Сурдаг машинд суурилсан халдлага илрүүлэх систем

Б. Өсөхбаяр, Ж.Нямжав
МУИС, Хэрэглээний Шинжлэх Ухаан, Инженерчлэлийн Сургууль
Электроник, Холбооны Инженерчлэлийн Тэнхим
Цахим шуудан: usukhbayar@seas.num.edu.mn

***Хураангуй*—Сүлжээнд холбогдсон систем, програм хангамжуудын хурдацтай өсөлтийг дагаад аюулгүй байдлыг нь найдвартай хангах хэрэгцээ шаардлагыг бий болж байна. Сүлжээний аюулгүй байдлыг хангахад халдлага илрүүлэх системийг түгээмэл хэрэглэдэг. Бид энэ судалгааны ажлаар сурдаг алгоритмуудад суурилсан халдлага илрүүлэх системийн архитектурыг боловсруулж, хэд хэдэн сурдаг алгоритмын гүйцэтгэлийн харьцуулсан судалгааг KDD99 жишиг өгөгдлийн санг ашиглан хийж гүйцэтгэнэ.**

Keywords—халдлага, аюулгүй байдал, сурдаг машин

I. Удиртгал

Сүлжээнд холбогдсон систем програм, хангамжуудын хурдацтай өсөлтийг дагаад аюулгүй байдлыг нь найдвартай хангах хэрэгцээ шаардлагыг бий болж байна. Хэдийгээр аюулгүй байдлыг криптографи, антивирус, хамгаалалтын хана гэх мэт механизм хэрэглэж хамгаалах аргууд байдаг ч аюулгүй байдлыг бүрэн дүүрэн хангах боломжгүй юм. Иймээс сүлжээний аюулгүй байдлыг хангахад халдлага илрүүлэх системийг түгээмэл хэрэглэж байна.

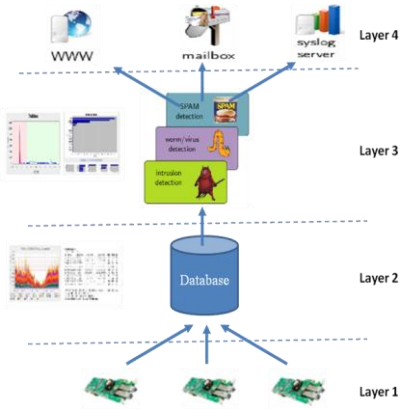
Халдлага илрүүлэх систем нь сүлжээний аюулгүй байдалд хор, хөнөөл учруулах зорилготой халдлага, дайралтуудыг илрүүлэхэд сүлжээ эсвэл системийн үйл ажиллагааг хянаж, удирдлагын хэсэгт халдлагын дохио илгээдэг механизм юм. Халдлага илрүүлэх системийг сүлжээнд суурилсан ба хостод суурилсан гэж хуваадаг ба халдлагыг илрүүлэхдээ сигнатюраар илрүүлэх болон гажилтаар илрүүлэх гэсэн хоёр үндсэн техникт тулгуурладаг [1].

Гажилтаар илрүүлэх техник нь шинээр гарч ирсэн халдлагуудыг илрүүлэх боломжтой байдгаараа сигнатюраар илрүүлэх техникээс давуу талтай. Сүүлийн үед гажилтаар илрүүлэх техникт өгөгдөл олборлох техник болон сурдаг машиныг хэрэглэх судалгаа эрчимтэй хийгдэж байгаа хэдий ч, үр дүн нь практикт нэвтэрч хэрэглээ болоогүй байна [2].

Бид энэ судалгааны ажлаар SVM, Decision tree, ANN гэх мэт сурдаг алгоритмуудад суурилсан халдлага илрүүлэх системийн архитектурыг боловсруулж эдгээр алгоритмуудын гүйцэтгэлийн харьцуулсан судалгааг KDD99 [3] жишиг өгөгдлийн санг ашиглан хийж гүйцэтгэнэ.

II. Халдлага илрүүлэх ухаалаг системийн архитектур

Энэ хэсэгт бид санал болгож буй хөнөөлт урсгал илрүүлэх системийн архитектур, бүтэц, зохион байгуулалтын талаар авч үзнэ. Бид энэ системийг сурдаг алгоритмд суурилсан халдлага илрүүлэх систем байхаар [4] судалгаанд үндэслэн боловсруулсан. Тухайн хөнөөлт урсгал илрүүлэх систем нь сүлжээний урсгалыг цуглуулан тодорхой давхаргат бүтцүүдээрээ дамжуулан боловсруулалт хийж сүлжээний урсгалын пакетуудыг халдлага агуулсан эсвэл хэвийн эсэхийг тодорхойлдог систем юм. Системийн архитектур давхаргат бүтэцтэй тул доод давхарга нь дээд давхаргад тодорхой сервисээр хангахаар зохицуулагдсан. Бидний боловсруулсан халдлага илрүүлэх системийн ерөнхий архитектурыг Зураг 1-д үзүүлэв. Энэ систем нь дараах үндсэн 4 модулиас бүрдэнэ: (1) сүлжээний пакет цуглуулагч буюу сенсор, (2) сүлжээний урсгалын өгөгдлийн сан (3) сүлжээний урсгал шинжлэгч (4) үр дүнг илтгэгч.



Зураг 1. Халдлага илрүүлэх системийн архитектур

- **Модуль 1:** Системийн хамгийн доод буюу суурь давхарга сүлжээний урсгалаас пакетуудыг цуглуулах давхаргад дамжуулах үүрэгтэй. Энэ давхарга пакетуудыг дамжуулах үүргийг tcpdump, nfdump гэх мэт пакет шиншлэгчүүдийг ашигласан сенсоруудыг сүлжээнд тархаан байршуулах замаар гүйцэтгэнэ.
- **Модуль 2:** Системийн хоёрдох давхарга буюу сенсорууд, тэдгээрээс илгээсэн пакетуудыг хүлээн авч өгөгдлийн санд хадгалах үүрэгтэй давхарга. Энэ давхарга нь пакетуудыг өгөгдлийн санд

хадгалахаас гадна санд цугласан өгөгдлүүдийн талаарх статистик мэдээллээр хангах болон менежмент хийх граффик интерфейстэй байна.

- **Модуль 3:** Системийн гуравдах давхарга буюу санд байгаа сүлжээний урсгалын өгөгдлүүдийг шинжлэх давхарга. Өгөгдлийг шинжлэхдээ сурдаг алгоритмд суурилсан халдлага илрүүлэх систем пакетуудыг хэвийн эсвэл халдлага агуулсан эсэхээр нь тодорхойлж, ялгана.
- **Модуль 4:** Системийн дөрөвдөх давхарга буюу үр дүнг илтгэх давхарга. Энэ давхарга шинжлэх давхаргын илрүүлсэн халдлага агуулсан сүлжээний урсгалын талаарх мэдээллийг сүлжээний администратор эсвэл сүлжээний аюулгүй байдлын мэргэжилтэнд төрөл бүрийн арга замуудаар илтгэнэ.

III. KDD99 ӨГӨГДЛИЙН САН

Бид судалгаандаа халдлага илрүүлэх системүүдийн шинжилгээнд хамгийн түгээмэл хэрэглэгдэг KDD99 жишиг өгөгдлийн санг ашигласан [5]. KDD99 өгөгдлийн санг АНУ-ын Батлан Хамгаалах Яамны Дэвшилтэт Судалгааны Төслийн Агентлаг болон Агаарын хүчний судалгааны лабораториудын дэмжлэгтэйгээр Массачусетийн технологийн институтийн Линкольн лабораторид халдлага илрүүлэх системүүдийг үнэлэхэд зориулан үүсгэсэн. Тухайн санг үүсгэхдээ төрөл бүрийн үйлдлийн систем, сервис бүхий гурван халдлага хүлээн авах компьютер болон төрөл бүрийн сүлжээний хаягаас халдлага эсвэл хэвийн хандалт хийх сүлжээний урсгал үүсгэгч нэмэлт гурван компьютер бүхий сүлжээнээс пакетийн урсгалыг цуглуулсан.

KDD99 сан нь 7 долоо хоногийн 5 өдөр тус бүрээр цуглуулсан 5 сая орчим холболтын бичлэгтэй, холболт тус бүр 100 байт орчим хэмжээтэй tcpdump форматтай 4 Гб хэмжээтэй шахсан файл юм. Үүнээс хоёр долоо хоногийн шалгах сан нь нийт 2 сая орчим холболтын бичлэгтэй. Холболт гэдэг нь тодорхой хугацааны мужид илгээгч, хүлээн авагчын хоорондох холболт тогтоохоос, холболт салгах хүртэлх TCP пакетууд дараалал буюу тодорхой протоколоор илгээгч IP хаягаас хүлээн авагч IP хаягийн хооронд илгээж, хүлээн авч буй өгөгдлийн урсгал юм. Холболт бүрийг хэвийн (normal) буюу тодорхой нэг төрөлд хамаарах дайралт (attack) гэж тэмдэглэсэн. KDD99 санд агуулагдаж буй халдлагуудыг дараах дөрвөн ерөнхий ангилалд хуваагдаг:

- **Denail of Service (DoS):** Халдагчийн зүгээс ердийн хэрэглэгчийн үйлчилгээг тасалдуулах оролдлого хийх, жиш. syn flooding.
- **Remote to Local (r2l):** Халдагч сүлжээгээр дамжуулан компьютерт нэвтрэх оролдого хийх, жиш. password guessing.
- **User to Root (u2r):** Халдагч компьютерт хязгаарлагдмал эрхээ ашиглан хандаж, администратор хэрэглэгчийн эрх олж авахыг оролдох, жиш. buffer overflow attacks.
- **Probe:** Халдагч компьютерийн мэдээллийг цуглуулах эсвэл сул талыг нь тодорхойлохыг оролдох, жиш. port scanning.

KDD-гийн сургах санд нийт 24 төрлийн халдлага агуулсан ба шалгах санд нэмэлт 14 төрлийн халдлагатай, нийт 38 төрлийн халдлага агуулсан [3].

3.1. Өгөгдөл боловсруулалт

KDD99 сангийн холболт тус бүрт 41 онцлог шинжийг тодорхойлсон [6,7] ба нийт онцлог шинжүүдийг дараах дөрвөн ангилалд хуваадаг:

- **Үндсэн онцлог шинж (Basic Features):** Эдгээр онцлог шинжүүдийг пакетийн өгөгдлийн хэсгийг оролцуулалгүйгээр толгой хэсгээс нь ялгадаг
- **Агуулгын онцлог шинж (Content features):** Тодорхой домэйн мэдлэгт тулгуурлан пакетуудын өгөгдлийн хэсгийг шинжилж ялгадаг онцлог шинжүүд. үнэлэхэд хэрэглэдэг. Жиш. Амжилтгүй нэвтрэх оролдлогын тоо энэ онцлог шинжид хамаардаг
- **Хугацаагаар ангилсан онцлог шинж (Time-based Traffic Features):** Эдгээр онцлог шинжүүд нь хоёр секундын хугацааны интервалд шинж чанаруудыг барьж авахад замаар тодорхойлогддог. Жишээ нь 2 секундын интервалд нэг хостод холбогдсон холболтын тоо юм
- **Хостоор нь ангилсан онцлог шинж (Host-based Traffic Features):** Зарим шиншлэх халдлагууд 2 секундаас илүү хугацааны интервалд хостуудад хандалт хийдэг (жиш. минутанд нэг удаа хостуудыг шалгах г.м.). Иймээс холболтыг хүлээн авагч хостоор ангилж болох бөгөөд тухайн хостод холбогдсон холболтын хугацааны интервалаар бус тоогоор нь (энэ тохиолдолд 100 холболт) авч үзэн онлог шинжүүдийг ялгасан

Бид судалгаандаа хэрэглэхээр KDD99 өгөгдлийн сангаас холболт тус бүрээр 41 онцлог шинжийг тодорхойлон, ялгаж, үүсгэсэн хэвийн (normal) болон дайралт (attack) гэж ангилсан 125973 мөр бичлэгтэй сургах болон 22544 мөр бичлэгтэй шалгах сангуудыг үүсгэсэн. Бид энэ ажилд гол бүрдүүлэгчийн шинжилгээ (PCA)-г хэрэглэж өгөгдлийн тоо хэмжээг багасгах мөн өгөгдлийн санг нормчилох байдлаар өгөгдлийн урьчилан боловсруулалтыг хийсэн.

IV. ТУРШИЛТ, ҮР ДҮН

Бид туршилтыг явуулахдаа Intel(R) Xeon(R) CPU X5650@2.67GHz , cores: 6 процессор, 24GB санах ой, 2TB хард дисктэй компьютер болон Ubuntu 12.04 линукс үйдлийн системд суурилсан сүлжээний аюулгүй байдлын мониторинг хийдэг SecurityOnion системийг хэрэглэсэн. Мөн Жавад суурилсан сурдаг машины алгоритмуудыг агуулсан нээлттэй эхтэй Weka [9] програмыг хэрэглэсэн.

Системийн илрүүлэлтийн үр дүнг тогтоох зорилгоор туршилтанд KDD99 өгөгдлийн сангаас холболт тус бүрээр 41 онцлог шинжийг тодорхойлон, ялгаж үүсгэсэн

өгөгдлийн сангийн сургах хэсгийг алгоритмуудыг сургахад ашиглаж, шалгах санг сурдаг машинд суурилсан халдлага илрүүлэх системийн шинж, чанарыг тодорхойлоход ашигласан. Мөн халдлага илрүүлэх системийн үр дүнг үнэлэхийн тулд хэд хэдэн хэмжигдэхүүнүүдийг авч үзсэн [8]. Үүнд:

- True Positives (TP): Халдлагыг халдлага гэдгээр нь зөв танисан тоо хэмжээ
- True Negatives (TN): Хэвийн урсгалыг хэвийн гэдгээр нь зөв танисан тоо хэмжээ
- False Positives (FP): Хэвийн урсгалыг хөнөөлтэй гэж танисан тоо хэмжээ
- False Negatives (FN): Хөнөөлтэй урсгалыг хэвийн гэж танисан тоо хэмжээ
- Мөн True Positive Rate (TPR) буюу Detection Rate (DR) $\frac{TP}{TP+FN} * 100\%$,
- False Positive Rate (FPR) $\frac{FP}{TN+FP} *100\%$,
- Overall Accuracy (OA) $\frac{TP+TN}{TP+TN+FP+FN} * 100\%$.

Бид үр дүнг үнэлэхдээ илрүүлэлт DR-ийн утга аль болох их байх болон FPR-ийн утга аль болох бага байлгахыг чухалчлан авч үзсэн. Мөн сурдаг алгоримтуудын боловсруулалтын хугацааг авч үзсэн.

4.1. Үр дүн

Туршилтын үр дүнг SVM, J48, ANN зэрэг сурдаг алгоритмуудын нарийвчлал, фолс позитив, тооцоолын хугацаагаар нь харьцуулж харуулав (Хүснэгт 1). Бид сонгож авсан онцлог шинжүүдээ PCA-г хэрэглэн багасгаж системийн илрүүлэлт цаашид нэмэгдэж байгаа эсэхийг торхойлсон. Үүний тулд эхлээд PCA-г хэрэглээгүй онцлог шинжүүдээрээ системээ сургаж үр дүнг шалгаад түүний дараа PCA функцийг идэвхижүүлсэний дараах онцлог шинжүүдээр системээ сургасан үр дүнг шалгасан. Туршилтын үр дүнгээс харахад сурдаг алгоритмуудаас SVM алгоритм хамгийн өндөр илрүүлэлттэй мөн хамгийн фолс позитив хувь болон тооцоолын хугацаа хамгийн бага байгаа нь харагдаж байна. Мөн PCA хэрэглэж боловсруулалт хийсний дараа системийн илрүүлэлт тодорхой хэмжээгээр нэмэгдсэн байна.

ХҮСНЭГТ 1. СУРДАГ АЛГОРИТМУУДЫН ҮР ДҮНГИЙН ХАРЬЦУУЛАЛТ

Learning algorithms	PCA used	DR (%)	FPR (%)	Time
SVM	no	99.45	1.94	78.65
	yes	99.97	1.56	7.65
Decision tree	no	97	1.94	11.51
	yes	98. 56	2.06	10.89
ANN	no	99.1	1.94	9.25
	yes	99.45	1.56	8.09

V. ДҮГНЭЛТ

Бид судалгааны ажынхаа хүрээнд халдлага илрүүлэх системүүдийн үнэлгээнд хамгийн түгээмэл хэрэглэдэг KDD99 жишиг өгөгдлийн сангийн судалгааг хийж, тухайн сангийн өгөгдлөөс нийт 41 онцлог шинжээр өгөгдлүүдийг ялгаж сан үүсгэн сурдаг алгоритмуудын судалгаанд хэрэглэсэн. Өгөгдлийн сан нь сургах, шалгах гэсэн хоёр хэсэгтэй бөгөөд сургах хэсэгт нийт 24 төрлийн халдлага агуулсан 125973 мөр бичлэгтэй ба шалгах сан нэмэлт 14 төрлийн халдлагатай, нийт 38 төрлийн халдлага агуулсан 125973 мөр бичлэгтэй.

Бид өгөгдлийг гол бүрдүүлэгчийн шинжилгээний аргаар тоо хэмжээг багасгаж, мөн нормчилох аргаар урьчилан боловсруулалтыг хийж, боловсруулалт хийхийн өмнө хийсэний дараа гэсэн байдлаар SVM, J48, ANN сурдаг алгоритмуудын үр дүнгийн харьцуулсан судалгааг хийсэн. Үр дүнгээс харахад SVM алгоритм илрүүлэлт өндөр, алдаатай илрүүлэлтийн хувь болон тооцооллын хугацаа хамгийн бага байна.

Цаашид бид энэ судалгааны үр дүн ашиглаж SVM алгоримд суурилсан халдлага илрүүлэх системийг сигнатюрт суурилсан халдлага илрүүлэх системийн фолс позитив буюу алдаатай илрүүлэлттэй харьцуулан судлах замаар хадлагын дохионоос бодит халдлагыг зөв тодорхойлох боломжийг авч үзнэ.

АШИГЛАСАН МАТЕРИАЛ

[1] Robert Mitchell, Ing-Ray Chen, A survey of intrusion detection techniques for cyber-physical systems, April 2014, ACM Computing Surveys Volume 46 Issue 4

[2] Lee, W., S. J. Stolfo, and K. W. Mok (1999a, 9–12 May). A data mining framework for building intrusion detection models. In Proc. of the 1999 IEEE Symp. on Security and Privacy, Oakland, CA, pp. 120–132. IEEE Computer Society Press.

[3] 1999 DARPA Intrusion Detection Evaluation Data Set, from http://www.ll.mit.edu/ideval/data/1999data.html.

[4] Mukkamala, S.; Sung, A.H., "A comparative study of techniques for intrusion detection," Tools with Artificial Intelligence, 2003. Proceedings. 15th IEEE International Conference on , vol., no., pp.570,577, 3-5 Nov. 2003

[5] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[6] Kayacik, H.G., Zincir-Heywood, A. N. and Heywood, M.L.(2006). Selecting features for Intrusion detection: a feature analysis on KDD 99 intrusion detection datasets.

[7] Lee, W. and S. J. Stolfo, A framework for constructing features and models for intrusion detection systems. Information and System Security 3 (4), 227–261, 2000.

[8] Weka 3: Data Mining Software in Java, http://www.cs.waikato.ac.nz/ml/weka/

[9] I.H. Witten, E. Frank, Data Mining: Practical Machine Learning Tools and Techniques, 2nd ed. Morgan Kaufmann, 2005.