Сүлжээний хөнөөлт урсгалыг илрүүлэх системийн загварчлал

Н.Угтахбаяр
Электроник, Холбооны Инженерчлэлийн Тэнхим
Монгол Улсын Их Сургууль
44911.n@gmail.com

Б.Өсөхбаяр
Электроник, Холбооны Инженерчлэлийн Тэнхим
Монгол Улсын Их Сургууль

***Хураангуй*— Хэрэглэгчид орон зай, цаг хугацаанаас үл хамааран хүссэн мэдээллээ авахыг эрмэлздэг болсонтой холбоотойгоор бизнес эрхлэгчид, төрийн байгууллага, боловсролын байгууллагууд хэрэглэгчийн шаардлагыг хангах бүтээгдэхүүн үйлдвэрлэхийг илүүд үзэх болсон. Сүүлийн жилүүдэд хэрэглэгчийн шаардлагад улам бүр ойртохын тулд BYOD, IoT зэрэг шинэ технологиуд асар хурдацтай хэрэглээнд нэвтэрч байна. Үүнээс үүдэн интернэт хэрэглэгчийн тоо өсөж байгаа бөгөөд тэр хэмжээгээр халдлагын тоо хэмжээ ч мөн адил нэмэгдэж шинж чанар нь өөрчлөгдөж байна. Иймд сүлжээгээр дамжиж буй мэдээллийн аюулгүй байдлыг хангах шаардлага улам бүр нэмэгдэж байгаа хэдий ч галт хана, хандалт удирдлагын жагсаалт гэх мэт одоогийн байдлаар хамгийн түгээмэл ашиглагдаж байгаа технологийн хүчин чадал хүрэлцэхгүй байгаа тул халдлага илрүүлэх системийг сайжруулах, хэрэглээнд түлхүү хэрэглэх шаардлага улам бүр нэмэгдсээр байгаа юм. Энэхүү судалгааны ажлын хүрээнд халдлага илрүүлэх системийг үр дүнтэйгээр ашиглах боломжийг бий болгох загвар гаргахыг зорин ажиллалаа. Уг ажлаар Bro халдлага илрүүлэх системийг өөрсдийн зохиосон сурдаг машинтай харьцуулах замаар илүү сайн сурдаг машин зохиохыг зорьлоо.**

Keywords—сурдаг машин, халдлага илрүүлэх систем, өгөгдөл олборлох, халдлага илрүүлэх

I. Удиртгал

Интернэт сүлжээ ашигладаггүй салбар байхгүй болсонтой холбоотойгоор сүлжээний аюулгүй байдлыг хангах нь аюулгүй байдлын салбарт чухал асуудал болоод байна. Засгийн газар, бизнес, боловсролын байгууллага гэх мэт бүхий л байгууллагууд интернэтээс тодорхой хэмжээгээр хамааралтай болсонтой холбогдуулан их хэмжээний өгөгдөл интернэт орчинд хадгалагдаж, дамжуулагдаж, боловсруулагдаж байна. Шинэ төрлийн халдлагууд нь өмнөх халдлагаас тодорхой шинж чанаруудаар өөрчлөгдөж байгаа болохоор галт хана болон бусад аюулгүй байдлын системүүд болох антивирус, антималвэйр гэх мэт сигнартурт суурилсан аргачлалууд илрүүлж чадахгүй хугацаа алдах тохиолдол маш их гарсаар байна. Иймд илүү боловсронгуй, уян хатан ажиллагаатай халдлага илрүүлэх систем бүтээх нь судлаачдын хувьд чухал асуудал байсаар байна. Сүүлийн жилүүдэд Сони зурагчлал, Таргет, Майнкрафт [17][18] зэрэг томоохон байгууллагууд халдлагад ихээр өртөж байгаа нь цахим аюулгүй байдлыг хангахад өнөөгийн түвшинд хүнд байгааг харуулж байна. Цискогийн 2013 оны тайланд “Гадаад IP урсгалын хэмжээ асар хурдацтай нэмэгдэж байгаа бөгөөд 2019 онд 24 тэрбум төхөөрөмж интернэт холболттой болж 120.6 эксабайт урсгал сар бүр сүлжээгээр дамжигдах болно” [1] гэжээ. Халдлага илрүүлэх систем нь компьютер, сүлжээнд хийгдэж буй үйл ажиллагаанд анализ хийх замаар халдлага мөн эсэхийг тодорхойлдог систем юм [2][4]. Халдлага илрүүлэх системийн талаарх анхны судалгааг 1980 онд гарсан “Компьтерийн аюулгүй байдлын хяналт, ажиглалт” нэртэй урсгалд анализ хийдэг систем гэж үзэж болно. Халдлага илрүүлэх системийг үндсэн хоёр хэсэгт ангилж үздэг: сигнатурт суурилсан, гажигт суурилсан. Сигнатурт суурилсан халдлага илрүүлэх систем нь халдлагыг урьдчилан судлаж түүний онцлогт таарсан дүрэм бичих замаар илрүүлдэг бөгөөд зөвхөн судлагдсан халдлагыг илрүүлэх боломжтой, шинэ эсвэл өмнөхөөсөө бага зэрэг өөрчлөгдсөн халдлагыг илрүүлэх боломжгүй сул талтай [3]. Харин гажигт суурилсан халдлага илрүүлэх систем нь халдлагад анализ хийх замаар илрүүлдэг бөгөөд халдлагын шинж чанар, ажиллагаа, ашиглаж буй өгөгдөл зэрэг олон зүйл дээр шинжилгээ хийх замаар илрүүлэх боломжтой систем юм. Уг системийн хувьд гажигийн тухай мэдээлэл буюу загвар систем сайн байх тусам шинэ төрлийн халдлагыг илрүүлэх боломж нь өндөр байдаг [5]. Гажигт суурилсан халдлага илрүүлэх системийн хувьд удирдамжтай (supervised), удирдамжгүй (unsupervised) аргачлалуудын аль нэгийг эсвэл хослуулан ашиглах боломжтой байдаг. Интернэт сүлжээ хэрэглэгчдийн тоо өсөхийн хирээр сүлжээний урсгал асар хурдацтайгаар өсөж байгаа тухай бид ярилцсан тэгвэл үүнтэй зэрэгцэн сүлжээнд суурилсан халдлага илрүүлэх системийн боловсруулалтын хурдыг багасгах найдвартай ажиллагааг сайжруулах шаардлага бий болж байна.

Энэхүү судалгааны ажлын хүрээнд өгөгдөл боловсруулалтын аргыг ашиглан халдлага илрүүлэх системийн танилтын хурд, танилтын хувийг сайжруулах боломжын талаарх судалгааг хийж гүйцэтгэлээ. Уг судалгаанд ихэнх судлаачдын ашигладаг KDD 99 нээлттэй эхийн санг ашигласан бөгөөд уг сан нь тэмдэглэл бүхий сангийн хамгийн түгээмэл ашиглагддаг загвар юм. Уг сангийн сургалтын хэсэг нь 5 сая халдлагатай, халдлагагүй холболтын мэдээллийг агуулсан хүчирхэг сан юм [6]. Боловсруулалтын хурдыг багасгахын тулд туршилтын сан дээр Markov blanket, шугаман корреляцийн аргуудыг ашиглан онцлог ялгах ажлыг хийж гүйцэтгэсэн бөгөөд үүнээс гарсан онцлогуудыг KDD 99 сан болон өөрсдийн

цуглуулсан урсгалын мэдээллийг ашиглан J48, Naïve Bayes ангиллын алгоритмуудаар ангилж туршилтын үр дүнг харьцуулж танилт хийх хугацааг бодож гаргасан. Бидний туршилтын үр дүнд халдлага илрүүлэх танилтын хувь 75 хүрч өссөн бол таних хугацаа ойролцоогоор 20 хувиар буурсан.

II. Судлагдсан байдал

Сүүлийн 10 орчим жилийн хугацаанд аюулгүй байдлын чиглэлээр судалгаа хийдэг маш олон судлаачид энэхүү салбарыг сонирхон судласаар иржээ. Энэхүү хугацаанд аюулгүй байдал, сүлжээний хөнөөлт урсгалыг илрүүлэх, халдлага илрүүлэх системд өгөгдөл олборлох аргыг ашиглах зэрэг сэдвүүдтэй холбоотой олон тооны судалгаа шинжилгээний ажлуудыг судлаачид хэвлүүлсэн байна. Уг судалгаануудын үр дүнгээс харахад халдлага илрүүлэх системд өгөгдөл олборлох, машин сургалтын аргуудыг ашиглах нь үр дүнтэй болохыг харуулж байна. Моради болон бусад судлаачдын [8] хийсэн судалгаагаар халдлага илрүүлэх системд өгөгдөл олборлох аргыг ашиглах нь маш үр дүнтэй боловч халдлага таних боловсруулалтын хугацаа нь сигнатурт суурилсан аргаас удаан байгаа талаар дурджээ. Харин [9] судалгаанд онцлог ялгаснаар халдлага илрүүлэх системийн ажиллагааг хурдасгах боломж байгаа талаар дурдсан бөгөөд судлаачид онцлог ялгахдаа санамсаргүй үргэлжлэх алгоритмыг ашиглажээ. [11] энэхүү өгүүлэл нь халдлага илрүүлэхэд мэдрэлийн (neural) сүлжээ ашиглах талаар хийгдсэн хамгийн сайн ажил гэж болох бөгөөд олон газар ишлэгддэг. Уг ажлын хүрээнд халдлага илрүүлэх системд мэдрэлийн сүлжээ ашиглах давуу болон дутагдалтай талуудыг гарган судласан бөгөөд үр дүн нь давуу тал олонтойг илэрхийлдэг. Мөн [12][13][14] судалгаануудын хувьд нэг төрлийн халдлагыг сонгон авч түүнийг илрүүлэх аргачлалыг боловсруулах нь илүү үр дүнтэй болон KDD 99 санд J48 ангиллын алгоритм ашиглах, сүлжээний бодит урсгалаас онцлог ялгах, зэрэг ажлуудыг хийж гүйцэтгэсэн байна. Эдгээр судлаачид болон бусад судлаачдын ажлаас үзэхэд бүгд гажиг шинжийг илүү үр дүнтэй илрүүлэх аргачлалыг боловсруулахыг зорьж туршилтын орчинд тодорхой үр дүнд хүрсэн байна. Гэвч бодит сүлжээний орчинд тухайн туршилт нь үр дүн багатай болох мөн туршилтаар батлагдсан утга өөрчлөгдөх зэрэг дутагдалтай талууд байсаар л байна.

III. Санал болгож буй загвар

Гажигт суурилсан халдлага илрүүлэх системийн хувьд удирдамжтай, удирдамжгүй аргуудыг хослуулан ашигласан судалгааны ажлууд сүүлийн жилүүдэд нэмэгдэх болсон. Гэвч аль ч салбарт судалгаанд ашиглаад үр дүнтэй байсан алгоритмуудын эхний байруудад Naïve Bayes, K Means, SVM, J48 аргууд орж байна [2][4][6][20][11][21][22]. Өнөөгийн байдлаар ихэнх халдлагууд тохиолдсоны дараа илрүүлэх үйл ажиллагаа хийгдэж байгаа бөгөөд бидний энэхүү санал болгож буй загварын хувьд халдлагыг урьдчилан таних, хийгдэж буй үед таслан зогсоох боломжийг бий болгох юм. Энэхүү аргачлал нь хамгийн түгээмэл ашиглагддаг Bro халдлага илрүүлэх системтэй хамтран ажилласнаар илүү үр дүнтэй болно.

Бидний санал болгож буй аргачлалын ерөнхий загварыг график 1-д харууллаа. Уг аргын хувьд Markov blanket, шугаман коррелиацын тусламжтайгаар судалгааны орчинд гаргаж авсан онцлогуудыг ашиглан J48, Naïve bayes ангиллын алгоритмуудыг ашиглаж үр дүнг харьцуулан судлаж байгаа бөгөөд Bro-ийн үр дүн болон өөрсдийн сурдаг машины үр дүнгүүдийг харьцуулж зөрүүтэй тохиолдолд систем аналист ангилан дахин сургах боломжтой сан үүсгэх түүнийг зөв ангилсаны дараа дахин сургах замаар сайжруулах гэсэн үндсэн ажиллагааны зарчимтай юм. Өөрөөр хэлбэл энэхүү аргачлалаар үр дүнд нөлөөлж буй эсвэл буруу танигдаж байгаа халдлагуудыг ангилж дахин сургах замаар үр дүнг сайжруулах гэж ойлгож болох юм.

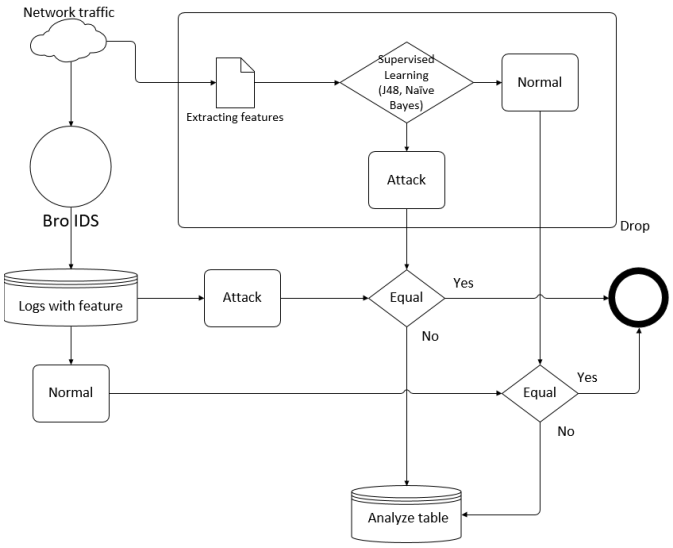


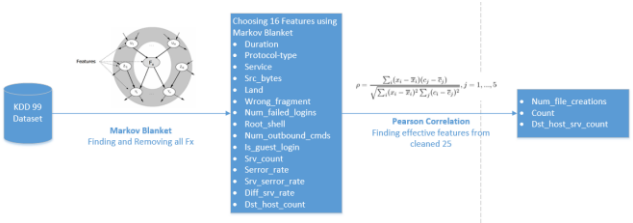
График 1. Санал болгож буй загвар

Бидний санал болгож буй загварын хувьд тархсан бүтэцтэй загвар гэж хэлж болно. Учир нь Bro системийг сүлжээний өгөгдөл цуглуулах, халдлага илрүүлэх зорилгоор сүлжээнд мэдрүүр хэлбэрээр байрлуулсан бөгөөд мэдрүүрийн тоо олон байх боломжтой юм. Уг загварын хувьд үндсэн 2 хэсгээс бүрдсэн бөгөөд эхний хэсэгт өгөгдөл цуглуулах, сан үүсгэх зорилгоор мэдрүүр ажиллуулах бол дараагийн хэсэгт KDD 99 санг ашиглан сургасан машинаар орж ирж буй урсгалыг халдлагатай, энгийн гэж ангилах юм. Уг хоёр хэсгийн үр дүнг харьцуулах замаар халдлагын санг бүрдүүлж уг санг дахин сургах замаар шинэ халдлагыг таних сургалтын хэсгийг сайжруулах юм. Бид туршилтаа хийхдээ KDD 99 санг ашиглан машинаа сургасан бөгөөд уг үйлдлийг Weka сургалтын програм дээр хийсэн. Сургасан машиныг экспортлож танилтын машиныг програмчилсан. Танилтын машины оролтонд өгөх зорилгоор сүлжээний өгөгдлөөс онцлог ялгах ажлыг libpcap, tcpdump нээлттэй эхийн програмын гаралтаар шийдсэн. Мэдрүүрийг 2nd үеийн Intel Atom Dual Core процессор, 2 Гбайт санах ой, 128 Гбайт SSD хатуу диск бүхий машин дээр тохируулсан бол сургалтын машиныг Intel i5-3400 2.4 GHz процессор, 16

Гбайт санах ой, энгийн сата диск бүхий машин дээр хийж гүйцэтгэсэн. Халдлагын танилтыг илүү сайжруулах зорилгоор Backtrack систем ашиглан 2012 оноос хойш гарсан зарим төрлийн эксплойт халдлагыг хийж онцлог ялгаж машинд сургасан. Машин сургахад KDD 99 сангийн 41 онцлогоос [23] сонгож авсан онцлогуудыг ашигласан бөгөөд туршилтанд мөн адил онцлогуудыг ашигласан.

IV. Туршилтын үр дүн

Уг судалгааны ажлын хүрээнд машин сургах эхний өгөгдөлд 100 % KDD 99 training санг ашигласан бөгөөд уг ажлыг Weka програм хангамжийн тусламжтайгаар хийж гүйцэтгэсэн. Уг програм хангамж нь сургасан машиныг экспортолж ашиглах боломжтой байдаг давуу талтай. Судалгааны ажлын эхний хэсэг болох онцлог ялгах хэсэгт Markov Blanket алгоритмын [15][16] тусламжтайгаар 16 онцлог шинж ялгаж авсан бөгөөд үүнд: “duration, protocol-type, service, src_bytes, land, wrong-fragment, num_failed logins, root_shell, num_file_creations, num_outbound_cmds, is_guest_login, srv_count, serror_rate, srv_serror_rate, diff_srv_error, dst_host_count” орно. Энэхүү онцлогуудын тусламжтайгаар сургасан машин төдийлөн бусад судлаачдын үр дүнд хүрэхгүй байсан тул үлдсэн онцлогуудаас шугаман корреляцийн аргыг ашиглаж онцлог ялгаж өмнөх онцлогтой нийлүүлж туршилтаа хийж гүйцэтгэсэн. Энэхүү туршилтын явцад “num_file_creations, count, dst_host_srv_count” гэсэн 3 онцлог нэмэгдэж нийт 19 онцлог шинжийг ашиглаж машинаа сургасан. Онцлог ялгах диаграмыг зураг 1–д үзүүллээ.



Зураг 1 Онцлог ялгах дараалал

Уг 19 онцлогын тусламжтайгаар туршилтын үр дүнг сайжруулсан бөгөөд буруу танилтын хувь тодорхой хэмжээгээр буурсан.

Хамгийн эхний туршилтаар KDD 99 сангийн туршилтын хэсгийг ашигласан бөгөөд шинэ халдлагыг таних танилтын хувь DoS, probe, R2L, U2R байхаас шалтгаалан 60 – 65 хувийн хооронд байсан. Үүний дараа 50 шинэ халдлагыг хийж дахин сургах (analyze table) санд байгаа өгөгдлийг өөрсдөө ангилж сургах машинаар дахин сургаж туршилтанд KDD 99 тестийн сан болон цуглуулсан өгөгдлийн 30 хувиас хэтрэхгүй байдлаар санамсаргүй сонгож авч ашигласан. Үүний үр дүнд халдлагыг 73 - 75 хувийн нарийвчлалтайгаар таньж чадсан бөгөөд туршилтын үр дүнг хүснэгт 1, 2–д харуулласа. Онцлогын тоог цөөрүүлсэн буюу 19 онцлогтой үед 41 онцлог ашиглан халдлага илрүүлэх дундаж хугацаанаас 18-21 хувийн хооронд халдлагын төрлөөс хамаарч буурч байсан.

Халдлагын төрөл	**J-48**		**Naïve Bayes**	
	Сонгогдсон онцлог	**Нийт онцлог**	**Сонгогдсон онцлог**	**Нийт онцлог**
Хэвийн	76.4%	77.8%	56.1%	60.2%
Probe	89.2%	83%	93.6%	84.7%
DoS	98.2%	95.6%	95.1%	92%
U2R	45.7%	48.2%	33.2%	35.1$
R2L	66.3%	60.2%	90.4%	79.6%
Нийт дундаж	**75.2%**	73%	**73.6%**	70.3%

Хүснэгт 1 ялгасан болон нийт онцлог шинжүүдийг ашиглан халдлагыг таньсан нарийвчлал

Энэхүү ажлаас харахад тухайн халдлагыг илрүүлэх боломжтой зөв онцлог шинжийг ялгасан үед халдлага таних хугацааг богиносгохоос гадна танилтын хувь, чанарыг сайжруулж байна. Мөн алгоритмуудын хувьд халдлага бүрийг танихдаа харилцан адилгүй байгаа нь ажиглагдаж байна. Жишээ нь хүснэгт 1-д үзүүлсэнээр DoS төрлийн халдлагыг J-48 өндөр хувьтай таньж байхад R2L төрлийн халдлагыг Naïve Bayes илүү өндөр хувьтай таньж байна.

Дүгнэлт болон Цаашид хийх ажил

Уг судалгааны ажлын хүрээнд бид халдлага илрүүлэх системийг дахин сургаж илүү сайжруулах боломжтой загварыг танилцууллаа. Уг загварыг ашиглан 2 дахь удаагийн сургалтын үр дүнд шинэ халдлагыг 73 - 75 хувийн танилт бүхий сургалтын машин бэлдэж чадлаа. Цаашид энэхүү аргыг дахин дахин ашиглах замаар танилтыг илүү сайжруулах боломжтой гэж үзэж байна. Мөн ангиллын алгоритм бүр халдлагыг таних танилтын хувьд ялгаатай байгаа нь туршилтын үр дүнд ажиглагдлаа. Иймд халдлага бүрээр онцлог ялгаж ялгаатай алгоритмууд ашиглах нь илүү үр дүнтэй байж болох юм гэсэн дүгнэлтэд хүрч байна. Энэхүү судалгааг үргэлжлүүлэн уг дүгнэлтээ бататгахын тулд цаашид үндсэн 4 төрлийн халдлага бүрээр онцлог шинж ялгасан үеийн халдлага илрүүлэх хугацааг илүү нарийвчлан гаргаж түгээмэл ашиглагддаг алгоритм бүрээр харьцуулан танилтын хувийг тооцох ажлыг хийж гүйцэтгэнэ. Үүнээс гадна өөсдийн системээр их хэмжээний урсгалыг дамжуулах замаар пакетын алдагдалыг тооцох ажлыг хийж гүйцэтгэнэ.

Ашигласан материалын жагсаалт

[1] Cisco, *“Cisco Visual Networking Index: Forecast and Methodology”*, 2012-2017, Cisco, 2013.

[2] Guide to Intrusion Detection and Prevention Systems (IDPS), *“Recommendations of the National Institute of Standards and Technology”*, Technology Administration U.S. Department of Commerce. NIST Special Publication 800-94.

[3] A. K. Pathan, “*The State of the Art in Intrusion Prevention and Detection”,* CRC Press, 2014.

[4] Li Hanguang, Ni Yu, “*Intrusion Detection Technology Research Based on Apriori Algorithm”,* 2012 International Conference on Applied Physics and Industrial Engineering, Physics Procedia 24 (2012) 1615 – 1620

[5] M.Naga Surya Lakshmi, Dr. Y. Radhika *"A complete study on intrusion detection using data mining techniques"* Volume IX, IJCEA Issue VI, June 2015

[6] Miroslav Stampar *"Artificial Intelligence in Network Intrusion Detection"*

[7] Senthilnayaki Balakrishnan, Venkatalakshmi K, Kannan A *"Intrusion detection system using Feature selection and Classification technique"* IJCSA Volume 3, Issue 4, pp. 144-151, 2014

[8] Moradi M and Zulkernine M *"A Neural Network based System for Intrusion Detection and Classification of Attacks"*, Proceedings of IEEE International Conference on Advances in Intelligent Systems – Theory and Applications, Luxembourg, Vol. 148, pp. 1-6, 2004.

[9] Wang Jianping, Chen Min and Wu Xianwen, *"A Novel Network Attack Audit System based on Multi-Agent Technology"*, Physics Procedia, Elsevier, Vol. 25, pp. 2152 – 2157, 2012.

[10] J.Li, Y.Liu and L.Gu *"DDoS attack detection based on neural network"*: Proceedings of the 2nd International Symposium on Aware Computing (ISAC), Tainan, 1–4 Nov.2010, pp.196–199.

[11] James Cannady. *"Artificial neural networks for misuse detection"*. In Proceedings of the 1998 National Information Systems Security Conference (NISSC'98) October 5-8 1998. *Arlington, VA.*, pages 443–456, 1998.

[12] B.B. Gupta, C.Joshi and M.Misra *"ANN based scheme to predict number of zombies in a DDoS attack"*, International Journal of Network Security. 13(3)(2011)216–225.

[13] T. Shon and J. Moon, *"A hybrid machine learning approach to network anomaly detection,"* Inf. Sci., vol. 177, no. 18, pp. 3799–3821, Sep. 2007.

[14] R. Jain and N. Abouzakhar, *"A comparative study of hidden markov model and support vector machine in anomaly intrusion detection,"* Journal of Internet Technology and Secured Transactions (JITST), vol. 2, no. 1/2/3/4, pp. 176–184, 2013.

[15] Cho S-B, Park H-J, *"Efficient anomaly detection by modeling privilege flows with hidden Markov model."* Computers and Security, 22(1), pp. 45-55, 2003.

[16] Tsamardinos I, Aliferis CF, Statnikov A, *"Time and sample efficient discovery of Markov blankets and direct causal relations."* 9th ACM SIGKDD international conference on knowledge discovery and data mining, ACM press, pp. 673-678, 2003.

[17] T.Gara, C.Warzel "Credit card breach at home depot" http://www.buzzfeed.com/tomgara/sony-hack

[18] A.Hernandez "Minecraft data breach affects users" http://techaeris.com/2015/01/20/reports-minecraft-data-breach-affects-users

[19] Anderson.J.P "Computer security threat monitoring and surveillance" Fort Washington, 1980

[20] М.Золжаргал, Н.Оюундарь, Ч.Алтангэрэл, Г.Белла "Монгол хэлний нэрлэсэн нэгж таниур – машин сургалтын аргаар", ММТ 2015. pp 21-24. 2015

[21] Н.Угтахбаяр, Ш.Содбилэг, Б.Өсөхбаяр, Ж.Нямжав "Хиймэл оюуны түүл ашиглан ТСП урсгалыг шинжлэх" Хүрэл тогоот 2014.

[22] Ugtakhbayar.N, Usukhbayar.B, Sodbileg.Sh and Nyamjav.J "Detecting TCP based attacks using Data mining algorihtms", ECBA'16 International Conference in HongKong, 2016

[23] H.Gunes Kayacik, A.Nur Zincir-Heywood, Malcom I.Heywood "Selecting features for intrusion detection: A feature relevance analysis on KDD 99 Intrusion detection datasets", Proceedings of the 3rd annual conference on Privacy, Security and Trust (PST-2015), 2015