Mongolian Journal of Engineering and Applied Sciences, 2022, 4–1

Мэдээллийн ажуулгүй байдал

Халдлага илрүүлэх хосолмол загварыг юмсын интернэтийн сүлжээнд ашиглах нь

Н.Уггахбаяр*, Б.Өсөхбаяр

Электроник холбооны инженерчлэлийн тэнхим, ХШУИС, МУИС

Received on 2022.04.30; Revised on 2022.05.13; Accepted on 2022.05.17

*44911.n@gmail.com

Хураангуй

Юмсын интернэтийн хэрэглээ, төрөл, үйлдвэрлэгчид сүүлийн жилүүдэд асар хурдацтай нэмэгдэж буйтай холбоотойгоор халдлагын тоо тодорхой хэмжээнд тасралтгүй нэмэгдэж буйг олон эх сурвалж дурьдаж байна. Үүнээс гадна энгийн хэрэглэгч болон үйлдвэрийн түвшинд ашиглагдаж буй энэхүү төхөөрөмжүүд нь ихэнх тохиолдолд интернэт сүлжээнд холбогдон ашиглагдаж байна. Иймээс халдлагын бай болох, хохирол учрах цар хүрээ нь уламжлалт сүлжээнээс дутахгүй өндөр байгаа юм. Ажуулгүй байдлын мэргэжилтнүүдийн хувьд халдлагыг судлан шинжлэх нь цаг хугацааны хувьд хязгаарлагдмал, шинээр гарах халдлагын төрөл олон болох бүрд улам хүндрэлтэй болж байна. Халдлагыг судлах, таньж илрүүлэх энэхүү хүндрэлтэй байдлыг тодорхой түвшинд эерэг үр дүнтэй даван туулахад гажигт суурилсан системүүд ашиглах нь үр дүнтэй гэдэг талаар олон судлаачдын бүтээлүүд байна. Гажигт суурилсан халдлага илрүүлэх системийг дангаар нь ашиглах нь тодорхой түвшний үр дүнтэй хэдий ч сигнатурт суурилсан халдлага илрүүлэх систем нь өндөр үр дүнтэй хэвээр байсаар байгаа тул эдгээрийг хослуулан хэрэглэх замаар халдлага илрүүлэх хосолмол систем бий болгох боломжтой гэж үзэн зэрэгцээ ажиллагаа бүхий загварыг энэхүү судалгааны ажлаар санал болгож байна.

Түлхүүр үг: ХИС-ийн хосолмол загвар, халдлага илрүүлэх систем, юмсын интернэт.

1 Удиртгал

Интернэт болон фог (fog) сүлжээний орчинд мэдээлэл дамжуулах зориулалт бүхий олон тооны мэдрүүр, хөдөлгөгч зэргээс тогтсон сүлжээ бүхий дэд бүтэц, системийн шийдэл нь юмсын интернэт юм. Ялгаатай байршилд байрлуулсан эдгээр төхөөрөмжүүд нь өгөгдлийг цуглуулах, барьж авах, дамжуулах, боловсруулах зэрэг олон төрлийн үйлдэл хийх боломжтой байдгаараа уламжлалт сүлжээтэй төстэй. Юмсын интернэт нь сүүлийн жилүүдэд бидний өдөр тутмын амьдралд тэдийгүй үйлдвэр, автоматжуулалт болон бусад салбарт хурдацтайгаар нэвтэрч байна. Энэхүү сүлжээнд ашиглагдаж буй ухаалаг мэдрэгч, хөдөлгөгч болон төхөөрөмжүүд нь тухайн орчны болон бизнесийн шаардлагаас хамаарч утастай болон утасгүй холболтыг ашиглах боломжтой. Утасгүй холболтын хувьд ажуулгүй байдлыг хангах нь чухал байдаг бөгөөд энэхүү холболтод ZigBee, Bluetooth Low Energy (BLE), Z-Wave, Low power Wireless PAN (6LoWPAN), NFC зэрэг олон протоколыг ашигладаг. Юмсын интернэтийн түгээмэл хэрэглээний нэг ухаалаг гэрийн шийдлүүд бөгөөд эдгээр шийдлийн хэрэгжүүлэлт нь гэрийн аливаа юмсыг автоматжуулах, тухайн автоматжуулсан юмсад орон зайн хязгаарлалтгүйгээр онлайн орчинд хандах боломжийг олгож байна [1]. Энэхүү технологийн шийдлийг хэрэгжүүлэхэд анхаарах чухал зүйлс нь хэрэглэгчид эвтэй, ажуулгүй, үнэ, өртөг бууруулсан байхад оршино [1]. [2]-д 2020 оны 6 сарын байдлаар эрүүл мэнд, аж үйлдвэр зэрэг хэд хэдэн салбарт ашиглагдаж буй 5 сая гаруй юмсын интернэтийн төхөөрөмжийн ажуулгүй байдлын шалгалтыг хийхэд 15% нь ямар нэг хамгаалалтгүй, 75% гаруй нь ямар нэг ажуулгүй байдлын зөрчилтэй гэж дүгнэжээ. Үүнтэй төстэй олон төрлийн судалгаа хийдгийн нэг нь Аваст компаний судалгаа бөгөөд үүнд ухаалаг гэрийн 5 төхөөрөмж тутмын 2 нь ямар нэг байдлаар халдлагад өртөх боломжтой, эмзэг байдалтай байна гэж үзжээ [3]. Үүнтэй уялдан ялгаатай, олон төрлийн шийдэл, мэдрүүр, хөдөлгөгч зэргийг зохион байгуулах, удирдахаас үүдэн ажуулгүй байдлын шинэ асуудлуудыг дагуулан бий болгож буйн нэг нь халдлагыг хурдан хугацаанд үр дүнтэй илрүүлэх, таслан зогсооход оршиж байна. Энэ чиглэлд цөөнгүй судалгаа, туршилт хийгдэж байгаа хэдий ч өнөөдрийн байдлаар зах зээлд борлуулагдаж буй юмсын интернэтийн фог сүлжээний орчны ажуулгүй байдлын асуудал дорвитой шийдэгдээгүй хэвээр байна. Үүний нэг шалтгаан нь Эрини болон бусад судлаачдын [4] өгүүлэлд дурьдсан юмсын интернэтийн сүлжээний орчинд, фог сүлжээний орчинд ашиглагдаж буй техник хангамжийн хүчин чадлаас хамаарч буй явдал юм. Үүнд тэжээ-

лийн эх үүсвэр дутмаг, санах ойн багтаамж бага, боловсруулах үйлдлийн тоо хязгаарлагдмал гэх мэт олон шалтгааныг дурьдаж болно. Сүүлийн арав орчим жилийн хугацаан дахь хэрэглээний болон зах зээлийн өсөлттэй уялдан юмсын интернэтийн аюулгүй байдлын шийдэл боловсруулах, аюулгүй байдлыг хангах талаар олон төрлийн судалгааны ажлууд хийгдсээр байна. Эдгээр судалгаанаас Фернандес болон бусад судлаачдын [5] өгүүлэлд юмсын интернэтийн сүлжээ болон уламжлалт сүлжээний орчин дахь аюулгүй байдлын шийдлүүдийн ялгаатай болон ижил төстэй байдлыг техник хангамж, програм хангамж болон протоколын түвшинд судалгаа хийсэн бөгөөд уламжлалт аюулгүй байдлын шийдэл нь үр нөлөө багатай гэсэн дүгнэлтэд хүрсэн байна. Энэхүү судалгааны үр дүнг боловсруулахад эдгээр системийн ашиглалтын ялгаатай байдал нөлөөлж буйг [6] нарын өгүүлэлд дурьдсан шифрлэлтийн аргачлалыг ашиглаж ялгаатай байдлаар тайлбарлаж болох юм. Өөрөөр хэлбэл уг өгүүлэлд дурьдсанаар юмсын интернэтийн мэдрүүр, хөдөлгөгч зэрэгт уламжлалт сүлжээтэй ижил нууцлалын алгоритм ашиглах нь тэжээлийн нөөц, боловсруулах хязгаар зэрэг олон зүйлд нөлөөлнө гэж үзэж буй юм. Үүнээс гадна Моханта болон бусад судлаачдын [7] ажилд юмсын интернэтийн өгөгдөл нь уламжлалт сүлжээнээс илүү олон төрлийн, олон талд мэдээлэл агуулж буй тул уламжлалт сүлжээнд ашиглаж буй машин сургалтын шийдлийг тодорхой хэмжээгээр өөрчлөн ашиглах нь зүйтэй гэсэн санааг дэвшүүлсэн байна. Дээрх судалгаанд үндэслэн уламжлалт сүлжээ болон юмсын интернэтийн сүлжээний хэрэглээ, протоколын ялгаатай байдлаас үүдэн гарах ялгаатай байдлыг арилгах замаар уламжлалт аюулгүй байдлын шийдлийг сайжруулах, юмсын интернэтийн сүлжээнд нийцүүлэн ашиглах боломжтой гэж үзэж байна. Юмсын интернэтийн хэрэглээтэй холбоотой zero-day халдлага улам бүр нэмэгдэж буй нь энэ төрлийн халдлага илрүүлэхэд автоматжуулалтын аливаа аргыг ашиглах нь илүү үр дүнтэй гэж үзэж байна. Учир нь уламжлалт сүлжээний хувьд төгсгөлийн төхөөрөмж болон дундын төхөөрөмжүүд нь пакет хүлээн авч боловсруулах боломжтой байдаг бол юмсын интернэтийн сүлжээний хувьд олон төрлийн мэдрэгч, хөдөлгөгчдийн үйл ажиллагаанаас шууд хамаардаг. Иймээс уламжлалт халдлага илрүүлэх системийг юмсын интернэтийн орчинд шууд ашиглах болон онцлогуудыг шинээр тохируулахгүйгээр ашиглах нь учир дутагдалтай болох юм. Юмсын интернэтийн сүлжээ нь мэдрэгч давхарга (perception layer), сүлжээний давхарга, хэрэглээний давхарга гэсэн үндсэн гурван хэсгээс бүрдэх бөгөөд уг судалгааны ажлын хувьд мэдрэгч давхаргад илрэх халдлагыг урьдчилан, бодит хугацаанд дөхөж танихыг зорьсон. Угтахбаяр нарын [8] судалгааны ажилд сигнатурт суурилсан болон гажигт суурилсан халдлага илрүүлэх системийг хослуулан ашиглах замаар уламжлалт сүлжээний орчинд халдлагыг хурдан, үр дүнтэй таних боломжтойг батлан харуулжээ. Сигнатурт суурилсан аргачлал нь zero-day халдлагыг судлан тухайн халдлагын онцлогыг агуулсан буюу тухайн халдлагыг таних боломжтой сигнатурыг үүсгэх замаар халдлагын мэдээлэл бүхий сигнатурын сан үүсгэж уг сантай урсгалын мэдээллийг тулгаснаар халдлагыг таньж илрүүлдэг [9]. Уг аргачлал нь гажигт суурилсан аргатай харьцуулахад илүү хурдан боловч юмсын интернэтийн орчин шиг шинэ, олон төрлийн халдлага бий болж буй нөхцөлд дангаараа төдийлөн үр дүнтэй биш ч бүрэн судлагдсан халдлагыг алдаагүй таних магадлал нь гажигт суурилсан системээс илүү юм. Гажигт суурилсан системийн хувьд тухайн илрүүлэх урсгалын шинж чанар, өгөгдлийн мэдээлэл, давтагдах байдал зэрэг хэд хэдэн мэдээллийг ашиглан боловсруулалт хийсний үр дүнд халдлага мөн эсэхийг тодорхойлдог [10]. Уг судалгааны ажлаар [8] өгүүлэлд танилцуулж байсан уламжлалт сүлжээний орчинд халдлага илрүүлэх хосолмол загварыг юмсын интернэтийн сүлжээнд ашигласан үр дүнг танилцуулана. Ингэж ашигласнаар zero-day халдлага болон судлагдсан, танигдсан халдлагыг зэрэг өндөр үр дүнтэй илрүүлэх боломжтой болох юм. Дээрх ажилд санал болгосон архитектурын сигнатурт суурилсан халдлага илрүүлэх системийн хувьд [11, 12] судалгааны ажлуудын үр дүнд үндэслэн пакетын алдагдал, RAM, CPU-ний ачаалал зэрэгт тулгуурлан Bro-IDS-ийг, Угтахбаяр нарын [13] өгүүллийн үр дүнд тулгуурлан гажигт суурилсан системийн алгоритмаар шийдвэрийн модыг сонгон ашигласан бөгөөд судалгааны ажил нь ... бүлэгтэй.

2 Судлагдсан байдал

Энэхүү хэсэгт юмсын интернэтийн орчинд халдлага илрүүлэхэд ашиглаж буй арга, аргачлалын ерөнхий судалгаа болон юмсын интернэтийн орчинд ашиглагдаж буй төвлөрсөн, хосолмол системүүдийн талаар орно. Юмсын интернэтийн орчинд хийгдэж буй халдлага илрүүлэх системийн судалгаа нь халдлага илрүүлэхэд ашиглаж буй аргачлалын хувьд сигнатурт суурилсан, гажигт суурилсан болон хосолмол; байрлуулж буй аргачлалын хувьд төвлөрсөн, тархсан болон хосолмол; үр дүнг хянан магадлаж буйн хувьд симуляцийн орчин ашигласан, оноолын судалгаа болон туршилт хийсэн гэж тус тус ангилж болохоор байна.

Юмсын интернэтийн орчинд аюулгүй байдлыг бууруулах, эрсдэлийг багасгах, халдлага илрүүлэх чиглэлд олон тооны судалгааны ажил хийгдэж байна. Эдгээрээс [11, 14, 15] зэрэг судалгааны ажлууд нь сигнатурт суурилсан Snort халдлага илрүүлэх систем ашиглан юмсын интернэтийн орчинд аюулгүй байдлыг хангахад чиглэсэн ажил байх бөгөөд тухайн системийн ажиллаж буй орчин, халдлагын төрөл зэргээс хамаарч халдлага илрүүлэхэд үзүүлж буй нөлөөг судласан байна. Киттихүн болон бу-

сад судлаачдын [11] ажилд уламжлалт сүлжээнд хамгийн түгээмэл ашиглагддаг Snort, Suricata, Bro гэсэн үндсэн гурван халдлага илрүүлэх системийн ачаалалтай холбоотой харьцуулсан судалгааг хийсэн байна. Уг ажлаар DoS, DNS, FTP, port scan, SNMP зэрэг халдлагуудыг ашигласан бөгөөд CPU-ний ачаалал, пакетын алдагдал, мэдэгдлийн тоо зэрэг үзүүлэлтийг харьцуулан судласан бөгөөд Bro IDS бусдаасаа сайн гэж гарсан бөгөөд энэхүү үр дүнд тулгуурлан сигнатурт суурилсан системээр Bro IDS-ийг сонгон авах нэг үзүүлэлт болсон. Бүзиани болон бусад судлаачдын [15] ажилд сүлжээний урсгалын ачаалал даах чадамжийн судалгааг хийж гүйцэтгэсэн бөгөөд тэдгээрийн давуу болон сул талуудыг харьцуулан гаргажээ. Уг ажлын хүрээнд Bro халдлага илрүүлэх систем нь пакетын алдагдалгүйгээр 1Gbps хүртэл урсгалын ачаалал даасан үр дүнг үзүүлсэн нь мөн уг системийг сонгох өөр нэг үзүүлэлт болсон.

Шихрэза болон бусад судлаачдын [16] ажилд гэрийн ухаалаг төхөөрөмжүүдээс урт болон богино хугацаанд цуглуулсан хэвийн бус нөхцөлүүдийг цуглуулан тэдгээрээс гажиг илрүүлэх судалгааг хийжээ. Уг судалгааны үр дүнд цөөн тооны төхөөрөмжтэй үед олон тооны буруу танилт үзүүлж буйг нотолсон ба халдлага, хэвийн бус байдлыг танихын тулд мэдрүүр, хөдөлгөгчийг олон тоогоор ашиглах нь зүйтэй гэж дүгнэжээ. Үүнээс гадна Гажевски болон бусад судлаачдын [17] судалгааны үр дүнгээр сүлжээний урсгалыг гадаад болон дотоод гэж ангилсны үр дүнд ялгаатай халдлагыг үр дүнтэй илрүүлэх боломжтойг нотолсон байна. Өөрөөр хэлбэл нэг ижил халдлага нь урсгалын тоо, холболтын тоо, сенсорын мэдээлэл зэрэг хэд хэдэн нөхцөл нь гадаад болон дотоод урсгалын хувьд ялгаатай байгааг тодорхойлсон энэхүү судалгааны ажилд тулгуурлан туршилтын өгөгдлийг ижил агуулгатай байхад анхааран судалгааны нэг шаардлага болгон ашиглалаа.

Амоур болон бусад судлаачдын [18] судалгаанд юмсын интернэтийн сүлжээнд халдлага илрүүлэх системийг машин сургалтын аргатай хослуулан ашиглаж болох талаар судалгаа хийсэн бөгөөд уг ажлыг гүйцэтгэхдээ сенсор бүрийн хэвийн гаралтыг цуглуулан тухайн гаралттай харьцуулах замаар гажиг бий эсэхийг тодорхойлсон бөгөөд гажиг бүрийг өндөр хувьтай таньж байсан сайн үр дүн үзүүлжээ. Уг ажлыг бүхэлд нь симуляцийн орчинд хийж гүйцэтгэсэн бөгөөд үүний дутагдалтай тал нь бодит орчинд гүйцэтгэх үед сенсорын тоо, төрөл олон болсноор гүйцэтгэлийн хурд, хувь буурах дутагдалтай хэмээн дүгнэжээ. Мөн Шүкла болон бусад судлаачдын [19] ажилд K-means болон шийдвэрийн модны аргуудыг халдлага илрүүлэхэд ашигласан бөгөөд уг ажлаар wormhole халдлага илрүүлэхээр ажилласан бөгөөд өндөр үр дүн үзүүлсэн. Уг судалгааны ажилд өөр төрлийн халдлага илрүүлэхээр ажиллаагүй нь дутагдалтай байна.

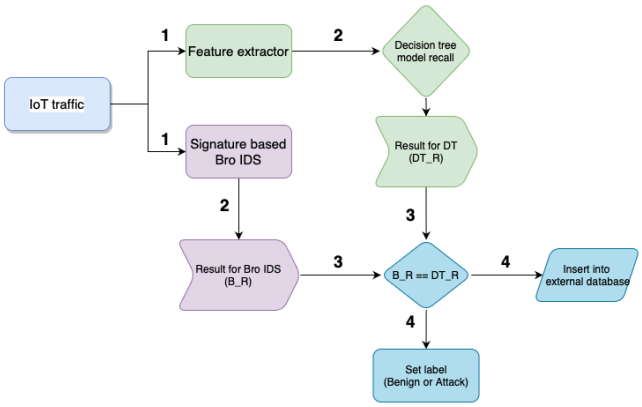
Лиао болон бусад судлаачдын [20] ажилд халдлага илрүүлэх хосолмол системийг виртуалчлалын орчинд туршсан бөгөөд Clam-AV антивирусны програм хангамж болон Snort халдлага илрүүлэх системийг хослуулан ашиглаж сигнатурын урт нэмэгдэхэд өндөр үр дүнтэй ажилласан байна. Эй-Ясын нарын [21] ажилд K-means алгоритмыг сайжруулан халдлага илрүүлэх хосолмол загвар боловсруулсан бөгөөд DoS, U2R, R2L халдлагыг 95.75%-ийн үр дүнтэй таньсан үр дүнг үзүүлжээ. Дээрх судалгааны ажлуудын давуу талуудыг зэрэгцээ, хосолсон загварт ашиглан судалгааны ажлаа гүйцэтгэв.

3 Судалгааны орчин

Юмсын интернэтийн орчинд халдлага илрүүлэх хосолмол системийг ашиглах нь танилтын хугацааг багасгах, халдлагыг өндөр үр дүнтэй таних зэрэг хэд хэдэн давуу талыг бий болгоно гэдэг нь өмнөх судалгааны ажлууд болон бусад судлаачдын судалгааны үр дүнд баталгаажиж байна. Бидний санал болгож буй уг арга нь [8] судалгааны ажилд санал болгосон гажигт суурилсан аргыг сигнатурт суурилсан аргатай зэрэгцээ байдлаар ашиглаж буй аргатай ижил бөгөөд уг аргыг юмсын интернэтийн орчинд ашиглахаар санал болгож буй шалтгаан нь тухайн арга нь уламжлалт сүлжээнд сайн үр дүн үзүүлсэн тул юмсын интернэтийн орчинд нийцүүлэн боловсруулав. Ингэснээр судлагдсан болон шинэ халдлагыг өндөр үр дүнтэй танина гэж үзэв. Уг ажлын гажигт суурилсан системийг боловсруулахдаа өмнөх [13] судалгааны ажлын үр дүнг ашигласан бөгөөд үүнд шийдвэрийн мод 98%-ийн танилт үзүүлсэн тул түүнийг ашиглахаар шийдэн шийдвэрийн модны C5.0 алгоритмыг суралцуулан ашигласан.

3.1 Санал болгож буй хосолмол загвар

Санал болгож буй халдлага илрүүлэх хосолмол системийг Зураг 1-д харуулсан байдлаар сигнатурт суурилсан болон гажигт суурилсан халдлага илрүүлэх системүүд зэрэгцээ байдлаар ажиллахаар зохион байгуулсан. Сигнатурт суурилсан халдлага илрүүлэх системээр ашиглахаар сонгосон Bro IDS нь урьд танигдсан халдлагын сигнатурын тусламжтайгаар халдлага илрүүлэх бөгөөд хэрвээ халдлагатай гэж үзвэл тухай бүрд байгууллагын сонгосон арга хэрэгсэлийг ашиглах боломжтой. Жишээ нь тухайн байгууллага админ эсвэл тодорхой албан тушаалтанд и-мэйл илгээхээр журамд заасан бол түүнийг хийх, халдлагыг зогсоохоор заасан бол халдлага зогсоох зэрэг боломжтой байхаар ашигласан. Хэдий дээрх үйлдлийг цаг тухай бүрд хийх боловч гажигт суурилсан системийн үр дүнтэй харьцуулах буюу зурагт үзүүлсэн 2 болон түүнээс хойшхи үйлдлийг үргэлжлүүлэн хийх юм. Өөрөөр хэлбэл өөрийн гаргасан үр дүнг B_R хувьсагчид хадгалан



Зураг 1: Санал болгож буй загвар

гажигт суурилсан системийн үр дүнтэй харьцуулах юм. Ингэснээр гажигт суурилсан халдлага илрүүлэх системийг тасралтгүй сайжруулах, суралцуулах боломжийг нэмж өгөх ба хэрвээ уг хоёр системийн хариу ижил буюу халдлага эсвэл энгийн гэж ижил утгатай танивал тухайн мэдээллийг цааш боловсруулахгүй зөвхөн үр дүнд ашиглах бөгөөд ялгаатай таньсан тохиолдолд администратор шинжилгээ хийх зориулалт бүхий санд (external database) хадгалах юм. Уг санд орж ирэх өгөгдлийг тухайн байгууллагын администратор эсвэл аюулгүй байдлын шинжээчид хянан магадлах замаар зөв шошгийг тавьж үр дүнг буруу боловсруулсан халдлага илрүүлэх системийг сайжруулах юм.

3.2 Туршилтын орчин

Энэхүү туршилтыг 3 дахь үеийн Intel i7 2.3GHz CPU, 8GB DDR4 RAM, 256GB SSD хатуу диск бүхий энгийн персонал компьютер дээр гүйцэтгэсэн бөгөөд үйлдлийн системээр Ubuntu-г сонгон ашигласан. Уг ажлыг гүйцэтгэхдээ бодит урсгалыг [13] ажилд ашигласан сан болон https://www.stratosphereips.org/datasets-iot23-д тавигдсан 8.8GB хэмжээтэй шошго бүхий урсгалын мэдээллийг ашигласан. Уг мэдээллийг ашиглахдаа энгийн урсгалтай ойролцоо байлгах зорилгоор 1000 урсгалын мэдээлэл ашигласан.

3.3 Туршилтад ашигласан сангийн боловсруулалт

Ажлын хувьд санг ямар нэг байдлаар урьдчилан боловсруулаагүй бөгөөд тухайн санд энгийн, Mirai, Toori, C&C, Okiru, DDoS гэсэн 6 ангиллын 2 төрлийн мэдээлэл агуулсан. Уг сангуудаас онцлог сонгоход мэдээллийн өсгөлтийн арга болон энтропи анализ хийсэн ба энэхүү туршилтыг Weka програм хангамжийг ашиглан боловсруулахдаа үндсэн утгыг ямар нэг байдлаар өөрчлөөгүй. Дараах хүснэгтэд ашигласан сангийн мэдээллийг Хүснэгт 1-д оруулав.

Хүснэгт 1: Туршилтад ашигласан сангийн онцлогууд

Онцлог	Тайлбар
s_time	Холболт эхлэсэн огноо
f_time	Холболт дууссан огноо
flags	Холболт, протоколын флагууд
flag_num	Холболт, протоколын флагын тоо
seq	Дараалал
d_port	Хүлээн авагчийн порт
s_port	Илгээгчийн порт
dura	Холболтын хугацаа
num_conn	Холболтын тоо

3.4 Туршилтын үр дүнг боловсруулах

Уг туршилтад гажигт суурилсан системийн машин сургах ажлыг Weka програм хангамжийн флов моделийн тусламжтайгаар үүсгэсэн бөгөөд үр дүн харьцуулах шийдлийг Н.Угтахбаяр нарын [8] ажлын Аргачлал бүлгийн D хэсэгт заасан алгоритмын шийдлийг шууд ашигласан бөгөөд тооцооллын хэмжүүрээр confusion матриц үүсгэсэн. Үүнийг үүсгэхдээ дараах утгуудыг ашигласан ба Хүснэгт 2-т заасаар боловсруулав. Үүнд:

True positive (TP) - Юмсын интернэтийн орчин дахь халдлагыг халдлага гэж зөв ангилсан тоо.

True negative (TN) - Юмсын интернэтийн орчин дахь хэвийн урсгалыг хэвийн урсгал гэж зөв ангилсан тоо.

False positive (FP) - Юмсын интернэтийн орчин дахь хэвийн урсгалыг халдлага гэж буруу ангилсан тоо.

False negative (FN) - Юмсын интернэтийн орчин дахь халдлагыг хэвийн урсгал гэж буруу ангилсан тоо.

Хүснэгт 2: Confusion матриц үүсгэх

	Халдлага гэсэн	Хэвийн гэсэн
Халдлага	TP	FN
Хэвийн	FP	TN

Танилтын нарийвчлалыг дараах томъёоллоор бодов.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

4 Үр дүн

Энэ хэсэгт бидний санал болгож буй загварын үр дүнг боловсруулан танилцуулна. Уг ажлыг гүйцэт-

гэхэд Хүснэгт 1-д заасан 9 онцлог шинжийг ашигласан бөгөөд шийдвэрийн модны машин сургахад нийт сангийн 20%-ийг ашигласан бөгөөд үр дүнг шалгахдаа сургасан хэсгийг оруулан нийт сангаар шалгасан. Хүснэгт 3-д гажигт суурилсан системийн туршилтын үр дүнг харуулж байна. Уг хүснэгтэд тэмдэглэсэн a нь хэвийн урсгалыг, b нь халдлагатай урсгалыг агуулна. Туршилтад ашигласан сангийн хувьд өмнө хэсэгт заасан болон [13] өгүүлэлд боловсруулсан сангуудын нийлбэр буюу энгийн 337 урсгал, халдлагатай 663 урсгалын мэдээллээс бүрдэнэ. Шийдвэрийн модны үр дүнд халдлага илрүүлэх нарийвчлал нь Accuracy = 0.978 буюу юмсын интернэтийн орчин дахь халдлага болон энгийн урсгалыг 97.8 хувийн нарийвчлалтай таньж байна. Халдлагын сигнатурыг Bro IDS-д тохируулан өгсний дараа туршилтын өгөгдлийг tcpreplay хэрэгсэлийн тусламжтайгаар оруулан халдлагыг танихад Хүснэгт 4-т үзүүлсэн үр дүнг харуулав. Хүснэгт 3,

Хүснэгт 3: Шийдвэрийн модны үр дүн - confusion матриц

	a	b
Хэвийн = a	332	5
Халдлага = b	16	617

Хүснэгт 4: Bro IDS-ийн үр дүн - confusion матриц

	a	b
Хэвийн = a	312	25
Халдлага = b	2	661

Хүснэгт 4-с үзэхэд сигнатурт суурилсан халдлага илрүүлэх систем нь урьдчилан танигдсан халдлагыг илүү нарийвчлалтай таниж буй бол шийдвэрийн модны машины хувьд энгийн урсгалыг халдлагаас илүү өндөр хувьтай таньж байна. Bro IDS-ийн үр дүнд халдлага илрүүлэх нарийвчлал нь Accuracy = 0.973 буюу юмсын интернэтийн орчин дахь халдлага болон энгийн урсгалыг 97.3 хувийн нарийвчлалтай таньж байна.

Хүснэгт 5-д шийдвэрийн санд орсон мэдээллийг нягталж үзэн confusion матрицийг байгуулж харуулав. Уг хүснэгтийг боловсруулахдаа a-аар DT_R-ийн халдлагыг халдлага гэж, энгийнийг энгийн гэж зөв таньсаныг b-ээр B_R-ийн халдлагыг халдлага гэж, энгийнийг энгийн гэж зөв таньсан нийлбэр тоог тус тус төлөөлүүлэн харуулав. Хүснэгт 5-с үзэхэд энэхүү туршилтын хувьд шийдвэрийн мод энгийн урсгалыг таних магадлал өндөр бол Bro IDS-ийн хувьд халдлагыг таних магадлал илүү өндөр байгаа нь харагдаж байна. Уг үр дүн нь бодит орчинд ашиглахад хангалттай сайн үр дүн биш боловч шийдвэрийн хүснэгтэд орсон мэдээллийн үр дүнг ашиглан сургалтын машин болон Bro IDS-ийг сайжруулах замаар тодорхой хугацааны дараа халдлагыг улам бүр сайжруулах боломжтой байна.

Хүснэгт 5: Шийдвэрийн сангийн үр дүн - confusion матриц

	a	b
a	21	17
b	19	22

Иймээс цаашид уг судалгааны ажлыг үргэлжлүүлэн хэд хэдэн удаагийн давталтын дараах үр дүнг боловсруулах, уг загварыг 2 шатлалт буюу зэрэгцээ болон цуваа хэлбэрээр ажиллах боломжтой болгон сайжруулах замаар машин сургалтаар энгийн гэж таньсан урсгалыг Bro IDS-д уншуулж үр дүнг шийдвэрийн санд оруулах, Bro IDS-ээр халдлагатай гэж үзсэн урсгалыг шийдвэрийн модны машинаар уншуулж үр дүнг шийдвэрийн санд оруулах замаар улам нарийвчлалтай болгох боломжтой гэж үзэж байна.

Дүгнэлт

Судлаачдын өмнөх судалгааны ажлаар сигнатурт суурилсан болон гажигт суурилсан халдлага илрүүлэх системүүдийг зэрэгцээ хэлбэрээр байрлуулан ашигласнаараа аль алиных нь давуу талуудыг этернэт сүлжээний орчинд халдлага илрүүлэхэд ашиглан халдлагыг өндөр хувьтай таньж байсан бол энэхүү судалгааны ажлын хүрээнд юмсын интернэтийн фог сүлжээний орчинд мөн адил халдлага таньж буй үр дүн сайн байгааг батлан харууллаа. Уг судалгааны үр дүнд фог сүлжээний орчинд ХИС-ийн хосолмол загвар нь халдлага таних танилтын хувь өндөр, харилцан дутагдалтай талуудаа нөхөж илүү үр дүнтэй ажиллах боломжтойг харууллаа. Шийдвэрийн модны аргачлалын хувьд Bro IDS-ээс 0.005%-иар илүү танилт үзүүлж байна. Үүнээс гадна уг хоёр системийн танилтын үр дүнд жингийн утга оруулах замаар танилтыг илүү нарийвчлан томъёолох боломжтой гэж үзэв. Цаашид уг системийг фог сүлжээний орчинд илүү нийцүүлэн боловсронгуй болгох замаар инновацийн шийдэл болгон хөгжүүлэх боломжтой юм.

Зохиогчийн оролцоо

Н.Угтахбаяр нь уг судалгааны ажлын санаа болон загварыг боловсруулж өмнөх судалгааны ажлын үр дүнг сайжруулах туршилтыг гүйцэтгэж өгүүллийг бичсэн. Б.Өсөхбаяр нь туршилт болон үр дүнгийн шинжилгээ хийж, өгүүллийг сайжруулах санааг тусган сайжруулав.

Санхүүжилт

Энэхүү судалгааны ажлыг МУИС-ийн Залуу судлаачдын багийн P2018-3630 дугаартай грантын сан-

хүүжилтээр хийж гүйцэтгэв.

Ашиг сонирхлын зөрчилгүйн баталгаа

Зохиогчид нь энэхүү судалгааны ажлаа гүйцэтгэхдээ санхүүжүүлэгч болон аливаа байгууллага, хувь хүнтэй ямар нэгэн ашиг сонирхлын зөрчилгүйгээр гүйцэтгэсэн болно.

Ашигласан ном

[1] Tom Hargreaves RHB Charlie Wilson. Learning to live in a smart home. Building research information. 2018;46.

[2] IOT security issues in 2022: A business perspective; 2021. Available from: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats.

[3] PR A. List of available regions. Avast; 2019. Available from: https://press.avast.com/en-us/two-out-of-five-digital-households-worldwide-at-cyber-risk-avast-reveals.

[4] Anthi E, Williams L, Słowińska M, Theodorakopoulos G, Burnap P. A Supervised Intrusion Detection System for Smart Home IoT Devices. IEEE Internet of Things Journal. 2019;6(5):9042-53.

[5] Fernandes E, Rahmati A, Eykholt K, Prakash A. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? IEEE Security Privacy. 2017;15(4):79-84.

[6] Sumit Singh Dhanda PJ Brahmjit Singh. Lightweight Cryptography: A Solution to Secure IoT. Wireless Personal Communications: An International Journal. 2020;112:1947-80.

[7] Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things. 2020;11:100227.

[8] Угтахбаяр, Өсөхбаяр, Нямжав, Байгалтөгс. Халдлага илрүүлэх системийн хосолмол загварын судалгаа. Монголын мэдээллийн технологи 2017. 2017;1:86-90.

[9] Pathan ASK. The state of the art in intrusion prevention and detection. Auerbach publications; 2014.

[10] M Naga Surya Lakshmi DYR. A complete study on intrusion detection using data mining techniques. IJCEA. 2015;9.

[11] Thongkanchorn K, Ngamsuriyaroj S, Visoottiviseth V. Evaluation studies of three intrusion detection systems under various attacks and rule sets. In: 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013); 2013. p. 1-4.

[12] Luthuli W, Oki O, Tarwireyi P, Adigun M. Evaluating the Effects of Hardware Configurations on Bro under DDoS Attacks. In: 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC); 2018. p. 1-6.

[13] Угтахбаяр, Болд, Өсөхбаяр. Юмсын интернэтийн хөдөлгөгчид чиглэсэн халдлагыг машин сургалтын алгоритм ашиглан илрүүлэх нь. Mongolian Journal of Engineering and Applied Sciences. 2021 Nov;2(1):27–32.

[14] Alhomoud A, Munir R, Disso JP, Awan I, Al-Dhelaan A. Performance Evaluation Study of Intrusion Detection Systems. Procedia Computer Science. 2011;5:173-80. The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT-2011) / The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011).

[15] Bouziani O, Benaboud H, Chamkar AS, Lazaar S. A Comparative Study of Open Source IDSs According to Their Ability to Detect Attacks. NISS19. New York, NY, USA: Association for Computing Machinery; 2019. Available from: https://doi.org/10.1145/3320326.3320383.

[16] Lotfi Shahreza M, Moazzami D, Moshiri B, Delavar MR. Anomaly detection using a self-organizing map and particle swarm optimization. Scientia Iranica. 2011;18(6):1460-8.

[17] Gajewski M, Mongay Batalla J, Levi A, Togay C, Mavromoustakis CX, Mastorakis G. Two-tier anomaly detection based on traffic profiling of the home automation system. Computer Networks. 2019;158:46-60.

[18] Amouri A, Alaparthy VT, Morgera SD. Cross layer-based intrusion detection based on network behavior for IoT. In: 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON); 2018. p. 1-4.

[19] Shukla P. ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. In: 2017 Intelligent Systems Conference (IntelliSys); 2017. p. 234-40.

[20] Liao HJ, Richard Lin CH, Lin YC, Tung KY. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications. 2013;36(1):16-24.

[21] Al-Yaseen WL, Othman ZA, Nazri MZA. Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. Expert Systems with Applications. 2017;67:296-303.