V. IKERGAZTE
NAZIOARTEKO IKERKETA EUSKARAZ

2023ko maiatzaren 17, 18 eta 19a
Donostia, Euskal Herria

ANTOLATZAILEA:
Udako Euskal Unibertsitatea (UEU)

INGENIARITZA ETA ARKITEKTURA

Latentziarik gabeko sareko identifikatzaileen aleatorizazioa kontrol industrialerako sistemetan proaktiboki errekonozimendu erasoak mitigatzeko

Xabier Etxezarreta Argarate,
Iñaki Garitano Garitano,
Mikel Iturbe Urretxa eta
Urko Zurutuza Ortega

55-62 or.
https://dx.doi.org/10.26876/ikergazte.v.03.07

Latentziarik gabeko sareko identifikatzaileen aleatorizazioa kontrol industrialerako sistemetan proaktiboki errekonozimendu erasoak mitigatzeko

Xabier Etxezarreta[1], Iñaki Garitano[1], Mikel Iturbe[1], Urko Zurutuza[1]

[1]Mondragon Unibertsitatea. Goiru Kalea, 2, 20500 Arrasate, Gipuzkoa

xetxezarreta@mondragon.edu

Laburpena

Kontrol industrialerako sistemak askotariko instalazio industrialetan erabiltzen dira, azpiegitura kritikoetan barne, segurtasun-eraso anitzen helburu nagusi bihurtuz. Sare industrialen konfigurazio eta topologia estatikoek, abantaila bat suposatzen dute erasotzaileentzat, erasoa egin aurretik gailu edo zerbitzu ahulak eskaneatzeko aukera ematen baitiete. Artikulu honek IP helbide, MAC helbide eta portu zenbakien aleatorizazioan oinarritutako errekonozimendu erasoen aurkako defentsa proaktibo bat aurkezten du. Lortutako informazioaren distortsioak erasotzaileek lortutako ezagutza gutxitzen du, sareko helbidean oinarritzen den edozein eraso oztopatuz. Sareko identifikatzaileen aleatorizazioa modu moldagarrian egiten da, sarean sartutako gainkarga minimizatuz eta komunikazioetan edozein errore eta latentzia saihestuz. Inplementazioa eta probak benetako ekipamendu industrialarekin gauzatu dira, aurkeztutako soluzioaren eraginkortasuna frogatuz.

Hitz gakoak: Zibersegurtasun industriala, Software bidez definitutako sareak, Moving Target Defense, Erasoen defentsa proaktiboa.

Abstract

Industrial Control Systems are used in a wide variety of industrial facilities, including critical infrastructures, becoming the main target of multiple security attacks. Static networks configurations and topologies, which characterize Industrial Control Systems, represent an advantage for attackers, allowing them to scan for vulnerable devices or services before carrying out the attack. This paper presents a proactive network reconnaissance defense mechanism based on the temporal randomization of network IP addresses, MAC addresses and port numbers. The obtained information distortion minimizes the knowledge acquired by the attackers, hindering any attack that relies on network addressing. The temporal randomization of network attributes is performed in an adaptive way, minimizing the overhead introduced in the network and avoiding any error and latency in communications. The implementation as well as the tests have been carried out in a laboratory with real industrial equipment, demonstrating the effectiveness of the presented solution.

Keywords: *Industrial cybersecurity, Software Defined Networking, Moving Target Defense, Proactive intrusion response.*

1 Sarrera eta motibazioa

Kontrol industrialerako sistemak (ICS) industria-prozesuak monitorizatzeko eta kontrolatzeko erabiltzen diren hainbat elementu espezializatu biltzen dituen termino orokorra da (Stouffer et al., 2015). Hainbat elementuz osatuta daude, hala nola, sentsoreak, eragingailuak, Kontrolagailu Logiko Programagarriak (PLC) edo Gainbegiratze Kontrolerako eta Datuak Eskuratzeko Sistemak (SCADA). Mota guztietako industriatan aurki daitezke, azpiegitura kritikoetan barne, gizartearen ongizaterako eta garapen ekonomikorako ezinbesteko elementuak bihurtuz. Azpiegitura kritikoen adibideak dira zentral nuklearrak, garraio sistemak, sare elektrikoak, presa hidroelektrikoak eta fabrikazio-planta kritikoak.

Tradizionalki, ICSak ingurune isolatuetan inplementatuak izan dira, jabedun hardware eta komunikazio protokoloak erabiliz. Gailuen isolamendua izan da industria prozesuen segurtasuna bermatzeko oinarria, baina teknologia berrien integrazioak, hala nola, Informazioaren Teknologia (IT), jatorriz isolatuak egon diren ICSak sare korporatiboetara agerian utzi ditu, Internetera barne. Aldaketa honen ondorioz, isolamenduan oinarritutako segurtasun neurriak eraginkortasuna galdu dute sare industrialetan. Isolamenduaren gutxitzeak sistema hauek erasoen aurka babesteko behar handiagoa dakar.

ICSen berezitasunak zaildu egiten du ITen segurtasun-soluzioek sistema horien baldintzak eta beharrak bete-

tzea. IT sareekin alderatuta, sare industrialen topologiak estatikoak dira, eta kontroleko sare trafikoa errepikakorra eta determinista da, trafiko gehiena prozesu automatizatuek sortutakoa baita (Iturbe et al., 2016). Industria-sareen ezaugarri estatiko hau egoera abantailatsua bihurtzen da erasotzailearentzat, erasoa hasi aurretik ahuleziak bilatzeko eta aztertzeko aukera emanez. Arazo hauek direla eta, segurtasun proaktibo teknika berrien garapena hasi zen Moving Target Defense (MTD) izenpean. MTD etengabe aldatzen ari den sistema gisa defini daiteke, eraso-azalera aldatzen edo murrizten duena, erasotzaile bati erasoak erraz arakatzea eta egitea zailduz.

Software bidez definitutako sarea (SDN) etorkizun handiko teknologia bihurtu da ICSen segurtasunerako, bai MTD teknikak garatzeko (Zheng eta Namin, 2019) eta, oro har, erasoak detektatzeko eta erantzuteko teknikak garatzeko (Sainz et al., 2018). SDN sare-zerbitzuen diseinua eta gestioa modu deterministan, dinamikoan eta eskalagarrian gauzatzeko erabiltzen den teknika-multzo bat da (Boucadair eta Jacquenet, 2014). Horretarako, kontrol-planoa zentralizatu egiten da; datu-planoa, berriz, sareko gailuetan mantentzen da, eta paketeen prozesamenduan zentratzen da beraien funtzionamendua. Sare tradizionalak ez daude optimizatuta egungo eta etorkizuneko ICSen beharrei erantzuteko. Sarearen kudeagarritasunak, sareko gailuen kopuruaren handitzeak eta ICS ekosistema ezberdinen arteko lankidetzak, malgutasun eta heterogeneotasun beharra dakar, zerbitzuaren kalitatea kaltetu gabe (Molina eta Jacob, 2018). Erasoak detektatzeko eta erantzuteko tekniken garapenaren ikuspegitik, SDN teknologiak abantailak eskaintzen ditu sare tradizionalen aurrean ondorengo alderdietan: (1) sare osoko ikusgarritasuna eskaintzen du, (2) sarearen programagarritasuna areagotzen du erabiltzaileek garatutako aplikazioak integratuz eta (3) sareko fluxuen kudeaketa dinamikoa eta zentralizatua ahalbidetzen du.

Artikulu honetan, SDN eta MTD kontzeptuak konbinatzen dira defentsa mekanismo proaktibo bat garatzeko, industria-kontroleko sareetan errekonozimendu erasoei erantzuna emateko helburuarekin. Lan honen ekarpen nagusiak puntu hauetan laburbil daitezke:

1. Sare-paketeen IP eta MAC helbideak eta portu-zenbakiak denbora errealean aleatorizatzen dituen MTD mekanismoa proposatzen da, erasotzaile batek errekonozimendu fasean lortutako informazioa desitxuratzeko eta gailuetara zuzeneko sarbidea eragozteko benetako informazioa erabiliz.
2. Erabiltzaileak definitutako baimen-zerrenda erabiliz sarearen atributuak aleatorizatzen dituzten eta trafikoa bere helmugara birbidaltzeko fluxu-erregelak hasieratzeko metodologia bat diseinatu da. Baimen-zerrenda honetan baimendutako sareko gailuen arteko komunikazioak jasotzen dira. Informazio honekin fluxu-erregelak instalatzen dira sareko trafikoa bere helmugara arazo gabe iritsi dadin.
3. Sareko identifikatzaileen aleatorizazio estrategia moldagarri bat diseinatu da, latentzia minimizatzeko eta sare industrialen denbora beharrekin betetzeko. Hau, fluxu-erregela gehigarriak eta OpenFlow protokoloaren *priority*-a erabiliz lortzen da.

2 Arloko egoera eta ikerketaren helburuak

Atal honek arloko egoeraren eztabaida labur bat aurkezten du. Alde batetik, arloko MTD teknika ezberdinei buruzko informazioa ematen da. Bestalde, MTDren aplikagarritasuna ICStan eztabaidatzen da.

2.1 MTD teknikak

MTD teknikek sareen izaera estatikoa aldatzea dute helburu, eraso-azalera dinamikoki aldatuz. Teknika hauek ondorengo lau talde operatibotan sailka daitezke (Cho et al., 2020):

Nahasketan oinarritutako MTD: Teknika hauek sarearen konfigurazioa dinamikoki aleatorizatzen dute, erasotzailea erasoaren errekonozimendu fasean nahastuz eta eraso-azalera murriztuz. Talde honetan IP helbideen aleatorizazioa (Jafarian et al., 2012; Sharma et al., 2018), portu zenbakien aleatorizazioa (Chowdhary et al., 2018), sareko trafikoak igarotzen den ibilbideen aleatorizazioa (Aydeger et al., 2021) eta sare-paketeen goiburua aleatorizatzen dituzten teknikak aurki daitezke (Skowyra et al., 2016; Wang et al., 2017). Literaturan badira, halaber, nahasketan oinarritutako MTD teknika ezberdinak konbinatzen dituzten proposamenak ere (Chavez et al., 2015; Zhou et al., 2021). Kampanakis et al. autoreek (2014) IP helbideen eta paketeen edukiaren aleatorizazioa konbinatzen duen proposamen bat aurkeztu zuten errekonozimendu erasoak mitigatzeko.

Aniztasunean oinarritutako MTD: Zerbitzu baliokideak eskaintzean datza, baina inplementazio desberdinekin. Kode aniztasunak programa bat exekuzio-ingurune ezberdinetan inplementa daitezkeen osagaietan banatzea du helburu (Koo et al., 2018). Software-aniztasun teknikek, berriz, web zerbitzari, aplikazio edo zerbitzari birtual baliokideak inplementatzen dituzte sarearen erresilientzia hobetzeko (Huang eta Ghosh, 2011). Azkenik, programazio-lengoaietako aniztasun-teknikek, kode edo SQL injekzio erasoak mitigatzea dute helburu (Taguinod et al., 2015).

Erredundantzian oinarritutako MTD: Funtzionalitate bera eskaintzen duten erreplikak inplementatzean datza. Badira sareko sesioetan erredundantzia eskaintzen duten teknikak (Li et al., 2014) edo funtzionalitate bera duten zerbitzarien erreplikak inplementatzen dituztenak (Kanellopoulos eta Vamvoudakis, 2020).

MTD hibridoa: Teknika hauek nahasketan, aniztasunean eta erredundantzian oinarritutako MTD teknikak konbinatzen dituzte (Alavizadeh et al., 2018a,b).

2.2 MTD kontrol industrialerako sistemetan

MTD teknikak sare industrialen izaera estatikoa iraultzeko sartu dira. Nahasketan oinarritutako MTD teknikak garatzen eta egokitzean zentratu da ikerketa, batez ere IP helbideak eta fluxu-bideak aleatorizatzen dituzten teknikatan.

IP helbideen aleatorizazioan oinarritzen diren teknikak, Linux kernelaren Netfilter (netfilter.org project, 2023) moduluaren erabilpenean oinarritzen dira IP paketeetan itzulpen prozesamenduak aplikatzeko. Hainbat lanek (Ulrich et al., 2017; Pappa et al., 2017) erakusten dute aleatorizazio tartea txikiagotzen den heinean, Joan-etorriko Denbora (RTT) nabarmen handitzen dela, arazo bihurtuz latentzia baxuko komunikazioak behar dituzten sistementzat.

Germano da Silva et al. autoreek (2015) fluxu-ibilbideak aleatorizatzeko teknika bat proposatzen dute, trafiko guztia bide beretik joan ez dadin saihesteko. Honetarako, trafikoa hainbat bidetatik banatzen da, bide batean dagoen erasotzaile batek trafiko guztia ez ikusteko edo jasotzeko. Artikulu horretan ibilbide ezberdinetarako trantsizioan ez denez latentzia kontutan hartzen, Ndonda eta Sadre autoreek (2017) trantsizio hau modu moldagarrian egitea proposatzen dute latentzia arazoak gutxituz. Hau, OpenFlow protokoloaren *hard-timeout* eremua eta fluxu-erregela gehigarriak erabiliz lortzen dute, SDNan oinarritutako sare industrialetan latentzia arazoak minimizatuz.

Chavez et al. autoreek (2015; 2019) soluzio berean nahasketan oinarritutako hainbat estrategia konbinatzea proposatzen dute. Alde batetik, SDN IP helbideen eta fluxu-ibilbideen aleatorizazioa inplementatzeko erabiltzen da, fluxu-erregelak switchetan instalatuz. Bestalde, portu zenbakien aleatorizazioa sareko gailu bakoitzean inplementatzen da Netfilter Linux kernelaren modulua erabiliz. Emaitzek erakusten dute portu zenbakien aleatorizazioa errendimenduan eragin gutxien duen teknika dela, baina sareko gailu bakoitzean eskuzko konfigurazioa egitera behartzen du, sare handi eta konplexutan inplementazioa zailduz.

Lehendik dauden argitalpenek ez bezala, lan honek SDN teknologia IP, MAC eta portuen aleatorizazioarekin konbinatzen ditu, denbora-sentikorrak diren inguruneetan, hala nola ICSetan, errekonozimenduen aurkako defentsa mekanismo proaktibo bat garatzeko. Aleatorizazio prozesua switchetan inplementatzen da, amaierako gailu edo host bakoitzean eskuzko konfiguraziorik behar izan gabe. IP, MAC eta portu zenbaki aleatorio berrietarako trantsizioa modu moldagarrian egiten da fluxu-erregela gehigarriak eta OpenFlow protokoloaren *priority* eremua erabiliz, sarean latentzia arazoak ekiditeko. Ebaluaziorako, benetako ekipamendu industriala erabili da, proposatutako soluzioa errekonozimendu-erasoak mitigatzeko gai dela frogatuz errendimendu-eragin minimoarekin.

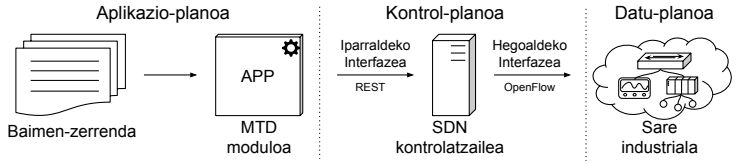
3 Ikerketaren muina

Atal honek, ICSetan SDN erabiliz IP, MAC eta portuen aleatorizazioa eskaintzen duen errekonozimenduen aurkako defentsa proaktibo mekanismoa aurkezten du. Lehenik eta behin, arkitektura eta modulu ezberdinak aurkezten dira. Bigarrenik, aleatorizazio prozesua azaltzen da. Hirugarrenik, latentziarik gabeko sareko fluxu-erregelen eguneraketa moldagarria definitzen da. Azkenik, benetako topologia industrial batean egindako probak eta emaitzak aurkezten dira.

3.1 Arkitektura

Arkitektura SDNan oinarritutako ingurune industrial batean integratzeko eta erabiltzeko diseinatuta dago. 1. irudiak sareko atributuen aleatorizazio arkitekturaren ikuspegi orokorra erakusten du. Arkitektura honen atal nagusiak hauek dira:

1. Irudia: Arkitekturaren ikuspegi orokorra.



Amaierako gailuak: ingurune industrialetan erabiltzen diren hainbat gailuz osatuta dago, hala nola SCADA zerbitzariak, PLCak edo lan-estazioak.

OpenFlow switch: gailu hauen funtzioa sareko trafikoa bere helmugara bideratzea da, aurrez zehaztutako fluxu-erregeletan oinarrituta. Kasu honetan, gailu hauek sare-paketeak prozesatzen dituzte, IP, MAC eta portu

zenbakiak aleatorizatuz.

SDN kontrolatzailea: datu-planoaren eta aplikazio-planoaren arteko komunikazioaz arduratzen da. Kontroladoreak MTD moduluaren eskaerak jasotzen ditu eta switchetara transmititzen ditu OpenFlow protokoloa erabiliz.

MTD modulua: aplikazio-planoan kokatutako aplikazioa da. Bere funtzioa sareko atributu erreal eta aleatorien arteko itzulpenak egiten dituzten fluxu-erregelak OpenFlow switchetan hasieratzea eta eguneratzea da. Hau, SDN kontrolagailuaren iparraldeko komunikazio interfazea erabiliz egiten da.

3.2 Sareko identifikatzaileen aleatorizazio proaktiboa

Hasierako fasean, switchetan instalatzen diren fluxu-erregelak erabiltzaileak definitutako baimen-zerrenda batean oinarritzen dira. Komunikazio bat baimenduta badago, gailuak elkarrekin komunikatzeko gai izango dira benetako IP, MAC eta portuak erabiliz. Aitzitik, baimenik gabeko komunikazioetan, gailu bat beste gailu batekin momentuan gailuari esleitutako ausazko IP, MAC eta portu zenbakia erabiliz soilik komunikatu ahal izango da.

Lehen urratsa sareko gailu bakoitzari ausazko IP helbide, MAC helbide eta portu zenbaki bat sortzean eta esleitzean datza. Alorreko argitalpenekin alderatuta, IP, MAC eta portu zenbakien esleipena modu zentralizatuan gauzatzen da SDN kontrolatzailea erabiliz, sareko gailuen konfigurazioa aldatu behar izan gabe. Aleatorioki esleitutako IP helbide, MAC helbide eta portu zenbaki hauek denbora-tarte baterako bakarrik izango dira baliozkoak eta hurrengo denbora tartean ausazko beste balio batzuekin ordezkatuko dira. Denbora tartea sareko administratzaileak definitzen du eta erabilera kasu bakoitzerako egokitu behar da. Ausazko IP, MAC eta portuak sortu eta gailuei esleitzen zaizkienean, sistemak bi IP, MAC edo portu zenbaki berdin sortu ez direla egiaztatzen du, sistemaren funtzionamenduan sortu daitezkeen erroreak ekiditeko. Kontutan izan gailuen sare-konfigurazioa ez dela aldatzen, itzulpenak OpenFlow switchetan egiten dira eta prozesua guztiz gardena da amaierako gailuentzat.

Ausazko sare-atributuak sortu eta amaierako gailu bakoitzari esleitzen zaizkionean, fluxu-erregelak instalatzen dira OpenFlow switchetan, baimendutako gailuak soilik komunika daitezen benetako IP, MAC eta portuak erabiliz. Fluxu-erregelak switchetan instalatuta daudenean, gailu batetik beste gailu batera doan pakete batek hurrengo prozesua jarraitzen du. Demagun *h1* eta *h2* gailuen arteko komunikazio baimendu bat. Pakete bat lehenengo OpenFlow switchera iristen denean, hau da, *h1* konektatuta dagoen switchera, benetako jatorrizko eta helmugako IP (*rIP*) eta MAC (*rMAC*) helbideak ausazko IP (*vIP*) eta MAC (*vMAC*) helbideetara aldatzen dira. Portu zenbakien kasuan, *h1* eskaera egiten ari bazaio *h2* gailuari, helmugako portu zenbakia soilik aldatuko da. Bestela, *h1*ak *h2*ren eskaera bati erantzuten badio, jatorrizko portua bakarrik aldatuko da. Jatorrizko switchean itzulpen-prozesu honen ondoren, trafikoa saretik bidaltzen da helmugako switchera iritsi arte, hau da, *h2* konektatuta dagoen switchera heldu arte. Trafikoa helmugako OpenFlow switchera iristen denean, ausazko *vIP*, *vMAC* eta *vPort* balio errealetara bihurtzen dira. Horrela, *h1* eta *h2* arteko komunikazio zuzena eta etenik gabea bermatzen da.

Baimenik gabeko komunikazio baten kasuan, aleatorizazio prozesua zertxobait aldatzen da. *h1* eta *h2* gailuen arteko baimenik gabeko komunikazio batean, helmugako gailuari esleitutako ausazko *vIP*, *vMAC* eta *vPort* balioak erabiliz bakarrik komunikatu daiteke. *h1*ek *h2*-ko zerbitzu bati eskaera egiten badio, eta *h1*ek erabiltzen dituen helmugako IP, MAC eta portu zenbakia ez badatoz bat denbora tarte horretan *h2*-ri esleitutako ausazko IP, MAC eta portu zenbakiarekin bat, paketea jatorrizko switchean baztertzen da, helmugara iritsi dadin eragotziz.

3.3 Latentziarik gabeko fluxu-erregelen eguneraketa

Gailuei esleitutako ausazko IP helbideak, MAC helbideak eta portu zenbakiak erabiltzaileak definitutako denbora tarte baterako soilik balio dute. Tarte bakoitzaren amaieran, sare-atributu hauek ausaz sortutako beste batzuengatik ordezkatzen dira, sortu berri den trafikoa ausazko sare-atributu berriak erabiliz bideratuz eta prozesatuz. Erabilgarri dauden fluxu-erregelak zuzenean ezabatzen edo eguneratzen badira, aurreko tarteko ausazko IP, MAC eta portuak erabiltzen ari diren komunikazioak gaizki bideratu daitezke helmugara, sarean erroreak sortuz. Gainera, alorrean dauden proposamenek, latentzia handia sortzen dute, sare industrialetan arazo bihurtuz. Arazo hau saihesteko eta sarean atzerapenak eta etenak ekiditeko, fluxu-erregelak eguneratzeko metodo moldagarri bat diseinatu da, fluxu-erregela gehigarriak eta OpenFlow protokoloaren *priority* eremua erabiliz. 2. irudiak fluxu-erregela eguneraketa prozesua aurkezten du.

Lehenengo faseak, 2a irudian irudikatuta, fluxu-erregelen hasierako egoera adierazten du. Egoera horretan, fluxu-erregelek denbora tarte aktibo horretan esleitutako IP, MAC eta portu zenbaki erreal eta ausazkoen arteko itzulpenak egiten dituzte (eta alderantziz).

Denbora tarte baten amaieran, hurrengo denbora tarterako ausazko IP, MAC eta portu zenbaki berriak sortzen dira. Fluxu-erregelak eguneratzen edo ezabatzen badira, aurreko denbora tarteko ausazko IP, MAC eta portu zenbakiak erabiltzen ari den trafikoan erroreak sortu daitezke. Arazo hau saihesteko, denbora tarte bakoitzaren amaieran, switch bakoitzean fluxu-erregela aktibo bakoitzeko fluxu-erregela gehigarri bat sortzen da. 2b irudian azaltzen den bezala, fluxu-erregela gehigarria aktiboaren kopia bat da, baina lehentasun baxuagoa duena.

2. Irudia: Fluxu-erregelak eguneratzeko jarraitzen den prozesua.

Flow Table		
Priority	**Match**	**Instruction**
10	$H_1 \rightarrow H_2$	src = IP_1, dst = IP_2

(a) Fluxu-erregelen hasierako egoera.

Flow Table		
Priority	**Match**	**Instruction**
10	$H_1 \rightarrow H_2$	src = IP_1, dst = IP_2
9	$H_1 \rightarrow H_2$	src = IP_1, dst = IP_2

(b) Fluxu-erregela gehigarri bat gehitzen da instrukzio berdinarekin baina lehentasun txikiagoarekin.

Flow Table		
Priority	**Match**	**Instruction**
10	$H_1 \rightarrow H_2$	src = IP_3, dst = IP_4
9	$H_1 \rightarrow H_2$	src = IP_1, dst = IP_2

(c) Lehentasun handiena duen instrukzioa ausazko balio berriekin eguneratzen da.

Flow Table		
Priority	**Match**	**Instruction**
10	$H_1 \rightarrow H_2$	src = IP_3, dst = IP_4

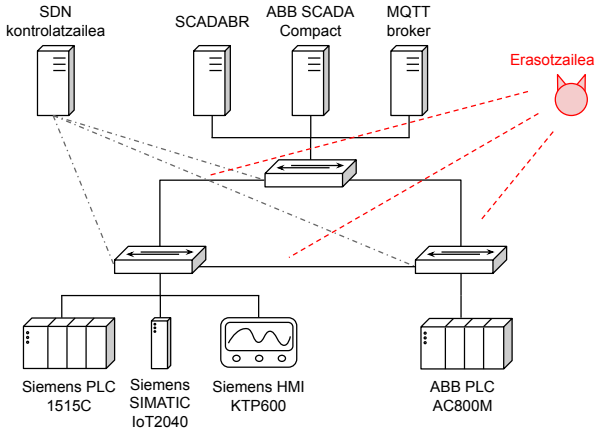
(d) Fluxu-erregela gehigarria fluxu-erregelaren taulatik ezabatzen da.

Fluxu-erregela gehigarriak instalatuta, fluxu-erregela aktiboak eguneratzen dira tarte berrirako sortutako ausazko IP, MAC eta portu zenbakiak esleituz. Fase hau 2c irudian irudikatzen da. Egoera honetan, trafiko berria lehentasun handiena duten fluxu-erregelak erabiltzen hasiko da, eta aurreko tartean sortutako trafikoa, berriz, fluxu-erregela gehigarriak erabiliko ditu. Teknika honekin, denbora tarteen arteko trantsizio moldagarria lortzen da, atzerapenik edo pakete-galerarik sortu gabe.

Azkenik, 2d irudian ikusten den bezala, fluxu-erregela gehigarriak tauletatik ezabatzen dira, hasierako egoerara itzuliz. Prozesu hau iteratiboki aplikatzen da denbora tarte bakoitzaren amaieran, erabiltzaileak zehaztutako denbora edozein dela ere.

3.4 Emaitzak

Ebaluaziorako erabilitako topologia industrial esperimentala, 3. irudian irudikatuta, saltzaile ezberdinetako bi produkzio-lerro independentez eta amaierako gailuz osatuta dago. Gailuak bi maila ezberdinetan daude kokatuta. Lehen mailan, prozesu industrial fisikotik hurbilago dauden gailuak daude instalatuta, hala nola PLCak edo HMIak. Bestalde, bigarren mailan, halako ingurunetan erabiltzen ez diren gailuak kokatu dira, hala nola SCADA edo MQTT zerbitzariak.



3. Irudia: Ebaluaziorako erabilitako topologia esperimentala.

3.4.1 Errendimendua

Aurkeztutako defentsa mekanismoak errendimenduan duen eragina neurtzeko, sarean sartutako atzerapena kontuan izan dugu Joan-etorriko Denbora (RTT) metrika erabiliz. Gainera, OpenFlow switchen fluxu-taulen luzera neurtu dugu eta sare estatiko eta MTD batean behar diren fluxu-erregela kopurua alderatu dugu.

Joan-Etorriko Denbora (RTT): Neurri honek helmugatik igaro ondoren datu-pakete batek bere igorlera itzultzeko behar duen denbora neurtzen du. Neurketak topologiako biderik luzeena kontuan hartuta egin dira, kasu honetan ABB PLC AC800M eta ABB SCADA zerbitzariaren arteko komunikazioa. Sei eszenatoki ezberdin aztertu dira. Alde batetik, sare estatiko batean egin dira neurketak IP, MAC eta portuak aleatorizatu gabe. Bestalde, MTD sare batean neurketak 60, 30, 10, 5 eta 1 segundoko ausazko tarteekin. Eszenatoki bakoitzerako, 150 segundoko 15 neurketa egin dira. 1. taulak neurketen emaitzen batez bestekoa, desbideratze estandarra eta RTT gutxieneko/gehieneko balioak aurkezten ditu.

Fluxu-taularen luzera: IP helbideen, MAC helbideen eta portuen arteko itzulpenak egiten dituzten fluxu-erregela kopurua aldatu egiten da sarean eskuragarri dauden azken gailu eta zerbitzu kopuruaren arabera. Azter

1. Taula: ABB SCADA eta PLCren arteko RTT neurketa emaitzak.

		MTD denbora tartea					
		MTD gabe	60s	30s	10s	5s	1s
RTT (ms)	avg	6.316	6.376	6.383	6.414	6.43	6.505
	stdv	0.166	0.132	0.119	0.148	0.173	0.222
	min	5.952	6.08	6.115	6.138	6.084	6.102
	max	6.818	6.925	6.866	6.991	7.068	7.323

dezagun sareko amaierako gailuen zerrenda bat $\delta \in \Delta$, non amaierako gailu bakoitzak TCP/UDP portu zenbaki kopuru jakin bat duen $p(\delta)$. N sareko amaierako gailuen kopuru osoa adierazten du.

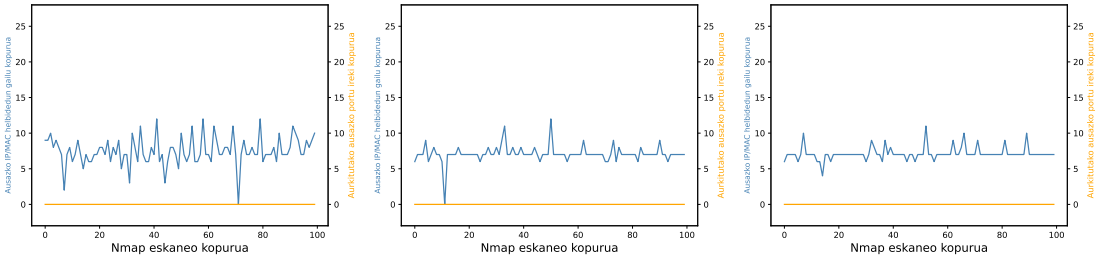
Sare estatiko batean, OSI erreferentzia-ereduaren bigarren geruzan soilik funtzionatzen duen switch S_w bat erabiliz eta paketeak helmugako MAC helbideak erabiliz prozesatzen badira, sareko gailu bakoitzeko fluxu erregela bat nahikoa izango litzateke, hau da, $F^S(S_w) = N$.

Artikulu honetan aurkezten den defentsa proaktiboak, bi gailuen arteko komunikazioan, guztira 2 fluxu-erregela behar dira ARP paketeetarako, 2 IP paketeetarako eta 2 fluxu-erregela TCP/UDP portu ireki bakoitzeko, hau da, $F^M(S_w) = 1 + 2\sum_{i=1}^{N-1}\sum_{j=i+1}^{N}(p(\delta_i) + p(\delta_j) + 2), \delta \in \Delta$.

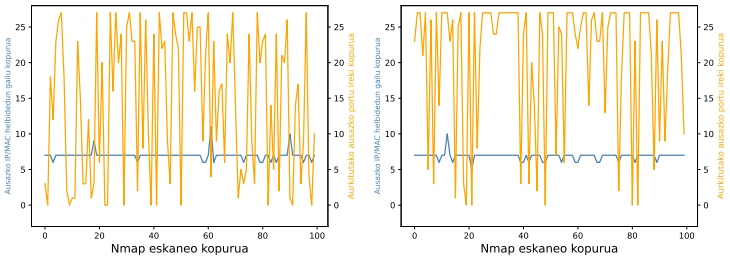
3.4.2 Errekonozimendu erasoen aurkako mitigazioa

Errekonozimendu erasoak mitigatzearen eraginkortasuna probatzeko, 100 eskaneo bata bestearen atzean egin genituen gure 24 biteko azpisare-maskarako sarean. Erasoak *nmap* tresna erabiliz egin dira, sarean gailu aktiboak eta zabalik dauden portuak bilatzeko helburuarekin. Hori probatzeko, jarraian 100 eskaneo eraso egin ziren ausazko tarte ezberdinekin (1, 5, 10, 30 eta 60 segundu). 4. irudiek 100 eskaneo jarraian egin ondoren aurkitutako ausazko IP/MAC helbideak eta portu irekiak aurkezten ditu.

4. Irudia: Konfigurazio esperimentalean lortutako emaitzak 100 nmap eskaneo jarraian eta ausazko denbora tarte ezberdinekin. Lerro urdinak nmap eskaneo bakoitzean ausazko IP eta MAC helbideekin aurkitutako gailu kopurua adierazten du. Lerro laranjak nmap eskaneo bakoitzean aurkitutako ausazko zabalik dauden portu kopurua adierazten du.



(a) 1 segundoko denbora tartea. (b) 5 segundoko denbora tartea. (c) 10 segundoko denbora tartea.



(d) 30 segundoko denbora tartea. (e) 60 segundoko denbora tartea.

Irudi ezberdinetan isladatzen den bezala, denbora tartea gutxitzen denean, ausazko IP eta MAC helbideekin aurkitutako gailu kopurua ausazko-tarte luzeagoekin baino gehiago aldatzen da. Hau da, denbora tarte luzeagoekin, sareko IP helbide-espazio osoaren eskaneatzea denbora tarte horren mugen barruan egiteko probabilitatea handitzen delako. Ausazko tarte laburragoetan, eskaneaketa osoa tarte batean baino gehiagotan gauzatzeko probabilitatea handiagoa da, emaitzen ausazkotasuna areagotuz.

Portuak eskaneatzeari dagokionez, 60 eta 30 segundoko ausazko tarteetan egindako eskaneoek bakarrik aurkitu ahal izan dituzte portu irekiak. Ausazko tarte laburragoekin, errekonozimendu erasoetan lortutako informazioa berehala baliogabetzen da. Erasotzaile batek sarean gailu aktibo bat aurkitu eta bere portuak eskaneatzen hasten

denean, aleatorizazio denbora tartea amaitzen bada eta gailu horri ausazko IP eta MAC helbide berriak esleitzen bazaizkio, erasotzaileak gailura sarbidea galtzen du aurreko denbora tarteko ausazko IP eta MAC helbideak erabiliz. Erasoarekin jarraitzeko, erasotzaileak IP helbide-espazioa berriro eskaneatu behar du sare industrialean gailu aktiboak aurkitzeko. IP/MAC helbide eta portu zenbaki espazio osoa eskaneatzeko behar den denbora dela eta, 10, 5 eta 1 segundoko aleatorizazio denbora tarteetan, IP/MAC helbideen informazioa portu eskaneoa egin baino lehenago aleatorizatzen da, zabalik dauden portuak identifikatzea ezinezko bihurtuz.

4 Ondorioak

Artikulu honek SDN teknologia erabiliz sare industrialetan IP helbideak, MAC helbideak eta portu zenbakiak aleatorizatzen dituen defentsa mekanismo bat aurkezten du. Sistema honen helburu nagusia errekonozimendu erasoak proaktiboki mitigatzea eta baimenik gabeko gailu bat beste gailu batekin komunikatzea saihestea da. Hori lortzeko, sareko gailu bakoitzari ausazko IP eta MAC helbideak eta portu zenbakiak esleitzen zaizkio, eta epe mugatu baterako baino ez dira baliozkoak. Emaitzek erakusten dute erasotzaile batek errekonozimendu fasean jasotzen duen informazioa ausazkoa dela eta denboran zehar aldatzen dela. Gainera, ausazko IP helbide, MAC helbide eta portu zenbaki berrietarako trantsizioa modu moldagarrian egiten denez, sare estatiko tradizional batekin alderatuta sartutako atzerapena minimoa da, denbora kritikoa den sistemetan inplementatzeko aukera emanez.

5 Etorkizunerako planteatzen den norabidea

Etorkizuneko lerro gisa, fluxu-erregelen eguneraketa fluxu bakoitzeko egitea gustatuko litzaiguke, fluxu-erregela guztiak batera eguneratzea arazo bihurtu ez dadin sare konplexu eta handietan, errendimenduan eragin gabe. Horrez gain, honeypot industrialak aurkeztutako MTD sarean integratzea gustatuko litzaiguke, erasoak gailu hauetara birbidaltzeko.

Erreferentziak

Alavizadeh, H., Hong, J. B., Jang-Jaccard, J., & Kim, D. S. (2018a). Comprehensive security assessment of combined mtd techniques for the cloud. In *Proceedings of the 5th ACM Workshop on Moving Target Defense*, MTD '18, 11–20, New York, NY, USA. Association for Computing Machinery.

Alavizadeh, H., Jang-Jaccard, J., & Kim, D. S. (2018b). Evaluation for combination of shuffle and diversity on moving target defense strategy for cloud computing. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 573–578.

Aydeger, A., Manshaei, M. H., Rahman, M. A., & Akkaya, K. (2021). Strategic defense against stealthy link flooding attacks: A signaling game approach. *IEEE Transactions on Network Science and Engineering*, 8(1):751–764.

Boucadair, M. & Jacquenet, C. (2014). Software-Defined Networking: A Perspective from within a Service Provider Environment. RFC 7149.

Chavez, A. R. (2019). Moving target defense to improve industrial control system resiliency. In *Industrial Control Systems Security and Resiliency*, 143–167. Springer.

Chavez, A. R., Stout, W. M., & Peisert, S. (2015). Techniques for the dynamic randomization of network attributes. In *2015 International Carnahan Conference on Security Technology (ICCST)*, 1–6. IEEE.

Cho, J.-H., Sharma, D. P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T. J., Kim, D. S., Lim, H., & Nelson, F. F. (2020). Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys Tutorials*, 22(1):709–745.

Chowdhary, A., Alshamrani, A., Huang, D., & Liang, H. (2018). Mtd analysis and evaluation framework in software defined network (mason). In *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, SDN-NFV Sec'18, 43–48, New York, NY, USA. Association for Computing Machinery.

Etxezarreta, X., Garitano, I., Iturbe, M., & Zurutuza, U. (2023). Low delay network attributes randomization to proactively mitigate reconnaissance attacks in industrial control systems. *Wireless Networks*, 1–15.

Germano da Silva, E., Dias Knob, L. A., Wickboldt, J. A., Gaspary, L. P., Granville, L. Z., & Schaeffer-Filho, A. (2015). Capitalizing on sdn-based scada systems: An anti-eavesdropping case-study. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 165–173.

Huang, Y. & Ghosh, A. K. (2011). Introducing diversity and uncertainty to create moving attack surfaces for web services. *Springer New York*, 131–151.

Iturbe, M., Garitano, I., Zurutuza, U., & Uribeetxeberria, R. (2016). Visualizing network flows and related anomalies in industrial networks using chord diagrams and whitelisting. In *VISIGRAPP (2: IVAPP)*, 101–108.

Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012). Openflow random host mutation: Transparent moving target defense using software defined networking. In *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, HotSDN '12, 127–132, New York, NY, USA. Association for Computing Machinery.

Kampanakis, P., Perros, H., & Beyene, T. (2014). Sdn-based solutions for moving target defense network protection. In *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, 1–6. IEEE.

Kanellopoulos, A. & Vamvoudakis, K. G. (2020). A moving target defense control framework for cyber-physical systems. *IEEE Transactions on Automatic Control*, 65(3):1029–1043.

Koo, H., Chen, Y., Lu, L., Kemerlis, V. P., & Polychronakis, M. (2018). Compiler-assisted code randomization. In *2018 IEEE Symposium on Security and Privacy (SP)*, 461–477.

Li, Y., Dai, R., & Zhang, J. (2014). Morphing communications of cyber-physical systems towards moving-target defense. In *2014 IEEE International Conference on Communications (ICC)*, 592–598.

Molina, E. & Jacob, E. (2018). Software-defined networking in cyber-physical systems: A survey. *Computers & Electrical Engineering*, 66:407–419.

Ndonda, G. K. & Sadre, R. (2017). A low-delay sdn-based countermeasure to eavesdropping attacks in industrial control systems. In *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 1–7.

netfilter.org project, T. (2023). Netfilter: Firewalling, nat and packet mangling for linux.

Pappa, A. C., Ashok, A., & Govindarasu, M. (2017). Moving target defense for securing smart grid communications: Architecture, implementation amp; evaluation. In *2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 1–5.

Sainz, M., Iturbe, M., Garitano, I., & Zurutuza, U. (2018). Software defined networking opportunities for intelligent security enhancement of industrial control systems. In Pérez García, H., Alfonso-Cendón, J., Sánchez González, L., Quintián, H., & Corchado, E., editors, *International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6–8, 2017, Proceeding*, 577–586, Cham. Springer International Publishing.

Sharma, D. P., Kim, D. S., Yoon, S., Lim, H., Cho, J.-H., & Moore, T. J. (2018). Frvm: Flexible random virtual ip multiplexing in software-defined networks. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 579–587.

Skowyra, R., Bauer, K., Dedhia, V., & Okhravi, H. (2016). Have no phear: Networks without identifiers. In *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, 3–14.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ics) security.

Taguinod, M., Doupé, A., Zhao, Z., & Ahn, G.-J. (2015). Toward a moving target defense for web applications. In *2015 IEEE International Conference on Information Reuse and Integration*, 510–517.

Ulrich, J., Drahos, J., & Govindarasu, M. (2017). A symmetric address translation approach for a network layer moving target defense to secure power grid networks. In *2017 Resilience Week (RWS)*, 163–169.

Wang, Y., Chen, Q., Yi, J., & Guo, J. (2017). U-tri: Unlinkability through random identifier for sdn network. In *Proceedings of the 2017 Workshop on Moving Target Defense*, MTD '17, 3–15, New York, NY, USA. Association for Computing Machinery.

Zheng, J. & Namin, A. S. (2019). A survey on the moving target defense strategies: An architectural perspective. *Journal of Computer Science and Technology*, 34(1):207–233.

Zhou, Y., Cheng, G., & Yu, S. (2021). An sdn-enabled proactive defense framework for ddos mitigation in iot networks. *IEEE Transactions on Information Forensics and Security*, 16:5366–5380.

6 Eskerrak eta oharrak

Eusko Jaurlaritzako Hezkuntza, Hizkuntza Politika eta Kultura Sailak (IT1676-22) laguntzen duen Sistema Industrialetarako Sistema Adimendunen taldeak garatu du lan hau. Lan hau Gipuzkoako Zientzia, Teknologia eta Berrikuntza Sarearen GAITZERDI Proiektuak finantzatu du partzialki (2022-CIEN-000065-01). Lan hau nazioarteko aldizkari baten artikulu bezala argitaratu zen (Etxezarreta et al., 2023).