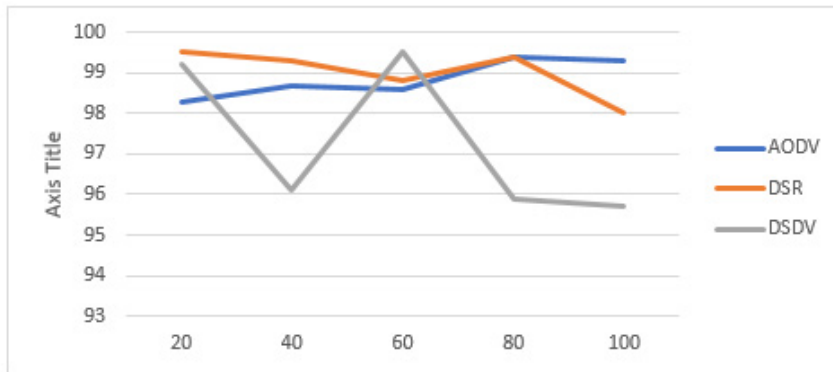
პროტოკოლები	DSDV, DSR, AODV
კვანძების რაოდენობა	20, 40, 60, 80, 100
გადაცემის ტიპი	TCP
პაკეტის ზომა	512 ბაიტი
რიგის სიგრძე	50
გადაცემის დიაპაზონი	250მ.
სიმულაციური ზონა	1000x1000
სიმულაციის დრო	160წმ.

ცხრილი 2 გვიჩვენებს, რომ DSR პროტოკოლი არის საუკეთესო უმეტეს

კვანძებზე, ვიდრე დანარჩენი ორი. მიუხედავად იმისა, რომ DSDV პროტოკოლს ზოგიერთ კვანძებში (20, 60) გააჩნია მაღალი მნიშვნელობა, რაც მიუთითებს იმაზე, რომ გამგზავნის მიერ გაგზავნილი პაკეტების დიდი რაოდენობა წარმატებით გადაიცა. თუმცა მთლიანობაში DSR წარმოადგენს წარმოდგენილი სცენარის მიხედვით საუკეთესო პროტოკოლს, რაც მიიღწევა პროტოკოლის დინამიკის გამო, თავიდან აიცილოს ქსელში მარყუჟის ფორმირება.

ცხრილი 2. სიმულაციის შედეგები

კვანძების რაოდენობა	AODV	DSR	DSDV
20	98.3	99.5	99.2
40	98.7	99.3	96.1
60	98.6	98.8	99.5
80	99.4	99.4	95.9
100	99.3	98	95.7



გრაფიკი 1. AODV, DSR, DSDV პროტოკოლების PDR მნიშვნელობები კვანძებთან მიმართებაში.

დასკვნითი ნაწილი

სამი პროტოკოლის ანალიზი, სხვადასხვა კვანძების რაოდენობით და კვანძების სხვადასხვა სიმკვრივით, გვაძლევს შემდეგ შედეგებს: PDR შესრულების მეტრიკაში, DSR პროტოკოლმა მოგვცა საუკეთესო შედეგი. ასე რომ, DSR უკეთესია, ვიდრე AODV და DSDV. ასევე AODV პროტოკოლმაც კარგი შედეგი აჩვენა, თუმცა DSR იყო საუკეთესო, DSR პროტოკოლის დინამიკის გამო. DSDV პროტოკოლმა არ მოგვცა კარგი შედეგი, მიუხედავად კვანძების სხვადასხვა ზონაში გაუმჯობესებისა. მობილური სამხედრო ქსელის სრულყოფილად შეფასებაში ასევე მნიშვნელოვანია სამომავლოდ შეფასდეს ისეთი პარამეტრები, როგორებიცაა საშუალო გამტარუნარიანობა (TP) და საშუალო დაყოვნება(E2E), რაც მოგვცემს იმის საშუალებას სრულყოფილად შეფასდეს ქსელი და წინასწარ მოხდეს განსაზღვრა იმ პარამეტრების რაც მოგვცემს მონაცემების უშეცდომოდ და უდანაკარგოდ გადაცემის საშუალებას.

გამოყენებული ლიტერატურა

- Kedir Lemma, Bule Hora. Survey on Performance Analysis of AODV, DSR and DSDV in MANET. Computer Engineering and Intelligent Systems Vol.11, No.3, 2020.
- D. O. Akande et al., "A Network Lifetime Extension-Aware Cooperative MAC Protocol for MANETs With Optimized Power Control," IEEE Access, vol. 7, pp. 546–557, 2019.
- G. Wang, N. Alamas, and M. Anggraeni, The use of internet of things and big data to improve customer data in insurance company, International Journal of Emerging Trends in Engineering Research, vol. 7, no. 12, pp. 756–761, 2019.
- Sushama Singh, Atish Mishra & Upendra Singh. Detection and Avoiding of Collaborative Blackhole attack on MANET using Trusted AODV Routing. In Colossal Data Analysis and Networking (CDAN), Symposium. IEEE 2016.
- Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, & Benachir El Hadadi. Modified AODV Routing Protocol to Improve Security and Performance against Blackhole attack. In Information Technology for Organizations Development (IT4OD), 2016 International Conference. IEEE 2016.
- S.H. Jaychandra, R Manjunatha, Nayab Hussain, B.U. Sujan, H.L. Gururaj & B.Ramesh. Analysis of Blackhole Attack in Ad-hoc Network using AODV and MAODV protocol. SPRINGER 2016.
- Neeraj Arya, Upendra Singh & Sushma Singh. Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. In Computer, Communication and Control (IC4), 2015 International Conference. IEEE 2015.
- Abdulleh, M.N., S. Yussof, and H.S. Jassim, Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols. Communications and Network, 7(02): p. 125. 2015.
- Zadin and T. Fevens, "Maintaining path stability with node failure in mobile ad hoc networks," Procedia Computer Science, vol. 19, pp. 1068–1073, 2013.
- Singh, G. and A. Singh, Performance Evaluation of Aodv and Dsr Routing Protocols for Vbr Traffic for 150 Nodes in Manets. International Journal of Computational Engineering Research. 2(5). 2012.