Mongolian Journal of Engineering and Applied Sciences, 2020, 2 (542), 27-32

ЮМСЫН ИНТЕРНЭТИЙН ХӨДӨЛГӨГЧИД ЧИГЛЭСЭН ХАЛДЛАГЫГ МАШИН СУРГАЛТЫН АЛГОРИТМ АШИГЛАН ИЛРҮҮЛЭХ НЬ

Н.Угтахбаяр*, П.Болд, Б.Өсөхбаяр**

Электроник холбооны инженерчлэлийн тэнхим, Монгол Улсын Их Сургууль

Received on 2020.11.29; revised on 2020.12.16; accepted on 2020.12.25
Холбоо баригч зохиогч: 44911.n@gmail.com, usukhbayar@num.edu.mn

Хураангуй

Юмсын интернэтийн төхөөрөмжийн хэрэглээ асар хурдацтай нэмэгдэх хирээр тухайн төхөөрөмжид чиглэсэн халдлагууд мөн адил өсөж байна. Халдлагын тоо өсөхөөс гадна халдлага амжилттай болох магадлал улам бүр нэмэгдэж буй нь өнөөдрийн байдлаар IP сүлжээний орчинд ашиглагдаж буй аюулгүй байдлын шийдэл, технологиудыг юмсын интернэтийн орчинд ашиглах боломж хомс байгаатай холбоотой. Үүнээс гадна олон хувь борлуулагдаж буй төхөөрөмжүүдэд чиглэсэн халдлага тасралтгүй гарсаар байх нь зайлшгүй болж байна. Энэхүү судалгааны ажлын хүрээнд андройд утас, лед гэрэл, температурын сенсор, Apple-ийн ухаалаг цаг зэргийн өгөгдөлд тулгуурлан халдлага илрүүлэх туршилтыг хийж гүйцэтгэсэн бөгөөд юмсын интернэтийн төхөөрөмжийн төрлөөс хамаарч аюулгүй байдлын ялгаатай шийдлүүд хэрэглэх хэрэгтэй гэж үзсэн.

Key words/Түлхүүр үг: Юмсын интернэтийн аюулгүй байдал, Машин сургалт, weka, Юмсын интернэт.

1. Удиртгал

Бид бүхний өдөр тутамдаа ашиглаж буй уламжлалт IP сүлжээний төгсгөлийн болон зангилаа төхөөрөмжүүдийн хүчин чадал хангалттай түвшинд байгаа тул сүлжээний аль ч зангилаа, төхөөрөмж дээр аюулгүй байдлын янз бүрийн шийдлүүдийг ашиглахаас гадна сүлжээний орчинд төвлөрсөн удирдлага бүхий аюулгүй байдлын технологийг ашиглан халдлагаас үр дүнтэй хамгаалж байна. Харин юмсын интернэт орчинд дээрх аргуудыг шууд ашиглах боломжгүй байгаа нь төхөөрөмжийн хувьд хязгаарлагдмал нөөцтэй байгаатай холбоотойгоос гадна юмсын интернэтийн сүлжээнд ашиглаж буй төхөөрөмж нь уламжлалт сүлжээний төхөөрөмжтэй харьцуулахад хэд дахин олон байгаа нь мөн нөлөөлж байна. Үүнээс гадна төрөл бүрийн өгөгдөл (эрүүл мэнд, үйлдвэрлэл, гэрийн автоматжуулалт гэх мэт) боловсруулах шаардлага бүхий олон төрлийн төхөөрөмжүүд ашиглагдаж буй нь аюулгүй байдлыг хангах зорилгоор нэг шийдлийг ашиглах боломжгүй байдалд хүргэж байна. Юмсын интернэт нь физик төхөөрөмж, сүлжээ, програм хангамжийн уулзвар хэрэглээ болон дэд бүтэц, хүрээлэн буй орчны хяналтын зорилгоор ашиглагдаж буй систем бөгөөд сүүлийн жилүүдэд энэ төрлийн системүүдийн аюулгүй байдлыг хангах нь чухал асуудал болоод байна (X.Li et al, 2011, X.Liu et al., 2017). Юмсын интернэтийн сүлжээний орчинд өгөгдлийн нууцлалыг тодорхой түвшинд хангаж буй хэдий ч хууран мэхлэх (spoofing) халдлага, сүлжээнд хөнөөлт ажиллагаа явуулах дайралтууд, үйлчилгээ бусниулах, жэйминг (jamming), нууцаар чагнах, хөнөөлт програмын эрсдэл зэрэг уламжлалт халдлагууд байсаар байна (R.Roman et al., 2013, S.Chen et al., 2014). Юмсын интернэтийн орчинд ашиглагдаж буй төхөөрөмжүүд нь IP сүлжээний бусад төхөөрөмжүүдээс тэжээл, ашиглагдаж буй зурвасын өргөн, санах ой, боловсруулалт хийх багтаамж харьцангуй бага байдгаараа ялгаатай. Иймд ийм төрлийн төхөөрөмж, сүлжээний орчинд тохирсон аюулгүй байдлын оновчтой шийдэл ашиглах шаардлага үүсэж байна. Одоогийн байдлаар юмсын интернэтийн орчинд баталгаажуулалт ашиглах замаар хууран мэхлэх халдлагаас, хандалт хяналтын тусламжтайгаар зөвшөөрөгдсөн хэрэглэгчийг юмсын интернэтийн системд нэвтрүүлэх, хөнөөлт програм илрүүлэх аргачлалаар юмсын интернэтийн төхөөрөмжийн өгөгдлийг алдахаас хамгаалах зэрэг шийдлүүдийг ашиглаж байна (L. Xiao et al., 2016, M. Abu Alsheikh et al., 2017, L. Xiao et al., 2017). Халдлага илрүүлэх систем нь сүлжээгээр дамжиж буй хөнөөлт урсгалыг илрүүлэх, хяналт тавих зэрэг давуу талуудтай бөгөөд сигнатурт суурилсан

болон гажигт суурилсан гэсэн үндсэн хоёр төрөлтэй (Ugtakhbayar.N et al., 2020). Юмсын интернэтийн сүлжээ нь IPv6 сүлжээний загвар протокол болох 6LoWPAN-г сүлжээний давхаргад ашигладаг бөгөөд уг протокол нь 20-250kbps өгөгдөл дамжуулдгаас гадна CoAP протоколыг ашигладаг (S. Raza et al., 2013). Өмнө дурьдсан аюулгүй байдлын шийдлүүдийг олон судлаачид (J. Granjal et al., 2015, M. Ambrosin et al., 2016) санал болгож буй хэдий ч эдгээр нь одоогийн байдлаар халдлагаас хангалттай хэмжээнд хамгаалж чадахгүй байгаагаас гадна сүлжээний ачааллыг нэмэгдүүлэх, нөөцийг их хэмжээгээр ашиглах зэрэг сул талуудтай нь энэхүү судалгааны ажлыг хийх үндсэн шаардлагыг бий болгож байна. Уг ажлын хүрээнд хөдөлгөгч [actuator]-үүдэд ачаалал өгөхгүйгээс гадна хөдөлгөгч, брокер хоорондын урсгалд анализ хийх замаар халдлага илрүүлэх боломжтой халдлага илрүүлэх системийн судалгааг хийж гүйцэтгэлээ. Халдлага илрүүлэх систем хэлбэрээр perception давхаргын урсгалд дүн шинжилгээ хийх симуляцийн орчин одоогоор байхгүй тул уг судалгааг туршилтын физик орчин үүсгэж хийж гүйцэтгэсэн. Уг судалгааны ажлыг гүйцэтгэхдээ i. Судалгааны туршилтын орчинг бий болгох ii. Одоогийн байдлаар мэдэгдэж буй халдлагуудын судалгааг гүйцэтгэх iii. Хөнөөлт програмын халдлагыг илрүүлэх туршилтыг хийж гүйцэтгэх (нээлттэй сан болох Bot-IOT (N. Koroniotis et al., 2018, I. Van der Elzen et al., 2017)-ийг туршилтад ашиглав) гэсэн дарааллаар хийсэн.

2. Судлагдсан байдал

Сүүлийн жилүүдэд юмсын интернэтийн орчинд технологийн болон аюулгүй байдлын талаарх судалгаа олон тоогоор хийгдэж байна.

Мишра болон бусад судлаачдын (A. Mishra et al.,) ажилд утастай болон утасгүй сүлжээ тэр дундаа юмсын интернэтийн сүлжээний хувьд архитектурын ялгаатай тул халдлагын илрүүлэхэд ашиглагдах нотлох баримт, параметрууд ялгаатай байгаа талаар дурьдаж нийт долоон төрлийн халдлага илрүүлэх системийн хувьд харьцуулсан судалгаа хийж түүний үр дүнд мобайл агентэд суурилсан загварууд нь юмсын интернэтийн орчинд илүү тохирох талаар дүгнэлтэд хүрчээ.

Кумар болон бусад судлаачид (S. Kumar et al., 2016) ажилдаа MANET сүлжээний орчинд халдлага илрүүлэх алгоритмуудын есөн ангиллын халдлага илрүүлэх аргачлалыг ашиглан туршилт явуулсан бөгөөд ангиллын хувьд сигнатурт суурилсан, гажигт суурилсан болон хосолмол; архитектурын хувьд төвлөрсөн, тархсан, агентад суурилсан болон шатласан; илрүүлэлтийн хувьд бодит хугацааны болон оффлайн өгөгдөл дээр суурилсан байдлаар туршилтыг явуулж үр дүнг гүйцэтгэл, халдлага илрүүлэлт, хурд, чиглүүлэлтийн протоколын төрөл зэрэг найман төрөлд боловсруулжээ. Судалгааны үр дүнд статик орчинд халдлага илрүүлэх нь хялбар байсан бол динамик орчинд халдлага илрүүлэх нь түвэгтэй бөгөөд төхөөрөмж, програм хангамжийн өгөгдлийг хянах асуудал хөндөгджээ.

Шиа болон бусад судлаачдын (L. Xiao et al., 2017) ажилд үүлэн тооцооллын системд суурилсан халдлага илрүүлэх туршилтыг хийж гүйцэтгэсэн бөгөөд мобайл хэрэглэгчийн аюулгүй байдлыг 33 хувиар өсгөсөн бол халдлага илрүүлэлтийг 40 хувиар өсгөсөн үр дүнг үзүүлжээ. Уг ажилд мөн хөнөөлт програмыг илрүүлснээр юмсын интернэтийн орчинд үйлдэгдэх эрсдэл болох өгөгдөл хулгайлах, тэжээлийг үр ашиггүй зарцуулах, сүлжээний өгөөжийг бууруулах зэргийг багасгах боломжтойг дурьджээ.

3. Юмсын интернэтийн аюулгүй байдлын асуудлууд

Юмсын интернэтийн аюулгүй байдал нь юмс буюу сенсорууд болон бусад зүйлс, түүн дээр ажиллаж буй үйлчилгээнүүд, сүлжээний архитектур, протокол зэрэгт сүлжээний орчноос, физик орчноос, програмын орчноос халдах халдлага, дайралтуудаар тодорхойлогдох бөгөөд ихэнх тохиолдолд өгөгдөл хулгайлах, үзүүлэлтийг бууруулах эрсдэлүүдийг бий болгож байдаг бөгөөд дараах байдлаар ерөнхийлөн ангилан үзэж болно.

3.1 Үйлчилгээ бусниулах халдлага

Халдагч нь тухайн юмсын интернэтийн төхөөрөмжүүдрүү тасралтгүй хүсэлт илгээх замаар хэвийн ажиллагааг алдагдуулах (I. Andrea et al., 2015). Энэ төрлийн халдлагын аюултай тохиолдолд нь тархсан үйлчилгээ бусниулах халдлага (DDoS) бөгөөд юмсын интернэтийн орчинд үүнээс сэргийлэх нь түвэгтэй бөгөөд халдлагад өртөх магадлал өндөр (R. Roman et al., 2013).

3.2 Хууран мэхлэх

Халдагч нь ямар нэгэн төхөөрөмжийн RFID

тагийн мэдээлэл, MAC хаяг зэрэг холболтод чухал үүрэг бүхий өгөгдлийг хулгайлах замаар аль нэг төхөөрөмжийн дүрд тоглон өгөгдлийг дундаас нь хулгайлах үйлчилгээ бусниулах халдлага гүйцэтгэх эх үүсвэрийг бий болгох зэрэг эрсдэл бий болгодог (L. Xiao et al., 2016).

3.3 Жэйминг

Халдагч нь хуурамч дохио дамжуулах замаар юмсын интернэтийн төхөөрөмжийг сүлжээнээс салгах, буруу мэдээлэл дамжуулах, ачааллыг нэмэгдүүлэх, зурвасын өргөнийг дүүргэх зэрэг байдлаар халдах боломжтой (G. Han et al., 2017).

3.4 Програмчлалын халдлага

Мобайл төхөөрөмжүүдэд чиглэсэн хөнөөлт програм ашиглах замаар өгөгдөл хулгайлах, тэжээлийг үр ашиггүй зарцуулах, сүлжээ, төхөөрөмжийн ачааллыг нэмэгдүүлэх зэрэг эрсдэл үүсгэнэ (L. Xiao et al., 2017).

3.5 Бусад

Энэ хэсэгт дээр дурьдагдаагүй ангилалууд багтах бөгөөд үүнд өгөгдөл хулгайлах; жишээ нь эрүүл мэндийн бугуйвч хэрэглэгчийн өгөгдлийг цуглуулах замаар хувь хүний мэдээллийг олон нийтэд зарах, серверийн орчноос алдах зэрэг эрсдэлд оруулах (N. Koroniotis et al., 2018), MITM халдлага; III.B, C, D зэрэгт дурьдсан аргачлалуудын тусламжтайгаар сүлжээнд халдаж улмаар сүлжээг хяналтандаа оруулах, өгөгдлийг өөрчлөх, цуглуулах, юмсын интернэтийн хоорондын нууцлалтай өгөгдлүүдийг илрүүлэх зэрэг олон төрлийн эрсдэл, халдлага байх боломжтой юм (I. Andrea et al., 2015).

4. Үр дүн ба хэлэлцүүлэг

Энэхүү хэсэгт уг ажлын хүрээнд үүсгэсэн юмсын интернэтийн сүлжээ, өгөгдөл цуглуулсан байдал, машин сургалтын алгоритм, туршилтын үр дүн зэргийг авч үзэх болно.

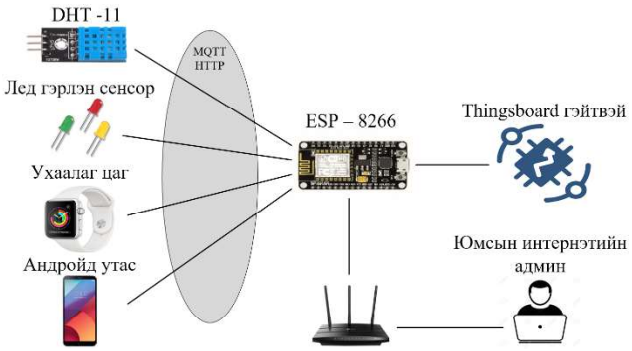
4.1 Туршилтын тоног төхөөрөмж

Уг ажлын хүрээнд home gateway төхөөрөмжөөр Raspberry PI 3b, юмсын интернэтийн хэрэглэгчийн интерфэйсээр Thingsboard гэйтвэй, юмсаар лед гэрэл, температур мэдрэгч, андройд утас, ухаалаг цаг, брокероор NODEMCU зэргийг ашигласан.

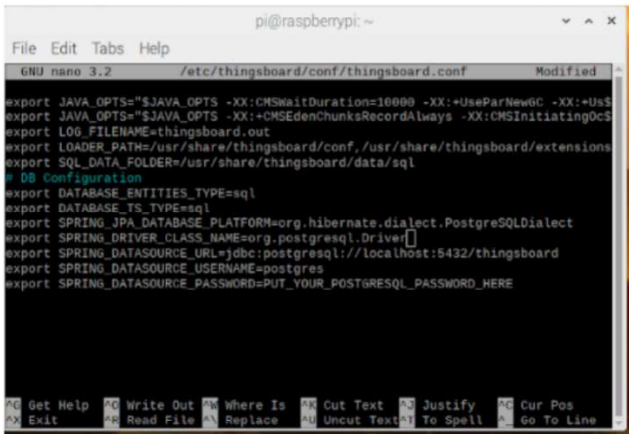
4.2 Сүлжээний ерөнхий зураглал

Туршилтад ашиглагдах сүлжээний ерөнхий загварыг Зураг 1-т үзүүллээ. Хөдөлгөгч сенсоруудаар DHT-11 температурын сенсор, лед гэрлэн сенсор, Apple-ийн ухаалаг цаг болон Андройд утас ашигласан бөгөөд эдгээр нь ESP-8266 брокерт MQTT, HTTP протоколуудаар өгөгдөл дамжуулж байгаа бөгөөд хэрэглэгчийн интерфэйсийн мэдээллийг Thingsboard гэйтвэй дээр цуглуулсан.

Зураг 2-т Thingsboard гэйтвэйний ерөнхий тохиргоог харууллаа. Уг хэсэгт хэдий хугацаанд брокероос мэдээлэл цуглуулах болон өгөгдлийн сангийн мэдээллийг тохируулж өгсөн.



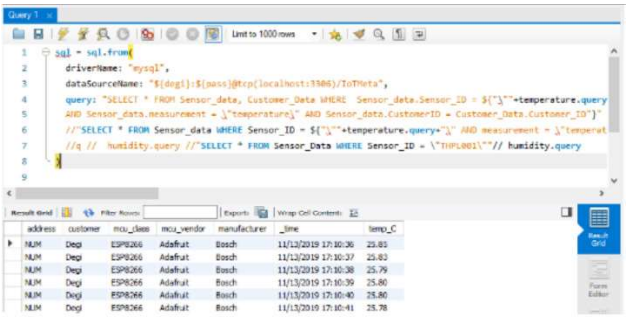
Зураг 1. Туршилтад ашиглагдах сүлжээний загвар



Зураг 2. Гэйтвэйний тохиргоо

4.3 Өгөгдөл цуглуулах

Туршилтын машин сургахад Bot-IoT санг ашигласан бөгөөд уг сан нь Bot-ийн сүлжээ үүсгэн юмсын интернэтийн орчинд халдлага болон энгийн урсгал дамжуулан цуглуулсан сан бөгөөд албан ёсны 44 онцлогтой.



Зураг 3. Цуглуулсан өгөгдлийн харагдах байдал

Туршилтад төхөөрөмж бүрийн дамжуулж буй өгөгдлийн ялгамжийг тодорхойлох, машин сургалтын алгоритмууд тухайн төхөөрөмжүүдийн сан дээр хэрхэн ажиллаж буйг тодорхойлох зорилгоор температурын сенсор, лед гэрлэн сенсор хоёрын өгөгдлийг нэг хэсэг (IoT sensor dataset), Apple-ийн ухаалаг цаг, Андройд утасны өгөгдлийг нэг хэсэг (IoT node (нөүд) dataset) болгон ялгаатай хоёр хэсэг өгөгдөл цуглуулж машин сургасан сантай ижил сан бий болгох зорилгоор сүлжээний орчинд timestamp скрипт ажиллуулсан. Уг санг бүрдүүлэхэд судлаачид нөүдэд DDoS, port scanning халдлага хийсэн бол сенсоруудад DDoS, жэйминг, brute force зэрэг халдлагыг хийж гүйцэтгэсэн. Зураг 3-т цуглуулсан өгөгдөлд query бичих замаар эхний хэсэг өгөгдлийн үр дүнг харууллаа. Харин хүснэгт 1-д туршилтад ашигласан сангийн мэдээллийг оруулав. Үүнд сенсоруудаас 100 урсгалын мэдээлэл цуглуулсан бол зангилаа төхөөрөмжүүдээс 237 урсгалын мэдээлэл цуглуулж туршилтад ашиглах 337 урсгалын мэдээллийг бэлдэв. Уг урсгалын мэдээлэлд Bot-IOT сангийн 44 онцлог шинжийг ямар нэгэн онцлог шүүх аргачлал ашиглалгүй бүгдийг нь ашигласан.

Хүснэгт 1. Туршилтын сангийн мэдээлэл

Сангийн нэрс	Урсгалын мэдээлэл (flows)
Сенсор сан	100
Нөүд сан	237
Нийт	**337**

4.4 Машин сургалтын алгоритмууд

Машин сургалтын туршилт, үр дүнг тооцохдоо “Weka” програм хангамж ашигласан бөгөөд энэ төрлийн судалгаанд түгээмэл ашиглагдаж буй Naïve Bayes(P. Domingos et al., 1997), Bayes Net (N. Friedman et al., 1997), Decision tree (J. Quinlan., 1986) гэсэн машин сургалтын алгоритмуудын (Ugtakhbayar N et al., 2020) хувьд судалгааны ажлын үр дүнг тооцоолсон. Уг ажлыг гүйцэтгэхдээ машин сургалтын алгоритмуудын параметруудыг програмын үндсэн утгаар ашигласан.

4.5 Танилтын хувийг тооцоолсон аргачлал

Танилтын нарийвчлалыг 1-р томъёоллыг ашиглан TP (true posi-tive), TN (True negative), FP (false positive), FN (false negative) утгуудын

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

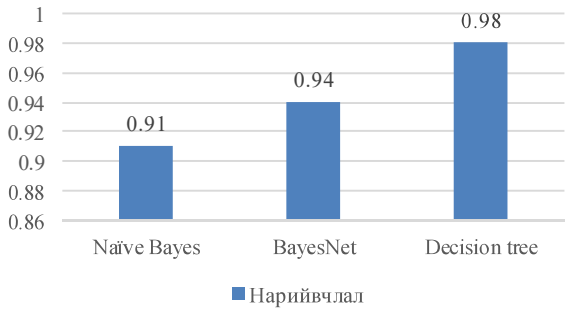
тусламжтайгаар тооцоолсон. Үүнээс гадна эдгээр утгуудыг ашиглан F1 оноо, персишн гэх мэт бусад үзүүлэлтийг тооцоолох боломжтой.

Хүснэгт 2-д үзүүлсэн 10 сенсорын 8 нь хэвийн урсгал дамжуулсан бөгөөд 2 сенсор нь халдлагатай өгөгдөл дамжуулсан гэж тооцоолсон. Машин сургалтын алгоритмын үр дүнг тооцохдоо энэхүү хүснэгтийн параметрүүдийг онцлог болгон нэмж ашигласан.

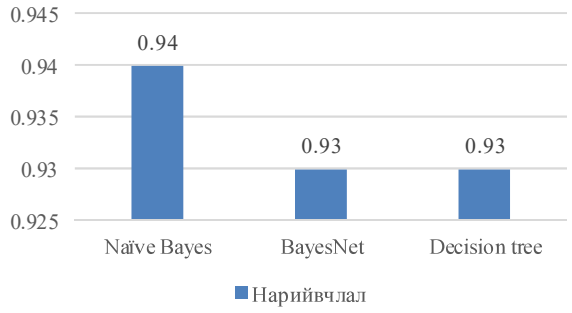
Хүснэгт 2. Туршилтын параметр

Парамет р	Утга
Ашигласан сенсорын тоо	10
Хамрах хүрээ	20*20м^2
Өгөгдөл цуглуулсан хугацаа	30 минут
Урсгал хооронд ын зай	30 секунд
Тээвэрлэлтийн түвшний протокол	TCP, UDP
Дамжуулах хурд	50kbps

Зураг 4-т IoT sensor сангийн үр дүнг сонгосон машин сургалтын алгоритмуудаар оруулан харьцуулсан үр дүнг харуулж байна. Уг зурагт харуулснаар decision tree 98%-ийн танилтын нарийвчлал үзүүлж сенсоруудаас ирж буй халдлагыг хамгийн өндөр хувьтай таньсан бол naïve bayes 91%-ийн танилт үзүүлсэн байна.



Зураг 4. Сенсор сангийн үр дүн

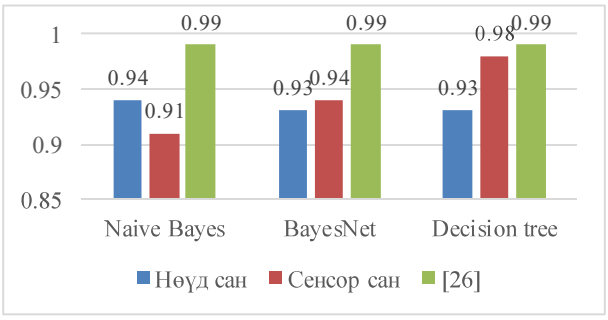


Зураг 5. Нөүд сангийн үр дүн

Зураг 5-д IoT нөүд сангийн үр дүнг сонгосон машин сургалтын алгоритмуудаар оруулан харьцуулсан үр дүнг харуулж байна.

Уг зурагт харуулснаар naïve bayes 94%-ийн танилтын нарийвчлал үзүүлж сенсоруудаас ирж буй халдлагыг хамгийн өндөр хувьтай таньсан бол bayes net, decision tree хоёр алгоритмын хувьд ижилхэн 93%-ийн танилт үзүүлсэн байна.

Судалгааны ажлын үр дүнг Мухаммад Шафик (Muhammad Shafiq et al., 2020) болон бусад судлаачдын Bot-IOT сан дээр хийсэн ажлын үр дүнтэй харьцуулан зураг 6-д харууллаа.



Зураг 6. IoT нөүд сан ашиглан машин сургалтын алгоритмуудын үр дүнг харьцуулсан байдал

5. Дүгнэлт

Уг ажлын хүрээнд юмсын интернэтийн орчинд ялгаатай хоёр төрлийн хөдөлгөгч болох сенсор, нөүдүүдийн халдлагатай урсгалыг тусад нь цуглуулж машин сургалтын алгоритмаар турших ажлыг хийж гүйцэтгэв. Ажлын үр дүнд сенсор болон нөүдүүдийн хувьд ялгаатай машин сургалтын алгоритм ашиглавал халдлагыг илүү үр дүнтэй таних боломжтой гэсэн дүгнэлтэд хүрлээ. Учир нь сенсорын хувьд decision tree алгоритм халдлагыг илүү өндөр хувьтай таньж байсан бол нөүдийн хувьд naïve bayes илүү өндөр хувьтай таньж байна. Уг ажлыг цаашид сайжруулах зорилгоор халдлагын төрөл бүрээр чухал онцлогыг тодорхойлж үр дүнг тооцоолох, тэжээл, сүлжээний ачаалалтай холбоотой параметруудыг нэмж халдлагын танилтыг тооцолох шаардлагатай гэж үзлээ.

Зохиогчийн оролцоо

Энэхүү судалгааны ажлын өгөгдөл цуглуулах хэсгийг судлаач П.Болд гүйцэтгэж түүн дээр анализ хийх, үр дүнг тооцоолох, өгүүлэл бичих ажлыг Н.Угтахбаяр хийж, үр дүн болон өгүүллийн бичиглэлийг хянан магадлах ажлыг Б.Өсөхбаяр хийж гүйцэтгэв.

Санхүүжилт

МУИС-ийн Залуу судлаачдын багийн P2018-3630 дугаартай грантын санхүүжилтээр хийж гүйцэтгэв.

Ашиг сонирхлын зөрчилгүйн баталгаа

Зохиогчид нь энэхүү судалгааны ажлаа хийж гүйцэтгэхдээ санхүүжүүлэгч болон бусад байгууллага, хувь хүнтэй ямар нэгэн ашиг сонирхолын зөрчилгүйгээр гүйцэтгэсэн болно.

Ном зүй

X. Li, R. Lu, X. Liang, X.Shen, “Smart community: An Internet of Things Application,” IEEE Communications, vol. 49, no. 11, pp. 68-75, Nov. 2011.

X. Liu, M. Zhao, S. Li, F. Zhang, W. Trappe, “A security Framework for the Internet of Things in the Future Internet Architecture,” Future Internet, vol. 9, no. 3, pp. 1-28, Jun. 2017.

R. Roman, J. Zhou, J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things,” Computer Networks, vol. 57, no. 10, pp. 2266-2279, Jul. 2013.

S. Chen, H. Xu, D. Liu, and B. Hu, “A vision of IoT: Applications, challeng-es, and opportunities with chinaperspective,” IEEE Internet of Things Journal, vol. 1 no. 4, pp. 349-359, Jul. 2014.

L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, “ PHY-layer spoofing detec-tion with reinforcement learning in wireless networks,” IEEE Trans. Veh. Technol., vol. 65, no. 12 , pp. 10037–10047, Dec. 2016.

M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Ta n, “Machine learning in wireless sensor networks: Algorithms, strategies, and applications,” IEEE Commun. Surveys Tutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.

L. Xiao, Y. Li, X. Huang, and X. J. Du, " Cloud-based malware detection game for mobile devices with offloading," IEEE Trans. Mobile Comput., vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

Ugtakhbayar N., Usukhbayar B., Baigaltugs S. (2020) A Hybrid Model for Anomaly-Based Intrusion Detection System. In: Pan JS., Li J., Tsai PW., Jain L. (eds) Advances in Intelligent Information Hiding and Multimedia Signal Processing. Smart Innovation, Systems and Technologies, vol 157. Springer, Singapore.

J. Granjal, E. Monteiro and J. Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, pp. 1294-1312, 2015

M. Ambrosin et al., "On the Feasibility of Attribute-Based Encryption on Internet of Things Devices," in IEEE Micro, vol. 36, no. 6, pp. 25-35, Nov.-Dec. 2016. doi: 10.1109/MM.2016.101.

A. Mishra, K. Nadkarni, A. Patcha, "Intrusion detection in wireless ad hoc net-works," IEEE Wireless Communications, vol. 11, no. 1, pp. 48–60, 2004.

S. Raza, L. Wallgren, and T. Voigt, "SVELTE: real-time intrusiondetection in the internet of things,"Journal of Ad Hoc Networks, vol. 11,no. 8, pp. 2661–2674, 2013.

S. Kumar, K. Dutta, Intrusion detection in mobile ad hoc networks: tech-niques,systems, and future challenges, Security and Communication Networks 9 (14)(2016) 2484–2556.

L. Xiao, Y. Li, X. Huang, and X. J. Du, "Cloud-based malware detection game for mobile devices with offloading,"IEEE Trans. Mobile Computing, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of ma-chine learning classifiers for mobilemalware detection,"Soft Computing, vol. 20, no. 1, pp. 343–357, Jan. 2016.

I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in Proc. IEEE Symp. Computers and Communication, Larnaca, Cyprus, Feb. 2015, pp. 180–187.

R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of things," Comput. Netw., vol. 57, no. 10, pp. 2266–2279, July 2013.

L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, " PHY-layer spoofing detec-tion with reinforcement learning in wireless networks," IEEE Trans. Veh. Technol., vol. 65, no. 12 , pp. 10037–10047, Dec. 2016.

G. Han, L. Xiao, and H . V. Poor, "Two-dimensional anti-jamming com-munication based on deep reinforcement learning," in Proc. IEEE Int. Conf. Acoustics Speech and Signal Processing, New Orleans, LA, Mar. 2017, pp. 2087–2091.

Z. Ya n, P. Zhang, and A. V. Va si la kos, "A survey on trust man-agement for Internet of things," J. Netw. Comput. Appl., vol. 42, no. 3, pp. 120–134, June 2014.

N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, "Towards the devel-opment of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," 2018, arXiv:1811.00701.

I. Van der Elzen, J. van Heugten, "Techniques for Detecting Compromised Iot Devices," University of Amsterdam, 2017.

P. Domingos, M. Pazzani, "On the optimality of the simple bayesian classifier under zero–one loss," Mach. Learn. 29 (1997) pp. 103–130.

N. Friedman, D. Geiger, M. Goldszmidt, "Bayesian network classifiers," Mach. Learn. 29 (1997), pp. 131–163.

J. Quinlan, "Induction of decision trees," Mach. Learn. (1986)

Muhammad Shafiq, Zhihong Tian, Yanbin Sun, Xiaojiang Du, Mohsen Gui-zani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," Future Generation Computer Systems, 107 (2020), pp. 433-442