**IDSIFORIHYBRIDICLOUD**

**MUSHTAQ-AHMAD-DARI  
DEPARTMENT-OF-I.T  
MTECH-I.T54-CHANDIANAIGANDERBAL**

mushtaqdar@hotmail.com

Abstract—NowadaysIIntrusionIDetectionISystemI(IDS),IwhichIisIincreasinglyIaIkeyIelementIofIsystemIsecurity,IisIusedItoIidentifyItheImaliciousIactivitiesIinIaIcomputerIsystemIorInetwork.IThereIareIdifferentIapproachesIbeingIemployedIinIintrusionIdetectionIsystems,IbutIunluckilyIeachIofItheItechniqueIsoIfarIisInotIentirelyIideal.ITheIpredictionIprocessImayIproduceIfalseIalarmsIinImanyIanomalyIbasedIintrusionIdetectionIsystems.IWithItheIconceptIofIfuzzyIlogic,ItheIfalseIalarmIrateIinIestablishingIintrusiveIactivitiesIcanIbeIreduced.IAIsetIofIefficientIfuzzyIrulesIcanIbeIusedItoIdefineItheInormalIandIabnormalIbehaviorsIinIaIcomputerInetwork.ITherefore,IsomeIstrategyIisIneededIforIbestIpromisingIsecurityItoImonitorItheIanomalousIbehaviorIinIcomputerInetwork.IInIthisIpaper,IIIpresentIaIfewIresearchIpapersIregardingItheIfoundationsIofIintrusionIdetectionIsystems,ItheImethodologiesIandIgoodIfuzzyIclassifiersIusingIgeneticIalgorithm,IwhichIareItheIfocusIofIcurrentIdevelopmentIeffortsIandItheIsolutionIofItheIproblemIofIIntrusionIDetectionISystemItoIofferIaIrealIworldviewIofIintrusionIdetection.IUltimately,IaIdiscussionIofItheIupcomingItechnologiesIandIvariousImethodologiesIwhichIpromiseItoIimproveItheIcapabilityIofIcomputerIsystemsItoIdetectIintrusionsIisIofferedIKeywords—IntrusionIDetectionISystemI(IDS),IAnomalyIbasedIintrusionIdetection,IGeneticIalgorithm,IFuzzyIlogic.IIntroductionI(IntrusionIdetectionIisItheIprocessIofImonitoringItheIeventsI([1],I[2],I[3])IoccurringIinIaIcomputer

systemIorInetworkIandIanalyzingIthemIforIsignsIofIprobableIincidents,IwhichIareIviolationsIorIforthcomingIthreatsIofIviolationIofIcomputerIsecurityIstrategies,IadequateIusedIpolicies,IorIusualIsecurityIpractices.IIntrusiveIeventsItoIcomputerInetworksIareIexpandingIbecauseIofItheIlikingIof

adoptingItheIinternetIandIlocalIareaInetworksI[4]IandInewIautomatedIhackingItoolsIandIstrategy.IComputerIsystemsIareIevolvingItoIbeImoreIandImoreIexposedItoIattack,IdueItoIitsIwideIspreadInetworkIconnectivity.IIurrently,InetworkedIcomputerIsystemsIplayIanIeverImoreImajorIroleIinIourIsocietyIandIits.Economyy.ITheyIhaveIbecomeItheItargetsIofIaIwideIarrayIofImaliciousIthreatsIthatIinvariablyIturnIintoIrealIintrusions.IThisIisItheIreasonIcomputerIsecurityIhasIbecomeIaIvitalIconcernIforInetworkIpractitioner.ITooIoften,IintrusionsIcauseIdisasterIinsideILANsIandItheItimeIandIcostItoIrenovateItheIdamageIcanIgrowItoIextremeIproportions.IInsteadIofIusingIpassiveImeasuresItoIrepairIandIpatchIsecurityIholeIonceItheyIhaveIbeenIexploited,IitIisImoreIefficientItoItakeIupIaIproactiveImeasureItoIintrusions.I36

IntrusionIDetectionISystemsI(IDS)IareIprimarilyIfocusedIonIidentifyingIprobableIincidents,ImonitoringIinformationIaboutIthem,ItriesItoIstopIthem,IandIreportingIthemItoIsecurityIadministratorsI[5]IinIreal-timeIenvironment,IandIthoseIthatIexerciseIauditIdataIwithIsomeIdelayI(non-real-time).ITheIlatterIapproachIwouldIinIturnIdelayItheIinstanceIofIdetection.IInIaddition,IorganizationsIapplyIIDSsIforIotherIreasons,IsuchIasIclassifyingIproblemsIwithIsecurityIpolicies,IdocumentingIexistingIattacks,IandIpreventingIindividualsIfromIviolatingIsecurityIpolicies.IIDSsIIaveIbecomeIaIbasicIadditionItoItheIsecurityIinfrastructureIofIalmostIeveryIorganization.IAIusualIIntrusionIDetectionISystemIisIdemonstratedIinIFigureI1.

**

NOTE:ITheIarrowIlinesIsymbolizeItheIamountIofIinformationIflowingIfromIoneIcomponentItoIanother

FigureI1.IVeryISimpleIIntrusionIDetectionISystem

IntrusionIDetectionISystemsIareIbroadlyIclassifiedIintoItwoItypes.ITheyIareIhost-basedIandInetwork-basedIintrusionIdetectionIsystems.IHost-basedIIDSIemploysIauditIlogsIandIsystemIcallsIasIitsIdataIsource,IwhereasInetwork-basedIIDSIemploysInetworkItrafficIasIitsIdataIsource.IAIhostIbased

IDSIconsistsIofIanIagentIonIaIhostIwhichIidentifiesIdifferentIintrusionsIbyIanalyzingIauditIlogs,IsystemIcalls,IfileIsystemIchangesI(binaries,IpasswordIfiles,Ietc.),IandIotherIrelatedIhostIactivities.IInInetwork-basedIIDS,IsensorsIareIplacedIatIstrategicIpositionIwithinItheInetworkIsystemItoIcaptureIallIincomingItrafficIflowsIandIanalyzeItheIcontentsIofItheIindividualIpacketsIforIintrusiveIactivitiesIsuchIasIdenialIofIserviceIattacks,IbufferIoverflowIattacks,Ietc.IEachIapproach

hasIitsIownIstrengthsIandIweaknesses.ISomeIofItheIattacksIcanIonlyIbeIdetectedIbyIhost-basedIorIonlyIbyInetwork-basedIIDSITheItwoImainItechniquesIusedIbyIIntrusionIDetectionISystemsIforIdetectingIattacksIareIMisuseIDetectionIandIAnomalyIDetection.IInIaImisuseIdetectionIsystem,IalsoIknownIasIsignatureIbasedIdetectionIsystem;IwellIknownIattacksIareIrepresentedIbyIsignatures.IAIsignatureIisIaIpatternIofIactivityIwhichIcorrespondsItoIintrusion.ITheIIDSIidentifiesIintrusionsIbyIlookingIforIthese

patternsIinItheIdataIbeingIanalyzed.ITheIaccuracyIofIsuchIaIsystemIdependsIonIitsIsignatureIdatabase.IMisuseIdetectionIcannotIdetectInovelIattacksIasIwellIasIslightIvariationsIofIknownIattacks.IAnIanomaly-basedIintrusionIdetectionIsystemIinspectsIongoingItraffic,ImaliciousIactivities,Icommunication,IorIbehaviorIforIirregularitiesIonInetworksIorIsystemsIthatIcouldIspecifyIanIattack.ITheImainIprincipleIhereIisIthatItheIattackIbehaviorIdiffersIenoughIfromInormalIuserIbehaviorIthatIInternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013I37IitIcannotIbeIdetectedIbyIcatalogingIandIidentifyingItheIdifferencesIinvolved.IByIcreatingIsupports

ofIstandardIbehavior,Ianomaly-basedIIDSIcanIviewIwhenIcurrentIbehaviorsImoveIawayIstatisticallyIfromItheInormalIone.IThisIcapabilityIgivesItheIanomaly-basedIIDSIabilityItoIdetectInewIattacksIforIwhichItheIsignaturesIhaveInotIbeenIcreated.ITheImainIdisadvantageIofIthisImethodIisIthatIthereIisInoIclearIcutImethodIforIdefiningInormalIbehavior.ITherefore,IsuchItypeIofIIDSIcanIreportIintrusion,IevenIwhenItheIactivityIisIlegitimate.IOneIofItheImajorIproblemsIencounteredIbyIIDSIisIlargeInumberIofIfalseIpositiveIalertsIthatIisItheIalertsIthatIareImistakenlyIanalyzedInormalItrafficIasIsecurityIviolations.IAnIidealIIDSIdoesInotIproduceIfalseIorIinappropriateIalarms.IInIpractice,IsignatureIbasedIIDSIfoundItoIproduceImoreIfalseIalarmsIthanIexpected.IThisIisIdueItoItheIveryIgeneralIsignaturesIandIpoorIbuiltIinIverificationItoolItoIauthenticateItheIsuccessIofItheIattack.ITheIlargeIamountIofIfalseIpositivesIinItheIalertIlogsIgeneratesItheIcourseIofItakingIcorrectiveIactionIforItheItrueIpositives,Ii.e.Idelayed,IsuccessfulIattacks,IandIlaborIintensive.IMyIgoalIisItoIdetectInovelIattacksIbyIunauthorizedIusersIinInetworkItraffic.IIIconsiderIanIattackItoIbeInovelIifItheIvulnerabilityIisIunknownItoItheItarget'sIownerIorIadministrator,IevenIifItheIattackIisIgenerallyIknownIandIpatchesIandIdetectionItestsIareIavailable.IIImostlyIlikeItoIciteIfourItypesIofIremotelyIlaunchedIattacks:IdenialIofIserviceI(DOS),IU2R,IR2L,IandIprobes.IAIDoSIattackIisIa

typeIofIattackIinIwhichItheIunauthorizedIusersIbuildIaIcomputingIorImemoryIresourcesItooIbusyIrItooIfullItoIprovideIreasonableInetworkingIrequestsIandIhenceIdenyingIusersIaccessItoIaImachineIe.g.IpingIofIdeath,Ineptune,Iback,Ismurf,Iapache,IUDPIstorm,ImailIbombIetc.IareIallIDoS

attacks.IAIremoteItoIuserI(U2R)IattackIisIanIattackIinIwhichIaIuserIforwardsInetworkingIpacketsItoIaImachineIthroughItheIinternet,IwhichIhe/sheIdoesInotIhaveIrightIofIaccessIinIorderItoIexposeItheImachinesIvulnerabilitiesIandIexploitIprivilegesIwhichIaIlocalIuserIwouldIhaveIonItheIcomputer

e.g.Iguest,Ixlock,Ixnsnoop,IsendmailIdictionary,IphfIetc.IAIR2LIattacksIareIregardedIasItheIexploitationsIinIwhichItheIunauthorizedIusersIstartIoffIonItheIsystemIwithIaInormalIuserIaccountIandItriesItoImisuseIvulnerabilitiesIinItheIsystemIinIorderItoIachieveIsuperIuserIaccessIrightsIe.g.Ixterm,Iperl.IAIprobingIisIanIattackIinIwhichItheIhackerIscansIaImachineIorIaInetworkingIdeviceIinIorderItoIdetermineIweaknessesIorIvulnerabilitiesIthatImayIlaterIbeIexploitedIsoIasItoInegotiateItheIsystem.IThisIpracticeIisIcommonlyIusedIinIdataIminingIe.g.Iportsweep,Isaint,Imscan,InmapIetc.ITheIIntrusionIDetectionISystemI(IDS)IisIalsoIcarriedIoutIbyIimplementingIGeneticIAlgorithmI(GA)ItoIefficientlyIidentifyIvariousItypesIofInetworkIintrusions.ITheIgeneticIalgorithmI[1]IisIappliedItoIachieveIaIsetIofIclassificationIrulesIfromItheIsupport-confidenceIframework,IandInetworkIauditIdataIisIemployedIasIfitnessIfunctionItoIjudgeItheIqualityIofIeachIrule.ITheIcreatedIrulesIareIthenIusedItoIclassifyIorIdetectInetworkIintrusionsIinIaIreal-timeIframework.IUnlikeImostIavailableIGA-basedIapproachesIremainedIinItheIsystem,IbecauseIofItheIeasyIdemonstrationIofIrulesIandItheIefficientIfitnessIfunction,ItheIproposedIsystemIisIveryIsimpleItoIemployIwhileIpresentingItheIflexibilityItoIeitherIgenerallyIdetectInetworkIintrusionsIorIpreciselyIclassifyItheItypesIofIattacks.ITheInormalIandItheIabnormalIintrusiveIactivitiesIinInetworkedIcomputersIareItoughItoIforecastIasItheIboundariesIcannotIbeIwellIexplained.IThisIpredictionIprocessImayIgenerateIfalseIalarmsI[1]IinImanyIanomalyIbasedIintrusionIdetectionIsystems.IHowever,IwithItheIintroductionIofIfuzzyIlogic,ItheIfalseIalarmIrateIinIdeterminingIintrusiveIactivitiesIcanIbeIminimized;IaIsetIofIfuzzyIrulesI(noncrispIfuzzyIclassifiers)IcanIbeIemployedItoIidentifyItheInormalIandIabnormalIbehaviorIinIcomputerInetworks,IandIfuzzyIinferenceIlogicIcanIbeIappliedIoverIsuchIrulesItoIdetermineIwhenIanIintrusionIisIinIprogress.ITheImainIproblemIwithIthisIprocessIisItoImakeIgoodIfuzzyIclassifiersItoIdetectIintrusions.

InternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013I38

ItIhasIbeenIshownIbyIBaruahI[6]IthatIaIfuzzyInumberI[a,Ib,Ic]IisIconcludedIwithIreferenceItoIaImembershipIfunctionIμ(x)IremainingIwithinItheIrangeIbetweenI0IandI1,IaI≤IxI≤Ic.IFurther,IheIhasIextendedIthisIdefinitionIinItheIfollowingIway.ILetIμ1(x)IandIμ2(x)IbeItwoIfunctions,I0I≤Iμ2(x)I≤Iμ1(x)I≤I1.IHeIhasIconcludedIμ1(x)ItheIfuzzyImembershipIfunction,IandIμ2(x)IaIreferenceIfunction,IsuchIthatI(μ1(x)I–Iμ2(x))IisItheIfuzzyImembershipIvalueIforIanyIx.IFinallyIheIhasIcharacterizedIsuchIaIfuzzyInumberIbyI{x,Iμ1(x),Iμ2(x);IxI∈IΩ}.ITheIcomplementIofIμxIisIalwaysIcountedIfromItheIgroundIlevelIinIZadehian’sItheoryI[9],IwhereasIitIactuallyIcountedIfromItheIlevelIifIitIisInotIasIzeroIthatIisItheIsurfaceIvalueIisInotIalwaysIzero.IIfIotherIthanIzero,ItheIproblemIarisesIandIthenIweIhaveItoIcountItheImembershipIvalueIfromItheIsurfaceIforItheIcomplementIofIμx.IInIFigureI2,IBaruahI[6]IexplainedIthatIforIaIfuzzyInumberIAI=I[a,Ib,Ic],ItheIvalueIofImembershipIforIanyIxI∈IΩIisIspecifiedIbyIμ(x)IforIaI≤IxI≤Ic,IandIisItakenIasIzeroIotherwise.IForItheIfuzzy

numberIAC,ItheIvalueIofImembershipIforIanyIxI∈IΩIisIgivenIbyI(1I-Iμ(x))IforIaI≤IxI≤Ic,Iotherwise,IheIvalueIisI1.ITheImainIdifferenceIisIthatIforIACItheImembershipIfunctionIholdsI1IallIoverItheIplaceIwithItheIreferenceIfunctionIbeingIμ(x),IwhereasIforIAItheImembershipIfunctionIisIμ(x)IwithItheIreferenceIfunctionIbeingI0Ieverywhere.

FigureI2.IExtendedIdefinitionIofIFuzzyISetIThisIproposedIsystemIforwardedIaIdefinitionIofIcomplementIofIanIextendedIfuzzyIsetIinIwhichItheIfuzzyIreferenceIfunctionIisInotIalwaysItakenIasIzero.ITheIdefinitionIofIcomplementIofIaIfuzzyIsetIforwardedIbyIBaruahI([6],I[7]),INeogIandISutI[8]IcouldIbeIviewedIaIparticularIcaseIofIwhatIIIamIproposing.IIIwouldIuseIBaruah’sIdefinitionIofItheIcomplementIofIaInormalIfuzzyIsetIinImyIwork.

2.IINTRUSIONIDETECTIONISTRATEGIES

TheIintrusionIdetectionIstrategiesIconcernsIfourIprimaryIissues.IFirstIisItheIdatasetIthatIisIcapturedIfromInetworkIcommunications.ITheIsecondIisIGeneticIAlgorithmsI(GA)IwhichIuseImutation,Irecombination,IandIselectionIappliedItoIaIpopulationIofIindividualsIinIorderItoIevolveIiterativelyIbetterIandIbetterIsolutionsIandIaIwayItoIgenerateIfuzzyIrulesItoIcharacterizeInormalIandIabnormalIbehaviorIofInetworkIsystems.ITheIthirdIisItoIgenerateIalertsIandIreportsIforImaliciousItrafficIbehavior,IandItheIfourthIisItheImaintenanceIofItheIidsIforIobservationIofIplacementIofIsensors,IandIqualifiedItrainedIintrusionIanalystsIsoIthatItheIlatestImaliciousItrafficIisIbeingIdetectedI2.1.ITheIDatasetIToIimplementItheIalgorithmIandItoIevaluateItheIperformanceIofItheIsystem,IIIproposeItheIstandardIdatasetsIemployedIinIKDDICupI1999I“ComputerINetworkIIntrusionIDetection”Icompetition.ITheIKDDI99IintrusionIdetectionIdatasetsIdependsIonItheI1998IDARPAIproposal,IwhichIoffersIdesignersIofIintrusionIdetectionIsystemsI(IDS)IwithIaIstandardIonIwhichItoIevaluateIdifferentImethodologiesI([21],I[24]).IHence,IaIsimulationIisIbeingIpreparedIfromIaIfabricatedImilitaryInetworkIwithIthreeI‘target’ImachinesIrunningIvariousIservicesIandIoperatingIsystems.ITheyIalso

appliedIthreeIextraImachinesItoIspoofIdifferentIIPIaddressesIforIgeneratingInetworkItraffic.IAIconnectionIisIaIseriesIofITCPIpacketsIbeginningIandIendingIatIsomeIwellIdefinedIperiods,IbetweenIwhichIdataIfloodsIfromIaIsourceIIPIaddressItoIaItargetIIPIaddressIunderIsomeIwellIdefinedIprotocolI([21],I[22],I[24]).IItIresultsIinI41IfeaturesIforIeachIconnection.IFinally,IthereIremainsIaIsnifferIthatIaccountsIallInetworkItrafficIbyImeansIofItheITCPIdumpIformatI[24].ITheItotalIsimulatedIperiodIisIsevenIweeks.INormalIconnectionsIareIshapedItoIoutlineIthatIexpectedIinIaImilitaryInetworkIandIattacksIareIcategorizedIintoIoneIofIfourItypes:IUserItoIRoot;IRemoteItoILocal;IDenialIofIService;IandIProbe.ITheIKDDI99IintrusionIdetectionIbenchmarkIconsistsIofIdifferentIcomponentsI[23]:

kddcup.data;kddcup.data\_10\_percent;Ikddcup.newtestdata\_10\_percent\_unlabeled;

kddcup.testdata.unlabeled;kddcup.testdata.unlabeled\_10\_percent;Icorrected.

IIproposeItoIuseI“kddcup.data\_10\_percent”IasItrainingIdatasetIandI“corrected”IasItestingIdataset.

InIthisIcaseItheItrainingIsetIconsistsIofI494,021IrecordsIamongIwhichI97,280IareInormalIconnectionIrecords,IwhileItheItestIsetIcontainsI311,029IrecordsIamongIwhichI60,593IareInormalIconnectionIrecords.ITableI1IshowsItheIintrusionItypesIdistributionIinItheItrainingIandItheItestingIdatasets.

TableI1.IIntrusionItypesIdistributionIinIdatasets

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DATASET | NORMAL | PROB | DOS | U2R | R2L | TOTAL |
| TRAIN | 97280 | 4107 | 391458 | 52 | 1124 | 494021 |
| TEST(“Corrected”) | 60593 | 4166 | 229853 | 228 | 16189 | 311029 |

**2.2.IGeneticIalgorithm**

2.2.1.IGeneticIalgorithmIoverview

AIGeneticIAlgorithmI(GA)IisIaIprogrammingItechniqueIthatIusesIbiologicalIevolutionIasIaIproblemIsolvingIstrategyI[20].IItIisIbasedIonIDarwinian’sItheoryIofIevolutionIandIsurvivalIofIfittestItoImakeIeffectiveIaIpopulationIofIcandidateIresultInearIaIpredefinedIfitnessI[13].ITheIproposedIGAIbasedIintrusionIdetectionIsystemIholdsItwoImodulesIwhereIeachIactsIinIaIdissimilarIstage.IInItheItrainingIstage,IaIsetIofIclassificationIrulesIareIproducedIfromInetworkIauditIdataIusingItheIGAIinIanIofflineIbackground.IInItheIintrusionIdetectionIphase,ItheIgeneratedIrulesIareIemployedItoIclassifyIincomingInetworkIconnectionsIinItheIreal-timeIenvironment.IOnceItheIrulesIareIgenerated,ItheIintrusionIdetectionIsystemIbecomesIsimple,IexperiencedIandIefficientIone.IInternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI201340IGAIappliesIanIevolutionIandInaturalIselectionIthatIemploysIaIchromosome-likeIdataIstructureIandIevolveItheIchromosomesIbyImeansIofIselection,IrecombinationIandImutationIoperatorsI[13].ITheIprocessIgenerallyIstartsIwithIrandomlyIgeneratedIpopulationIofIchromosomes,IwhichIsignifyIallIpossibleIsolutionIofIaIproblemIthatIareImeasuredIcandidateIsolutions.IFromIeachIchromosomeIdifferentIpositionsIareIsetIasIbits,IcharactersIorInumbers.ITheseIpositionsIareIregardedIasIgenes.IAnIevaluationIfunctionIisIemployedItoIfindItheIdecencyIofIeachIchromosomeIaccordingItoItheIrequiredIsolution;IthisIfunctionIisIknownIasI“FitnessIFunction”.IDuringItheIprocessIofIevaluationI“Crossover”IisIappliedItoIhaveInaturalIreproductionIandI“Mutation”IisIappliedItoImutationIofIspeciesI[13].IForIsurvivalIandIcombinationItheIselectionIofIchromosomesIisIpartialItowardsItheIfittestIchromosomes.IWhenIIIuseIGAIforIsolvingIvariousIproblemsIthreeIfactorsIwillIhaveIcrucialIimpactIonItheIuseIofItheIalgorithmIandIalsoIofItheIapplicationsI[2].ITheIfactorsIareI:Ii)ItheIfitnessIfunction,Iii)ItheIrepresentationIofIindividuals,IandIiii)ItheIgeneticIalgorithmIparameters.ITheIdeterminationIofItheseIfactorsIoftenIdependsIonIimplementationIofItheIsystem.I2.2.2IFuzzyIlogicIZadehIexplainedIthatIFuzzyIlogicI[9]IisIanIextensionIofIBooleanIlogicIthatIisIoftenIusedIforIcomputer-basedIcomplexIdecisionImaking.IWhileIinIclassicalIBooleanIlogicIanIelementIcanIbeIeitherIaIfullImemberIorInon-memberIofIaIBooleanI(sometimesIcalledI”crisp”)Iset,ItheImembershipIofIanIelementItoIaIfuzzyIsetIcanIbeIanyIvalueIwithinItheIintervalI[0,I1],IallowingIalsoIpartialImembershipIofIanIelementIinIaIset.IAIfuzzyIexpertIsystemIconsistsIofIthreeIdifferentItypesIofIentities:IfuzzyIsets,IfuzzyIvariablesIandIfuzzyIrules.ITheImembershipIofIaIfuzzyIvariableIinIaIfuzzyIsetIisIdeterminedIbyIaIfunctionIthatIproducesIvaluesIwithinItheIintervalI[0,I1].ITheseIfunctionsIareIcalledImembershipIfunctions.IFuzzyIvariablesIareIdividedIintoItwoIgroups:IantecedentIvariables,IthatIareIassignedIwithItheIinputIdataIofItheIfuzzyIexpertIsystemIandIconsequentIvariables,IthatIareIassignedIwithItheIresultsIcomputedIbyItheIsystem.ITheIfuzzyIrulesIdetermineItheIlinkIbetweenItheIantecedentIandItheIconsequentIfuzzyIvariables,IandIareIoftenIdefinedIusingInaturalIlanguageIlinguisticIterms.IForIinstance,IaIfuzzyIruleIcanIbeI”ifItheItemperatureIisIcoldIandItheIwindIisIstrongIthenIwearIwarmIclothes”,IwhereItemperatureIandIwindIareIantecedentIfuzzyIvariables,IwearIisIaIconsequentIfuzzyIvariableIandIcold,IstrongIandIwarmIclothesIareIfuzzyIsets.

TheIprocessIofIaIfuzzyIsystemIhasIthreeIsteps.ITheseIstepsIareIFuzzification,IRuleIEvaluation,IandIDefuzzification.IInItheIfuzzificationIstep,ItheIinputIcrispIvaluesIareItransformedIintoIdegreesIofImembershipIinItheIfuzzyIsets.ITheIdegreeIofImembershipIofIeachIcrispIvalueIinIeachIfuzzyIsetIisIdeterminedIbyIpluggingItheIvalueIintoItheImembershipIfunctionIassociatedIwithItheIfuzzyIset.IInItheIruleIevaluationIstep,IeachIfuzzyIruleIisIassignedIwithIaIstrengthIvalue.ITheIstrengthIisIdeterminedIbyItheIdegreesIofImembershipsIofItheIcrispIinputIvaluesIinItheIfuzzyIsetsIofIantecedentIpartIofItheIfuzzyIrule.ITheIdefuzzificationIstageItransposesItheIfuzzyIoutputsIintoIcrispIvalues.ItIhasIbeenIrevealedIbyIBaruahI[6]IthatIaIfuzzyInumberI[a,Ib,Ic]IcanIbeIexplainedIwithIreferenceItoIaImembershipIfunctionIμ(x)IremainingIbetweenI0IandI1,IaI≤IxI≤Ic.IFurther,IheIhasIextendedIthisIdefinitionIinItheIfollowingIway.ILetIμ1(x)IandIμ2(x)IbeItwoIfunctions,I0I≤Iμ2(x)I≤Iμ1(x)I≤I1.HeIhasIconcludedIμ1(x)ItheIfuzzyImembershipIfunction,IandIμ2(x)IaIreferenceIfunction,IsuchIthatI(μ1(x)I–Iμ2(x))IisItheIfuzzyImembershipIvalueIforIanyIx.IFinallyIheIhasIcharacterizedIsuchIafuzzyInumberIbyI{x,Iμ1(x),Iμ2(x);IxI∈IΩ}.InternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013

41

i=1

q

i=1

p

i=1

p

i=1

q

TheIcomplementIofIμxIisIalwaysIcountedIfromItheIgroundIlevelIinIZadehian’sItheoryI[9],IwhereasIitIactuallyIcountedIfromItheIlevelIifIitIisInotIasIzeroIthatIisItheIsurfaceIvalueIisInotIalwaysIzero.IIfIotherIthanIzero,ItheIproblemIarisesIandIthenIweIhaveItoIcountItheImembershipIvalueIfromItheIsurfaceIforItheIcomplementIofIμx.IThusIIIcouldIconcludeItheIfollowingIstatementI–ComplementIofIμxI=I1IforItheIentireIlevelIMembershipIvalueIforItheIcomplementIofIμxI=I1-Iμx

IIhaveIforwardedIBaruah’sIdefinitionIofIcomplementIofIanIextendedIfuzzyIsetIwhereItheIfuzzyIreferenceIfunctionIisInotIalwaysItakenIasIzero.ITheIdefinitionIofIcomplementIofIaIfuzzyIsetIrecommendIbyIBaruahI([6],I[7]),INeogIandISutI[8]IcouldIbeIconsideredIaIparticularIcaseIofIwhatIIIamIgiving.IIIwouldIuseIBaruah’sIdefinitionIofItheIcomplementIofIaInormalIfuzzyIsetIinImyIproposedIwork.

InItheItwoIclasses’IclassificationIproblem,ItwoIclassesIareIavailableIwhereIeveryIobjectIshouldIbeIclassified.ITheseIclassesIareIcalledIpositiveI(abnormal)IandInegativeI(normal).ITheIdataIsetIemployedIbyItheIlearningIalgorithmsIholdsIaIsetIofIobjectsIwhereIeachIobjectIcontainsIn+1Iattributes.ITheIfirstInIattributesIidentifiesItheImonitoredIparametersIofItheIobjectIcharacteristicsIandItheIlastIattributeIidentifiesItheIclassIwhereItheIobjectIbelongsItoItheIclassificationIattribute.

AIfuzzyIclassifierIisIaIsetIofItwoIrulesIforIsolvingItheItwoIclasses’IclassificationIproblem,IoneIforItheInormalIclassIandIotherIforItheIabnormalIclass,IwhereItheIconditionalIpartIisIdescribedIbyImeansIofIonlyItheImonitoredIparametersIandItheIconclusionIpartIisIviewedIasIanIatomicIexpressionIforItheIclassificationIattribute.

**2.2.3IFitnessIfunction**

TheIauthorsIinI[1]IusedItheIfuzzyIconfusionImatrixItoIcalculateItheIfitnessIofIaIchromosome.IInItheIfuzzyIconfusionImatrixItheIfuzzyItruthIdegreeIofItheIconditionIrepresentedIbyItheIchromosomeIandItheIfuzzyInegationIoperatorIareIusedIdirectly.ITheIfitnessIofIaIchromosomeIfor

theIabnormalIclassIisIevaluatedIaccordingItoItheIfollowingIsetIofIequations:

TPI=IΣIpredictedI(class\_datai)

TNI=IΣ1I–IpredictedI(other\_class\_datai)

FPI=IΣIpredictedI(other\_class\_datai)

FNI=IΣI1–IpredictedI(class\_datai)

Where,

SensitivityI=ITP/(TP+FN)

SpecificityI=IFP/(IFP+ITN)

InternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013

42

LengthI=I1I–IchromosomeIlength/10

SoIfinallyIFitnessIofIaIchromosomeIisIcalculatedIasIfollowsI–

FitnessI=IW1I\*ISensitivityI+IW2I\*ISpecificityI+IW3I\*ILength

Where,

TP,ITN,IFP,IFNIareItrueIpositive,ItrueInegative,IfalseIpositive,IfalseInegativeIvalueIforItheIrule,IpIisItheInumberIofIsamplesIofItheIevolvedIclassIinItheItrainingIdataIset,IqIisItheInumberIofIsamplesIofItheIremainingIclassIinItheItrainingIdataIset,IpredictedIisItheIfuzzyIvalueIofItheIconditionalIpart

ofItheIrule,Iclass\_dataIiIisIanIelementIofItheIsubsetIofItheItrainingIsamplesIofItheIevolvedIclass,Iother\_class\_dataIiIisIanIelementIofItheIsubsetIofItheIremainingIclassesIinItheItrainingIsamples,IandIW1,IW2,IW3IareItheIassignedIweightsIforIeachIruleIcharacteristicsIrespectively.

2.3IGenerateIalertsIandIreportsITheIreportsIportraitsIanIentireIimageIofItheIstatusIofItheInetworkIunderIobservation.IItIhandlesIallItheIoutputIfromItheIsystem,IwhetherIthatIbeIanIautomatedIresponseItoItheIsuspiciousIactivity,IorIwhichIisImostIcommon,ItheInotificationIofIsomeIsecurityIofficer.IIDSsIshouldIprovideIfacilitiesIforIpractitionersItoIfine-tuneIthresholdsIforIgeneratingIalarmsIasIwellIasIfacilitiesIforIsuppressingIalarmsIselectively.IReportingIcanIdemonstrateItheIeconomicIvalueIofItheImonitoringItools.IItIcanIalsoIeaseItheIburdenIofImonitoring.ITheIIDSIshouldIgenerateIreportsIthatIhelpIpractitionersIinvestigateItheIalarms.IInIaddition,ItheIintrusionIdetectionIsystemIcanIassistInetworkIpractitionersIprioritizeItheirItasks,IbyIassigningIprioritiesItoIalarms,IorIprovidingIeachIalarmItoIaIpractitionerIforIfurther

investigation.

**2.4IIDSIMaintenance**

**2.4.1IMaintenance**

IDSImaintenanceIisIessentialIforIallIIDSItechnologiesIbecauseIallIsortsIofIthreatsIandIpreventionItechnologiesIareIconstantlyIvarying,Ipatches,Isignatures,IandIconfigurationsImustIbeImodernizedItoIensureIthatItheIlatestImaliciousItrafficIisIbeingIdetectedIandIprevented.IWeIcouldImaintainIIDSIfromIaIconsoleIusingIaIgraphicalIuserIinterfaceI(GUI),Iapplication,IorIsecureIweb-basedIinterface.

NetworkIadministratorsIcouldImonitorIIDSIcomponentsIfromItheIconsoleItoImakeIsureItheyIareIoperational,IvalidateItheyIareIworkingIproperly,IandIcarryIoutIvulnerabilityIassessmentsI(VA)IandIupdates.

**2.4.2ITuning**

ToIbeIeffectiveIinIdetectionIpolicy,IIDSImustIbeItunedIprecisely.ITuningIrequiresIvaryingIdifferentIsettingsItoIbeIinIconformityIwithItheIsecurityIguidingIprinciplesIandIobjectiveIofItheIIDSIadministrator.IScanningItechniques,Ithresholds,IandIfocusIcanIbeIregulatedItoImakeIcertainIthatIanIIDSIisImakingIoutIrelevantIdataIwithoutIoverloadingItheInetworkIadministratorIwithIwarningsIorItooImanyIfalseIpositives.ITuningIisItime-consuming,IbutIitImustIbeIperformedItoImakeIsureIanIefficientIIDSIconfiguration.IItIisItoIbeInotedIthatItuningImustIbeIspecificItoItheIIDSIproductIonly.IInternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013I43

**2.4.3IDetectionIAccuracy**

TheIaccuracyIofIintrusionIdetectionIsystemIreliesIonItheItechniqueIinIwhichIitIidentifies,IsuchIasIbyItheIruleIset.ISignature-basedIdetectionIdetectsIonlyIsimpleIandIrecognizedIattacks,IwhileIanomaly-basedIdetectionIcanIdetectImoreItypesIofIattacks,IbutIhasIaIhigherInumberIofIfalseIpositivesIratios.ITuningIisIessentialItoIreduceItheInumberIofIfalseIpositivesIandItoImakeItheIdataIfurtherIfunctional.

**3.ICHALLENGESIINIIDS**

ThereIareInumberIofIchallengesIthatIimpactIonIorganization’sIdecisionItoIuseIIDS.IInIthisIsectionIIIhaveIdescribedIaIfewIchallengesIthatItheIorganizationsIencounterIwhileIinstallingIanIintrusionIdetectionIsystem.ITheseIareIdiscussedIbelowI–

**1.IHumanIinterventionI-**IIDSItechnologyIitselfIisIexperiencingIaIlotIofIenhancements.IItIisIthereforeIveryIimportantIforIorganizationsItoIclearlyIdefineItheirIprospectIfromItheIIDSIimplementation.ITillInowIIDSItechnologyIhasInotIachievedIaIlevelIwhereIitIdoesInotIrequireIhumanIinterference.IOfIcourseItoday'sIIDSItechnologyIrecommendsIsomeIautomationIlikeIreportingItheIadministratorIinIcaseIofIdetectionIofIaImaliciousIactivity,IavoidingItheImaliciousIconnectionIforIaIconfigurableIperiodIofItime,IdynamicallyIchangingIaIrouter'sIaccessIcontrolIlistIinIorderItoIpreventIaImaliciousIconnectionIetc.IThereforeItheIsecurityIadministratorImustIinvestigateItheIattackIonceIitIisIdetectedIandIreported,IdetermineIhowIitIoccurred,IcorrectItheIproblemIandItakeInecessaryIactionItoIpreventItheIoccurrenceIofItheIsameIattackIinIfuture.

**2.IHistoricalIanalysis**I-IItIisIstillIveryIimportantIfactorItoImonitorItheIIDSIlogsIregularlyItoIcontinueIonItopIofItheIincidenceIofIevents.IMonitoringItheIlogsIonIaIdailyIbasisIis

necessaryItoIanalyzeItheIdifferentItypeIofImaliciousIactivitiesIdetectedIbyItheIIDSIoverIaIperiodIofItime.IToday'sIIDSIhasInotIyetIachievedItheIlevelIwhereIitIcanIprovideIhistoricalIanalysisIofItheIintrusiveIactivitiesIdetectedIoverIaIspanIofItime.IThisIisIstillIaImanualIactivity.IHenceIitIisIvitalIforIanIorganizationItoIhaveIaIdistinctIincidentIhandlingIandIresponseIplanIifIanIintrusionIisIdetectedIandIreportedIbyItheIIDS.IAlso,ItheIorganizationIshouldIhaveIexpertIsecurityIpersonnelItoIhandleIthisIkindIofIsituation.I3.IDeploymentI-ITheIsuccessIofIanIIDSIimplementationIdependsItoIaIlargeIdegreeIonIhowIitIhasIbeenIdeployed.IAIlotIofIplanIisInecessaryIinItheIdesignIasIwellIasItheIimplementationIphase.IInImostIcases,IitIisIrequiredItoIapplyIaIfusionIsolutionIofInetworkIbasedIandIhostIbasedIIDSItoIgainIfromIbothIcases.IInIfactIoneItechnologyIcomplementsItheIother.IHowever,IthisIdecisionIcanIdifferIfromIoneIorganizationItoIanother.IAInetworkIbasedIIDSIisIanIinstantIchoiceIforImanyIorganizationsIbecauseIofIitsIcapabilityItoImonitorImultiple

systemsIandIalsoItheItruthIthatIitIdoesInotIneedIaIsoftwareItoIbeIloadedIonIaIproductionIsystemIdifferentIfromIhostIbasedIIDS.ISomeIorganizationsIimplementIaIhybridIsolution.IOrganizationsIinstallingIhostIbasedIIDSIsolutionIneedsIrememberIthatItheIhostIbasedIIDSIsoftwareIisIprocessorIandImemory

Challenging.ISoIitIisIveryIimportantItoIhaveIsufficientIavailableIresourcesIonIaIsystemIbeforeIestablishingIaIhostIbasedIsensorIonIit.IInternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013I44

**4.ISensors**I-IItIisIimportantItoImaintainIsensorItoImanagerIratio.IThereIisInoIstrictIruleIasIsuchIforIcalculatingIthisIratio.IToIaIlargeIdegreeIitIdependsIuponIhowImanyIdifferentItypesIofItrafficIisImonitoredIbyIeachIsensorIandIinIwhichIbackground.IMostIofItheIorganizationsIdeployIaIratioIofI10:1,IwhileIsomeIorganizationsImaintainI20:1IandIsomeIothersIgoIforI15:1.IItIisIveryIimportantItoIplanItheIbaselineIstrategyIbeforeIstartingItheIIDSIimplementationIandIavoidIfalseIpositives.IAIpoorlyIconfiguredIIDSIsensorImayIpostIaIlotIofIfalseIpositiveIratiosItoItheIconsoleIandIevenIaIratioIofI10:1IorIevenIenoughIbetterIsensorsItoItheIconsoleIratioIcanIbeImissing.

**5.IFalseIpositiveIandInegativeIalarmsIrate**I–IItIisIimpossibleIforIIDSItoIbeIidealImostlyIbecauseInetworkItrafficIisIsoIcomplicated.ITheIerroneousIresultsIinIIDSIareIdividedIintoItwoItypes:IfalseIpositivesIandIfalseInegatives.IFalseIpositivesItakeIplaceIwhenItheIIDSIerroneouslyIidentifyIaIproblemIwithIbenignItraffic.IFalseInegativesIoccurIwhenIredundantItrafficIisIoverlookedIbyItheIIDS.IBothIcreateIproblemsIforIsecurityIadministratorsIorIpractitionersIandIdemandsIthatItheImaliciousIthreatsImustIbeIdetectedIpowerfully.IAIgreaterInumberIofIfalseIpositivesIareIgenerallyImoreIacceptableIbutIcanIburdenIaIsecurityIadministratorIwithIbulkyIamountsIofIdataItoIfilterIthrough.IHowever,IbecauseIitIisIunnoticed,IfalseInegativesIdoInotIprovideIaIsecurityIadministratorIaIchanceItoIcheckItheIdata.IThereforeIIDSItoIbeIimplementedIshouldIminimizeIbothIfalseIpositiveIandInegativeIalarms.

**6.ISignatureIdatabase**I-IAIcommonIpolicyIforIIDSIinIdetectingIintrusionsIisItoIrememberIsignaturesIofIknownIattacks.ITheIinherentIweakIpointsIinIrelyingIonIsignaturesIareIthatItheIsignatureIpatternsImustIbeIacknowledgedIfirst.INewIthreatsIareIoftenIunrecognizableIbyIeminentIandIpopularIIDS.ISignaturesIcanIbeImaskedIasIwell.ITheIongoingIeventIbetweenInewIattacksIandIdetectionIsystemsIhasIbeenIaIchallenge.IThereforeItheIsignatureIdatabaseImustIbeIupdatedIwheneverIaIdifferentIkindIofIattackIisIdetectedIandIrepairIforItheIsameIisIavailable.

7.IMonitorItrafficIinIlargeInetworksI-INetworkIIntrusionIDetectionISystemI(NIDS)IcomponentsIareIspottedIthroughoutIaInetwork,IbutIifInotIplacedItactically,ImanyIattacksIcanIaltogetherIavoidINIDSIsensorsIbyIpassingIthroughIalternateIwaysIinIaInetwork.IMoreover,IthoughImanyIIDSIproductsIavailableIinItheImarketIareIefficientItoIdistinguishIdifferentItypesIofIattacks,ItheyImayIfailItoIrecognizeIattacksIthatIuseImanyIattackIsources.IManyIIDSIcannotIcleverlyIcorrelateIdataIfromInumerousIsources.INewerIIDSItechnologiesImustIinfluenceIintegratedIsystemsItoIincreaseIanIoverviewIofIdistributedIintrusiveIactivity.IThereforeIIDSImustIbeIableItoIsuccessfullyImonitorItrafficIinIaIlargeInetwork.

4.IPRIORIWORKS

InIthisIsection,IIIdescribeItheIimportantIandIrelevantIresearchIworksIofIdifferentIauthorsIthatIIIhaveIcomeIacrossIduringItheIliteratureIsurveyIofImyIproposedIwork.IIIillustrateIeachIattackImannerIandIpointItoItheIimpactIofIthisIattackIandIitsIintrusiveIactivities.IFromIanIintruder’sIpointIofIview,IIIanalyzeIeachIofItheIattack’sImodes,Iintention,IbenefitsIandIsuitableIconditionsIandItryItoIfindIoutItheIsolutionIhowItoIimproveItheIattackIbyIintroducingItheIconceptIofIfuzzyIlogic-basedItechniqueIandIgeneticIalgorithm.IInternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013I45ITheInormalIandIabnormalIbehaviorsI[1]IinInetworkedIcomputersIareIhardItoIforecast,IasItheIlimitsIcannotIbeIexplainedIclearly.IThisIpredictionImethodIusuallyIgeneratesIfakeIalarmsIinImanyIanomalyIbasedIintrusionIdetectionIsystems.IInI[1]ItheIauthorsIintroducedItheIconceptIofIfuzzyIlogicItoIreduceItheIfakeIalarmIrateIinIdeterminingIintrusiveIbehavior.ITheIsetIofIfuzzyIrulesIisIappliedItoIidentifyItheInormalIandIabnormalIbehaviorIinIaIcomputerInetwork.ITheIauthorsIproposedIaItechniqueItoIgenerateIfuzzyIrulesIthatIareIableItoIdetectImaliciousIactivitiesIandIsomeIspecificIintrusions.IThisIsystemIpresentedIaInovelIapproachIforItheIpresentationIofIgeneratedIfuzzyIrulesIinIclassifyingIdifferentItypesIofIintrusions.ITheIadvantageIofItheirIproposedImechanismIisIthatItheIfuzzyIrulesIareIableItoIdetectItheImaliciousIactivities.IButItheyIfailedItoIimplementItheIrealItimeInetworkItraffic,ImoreIattributesIforItheIclassificationIrules.IInIdeterminingItheIfuzzyIrules,ItheyIusedItheIconceptIofIfuzzyImembershipIfunctionIandIreferenceIfunction,IbutItheyIsaidIthatItheImembershipIfunctionIandIreferenceIfunctionIareIsame.IInIreality,ItheseItwoIconceptsIareItotallyIdifferentIconcepts.IIIhaveIforwardedItheIextendedIdefinitionIofIfuzzyIsetIofIBaruahI([6],I[7]),INeogIandISutI[8].IInI[9]IZadehIinitiatedItheIideaIofIfuzzyIsetItheoryIandIitIwasImainlyIintendedImathematicallyItoIsignifyIuncertaintyIandIvaguenessIwithIformalizedIlogicalItoolsIforIdealingIwithItheIvaguenessIconnectedIinImanyIrealIworldIproblems.ITheImembershipIvalueItoIaIfuzzyIsetIofIanIelementIdescribesIaIfunctionIcalledImembershipIfunctionIwhereItheIuniverseIofIdiscourseIisItheIdomainIandItheIintervalIliesIinItheIrangeI[0,I1].ITheIvalueI0ImeansIthatItheIelementIisInotIaImemberIofItheIfuzzyIset;ItheIvalueI1ImeansIthatItheIelementIisIfullyIaImemberIofItheIfuzzyIset.ITheIvaluesIthatIremainIbetweenI0IandI1IdistinguishIfuzzyImembers,IwhichIconfinedItoItheIfuzzyIsetImerelyIpartially.IButItheIauthorIgaveIanIexplanationIthatItheIfuzzyImembershipIvalueIandIfuzzyImembershipIfunctionIforItheIcomplementIofIaIfuzzyIsetIareIsameIconceptsIandItheIsurfaceIvalueIisIalwaysIcountedIfromItheIgroundIlevel.IBaruahI([6],I[7]),INeogIandISutI[8]IhaveIforwardedIanIextendedIdefinitionIofIfuzzyIsetIwhich

enablesIusItoIdefineItheIcomplementIofIaIfuzzyIset.IMyIproposedIsystemIagreesIwithIthemIasIthisInewIdefinitionIsatisfiesIallItheIpropertiesIregardingItheIcomplementIofIaIfuzzyIset.IInI[2]IGong,IZulkernine,IAbolmaesumiIgaveIanIimplementationIofIgeneticIbasedIapproachItoINetworkIIntrusionIDetectionIusingIgeneticIalgorithmIandIshowedIsoftwareIimplementationItoIdetectItheImaliciousIactivities.ITheIapproachIderivedIaIsetIofIclassificationIrulesIfromInetworkIauditIdataIandIutilizesIaIsupport-confidenceIframeworkItoIjudgeItheIqualityIofIeachIrule.ITheIgeneratedIrulesIareIthenIusedIinIintrusionIdetectionIsystemItoIdetectIandItoIclassifyInetworkIintrusionsIefficientlyIinIaIreal-timeIenvironment.IBut,IsomeIlimitationsIofItheirIimplementedImethodIareIobserved.IFirst,ItheIgeneratedIrulesIwereIpartialItoItheItrainingIdataset.ISecond,IthoughItheIsupport-confidenceIframeworkIisIsimpleItoIimplementIandIprovidesIimprovedIaccuracyItoIfinalIrules,IitIrequiresItheIwholeItrainingIdatasetsItoIbeIloadedIintoImemoryIbeforeIanyIcomputation.IForIlargeItrainingIdatasets,IitIisIneitherIefficientInorIfeasible.

InI[12]IHoque,IMukitIandIBikasIpresentedIanIimplementationIofIIntrusionIDetectionISystemIbyIapplyingItheItheoryIofIgeneticIalgorithmItoIefficientlyIdetectIvariousItypesIofInetworkIintrusiveIInternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013I46Iactivities.IToIapplyIandImeasureItheIefficiencyIofItheirIsystemItheyIusedItheIstandardIKDDI99

intrusionIdetectionIbenchmarkIdatasetIandIobtainedIrealisticIdetectionIrate.IToImeasureItheIfitnessIofIaIchromosomeItheyIusedItheIstandardIdeviationIequationIwithIdistance.IButItheirIperformanceIofIdetectionIrateIwasIpoorIandItheyIfailedItoIreduceItheIfalseIpositiveIrateIinIIntrusionIDetectionISystem.

5.ICONCLUSION

InIthisIpaper,IIIhaveIdescribedIanIoverviewIofIsomeIofItheIcurrentIandIpastIintrusionIdetectionItechnologiesIwhichIareIbeingIutilizedIforItheIdetectionIofIintrusiveIactivitiesIagainstIcomputerIsystemsIorInetworks.ITheIdifferentIdetectionIchallengesIthatIaffectItheIdecisionIpolicyIofItheIIDSIemployedIinIanIorganizationIareIclearlyIoutlined.IIIproposeItoIuseItheInewIdefinitionIofItheIcomplementIofIfuzzyIsetsIwhereItheIfuzzyImembershipIvalueIandIfuzzyImembershipIfunctionIforItheIcomplementIofIaIfuzzyIsetIareItwoIdifferentIconceptsIbecauseItheIsurfaceIvalueIisInotIalwaysIcountedIfromItheIgroundIlevel.IThisInewIdefinitionIofIfuzzyIsetsIcanIclassifyIefficientIruleIsets.IThisIwouldIhelpIinIreducingItheIfalseIalarmIrateIoccurredIinIintrusionIdetectionIsystem.

ACKNOWLEDGEMENTS

IIwouldIlikeItoIextendImyIsincereIthanksIandIgratefulnessItoIH.K.IBaruah,IProfessor,IDepartmentIofIStatistics,IGauhatiIUniversity,IGuwahati,IIndiaIforIhisIkindIhelp,ImoralIsupportIandIguidanceIinIpreparingIthisIarticle.

**REFERENCES**

[1]IJ.IGomezI&ID.IDasgupta,I(2002)I“EvolvingIFuzzyIClassifiersIforIIntrusionIDetection”,IIEEE

ProceedingsIofItheIIEEEIWorkshopIonIInformationIAssurance,IUnitedIStatesIMilitaryIAcademy,

WestIPoint,INY.

[2]IR.IH.IGong,IM.IZulkernineI&IP.IAbolmaesumi,I(2005)I“AISoftwareIImplementationIofIaIGenetic

AlgorithmIBasedIApproachItoINetworkIIntrusionIDetection”,IProceedingsIofItheISixthIInternational

ConferenceIonISoftwareIEngineering,IArtificialIIntelligence,INetworkingIandIParallel/Distributed

ComputingIandIFirstIACISIInternationalIWorkshopIonISelf-AssemblingIWirelessINetworks.

[3]IT.IXia,IG.IQu,IS.IHaririI&IM.IYousif,I(2005)I“AnIEfficientINetworkIIntrusionIDetectionIMethod

BasedIonIInformationITheoryIandIGeneticIAlgorithm”,IProceedingsIofItheI24thIIEEEIInternational

PerformanceIComputingIandICommunicationsIConference,IPhoenix,IAZ,IUSA.

[4]IYao,IJ.IT.,IS.L.IZhaoI&IL.V.ISaxton,I(2005)I“AIStudyIOnIFuzzyIIntrusionIDetection”,IInIProceedings

ofItheIDataIMining,IIntrusionIDetection,IInformationIAssurance,IAndIDataINetworksISecurity,ISPIE,

Vol.I5812,IOrlando,IFlorida,IUSAI,Ipp.I23-30.

[5]IB.IAbdullah,II.IAbd-alghafar,IGoudaII.ISalamaI&IA.IAbd-alhafez,I(2009)I“PerformanceIEvaluationIof

aIGeneticIAlgorithmIBasedIApproachItoINetworkIIntrusionIDetectionISystem”,I13thIInternational

ConferenceIonIAerospaceISciencesIandIAviationITechnologyI(ASAT),IMayI26-28.

[6]IHemantaIK.IBaruah,I(2011)I“TowardsIFormingIAIFieldIOfIFuzzyISets”,IInternationalIJournalIof

Energy,IInformationIandICommunicationsI(IJEIC),IVol.I2,IIssueI1,IFebruary,Ipp.I16-20.

[7]IHemantaIK.IBaruah,I(2011)I“TheITheoryIofIFuzzyISets:IBeliefsIandIRealities”,IInternationalIJournal

ofIEnergy,IInformationIandICommunicationsI(IJEIC),IVol.I2,IIssueI2,Ipp.I1-22.

[8]ITridivIJyotiINeogI&IDushmantaIKumarISut,I(2011)I“ComplementIofIanIExtendedIFuzzyISet”,

InternationalIJournalIofIComputerIApplicationsI(IJCA),IVol.I29-No.3,ISeptember,Ipp.I39-45.

[9]IZadehILIA,I(1965)I“FuzzyISets”,IInformationIandIControl,IVol.8,Ipp.I338-353.

[10]IY.IDhanalakshmiI&IDr.II.IRameshIBabu,I(2008)I“IntrusionIDetectionIUsingIDataIMiningIAlong

FuzzyILogicIandIGeneticIAlgorithms”,IInternationalIJournalIofIComputerIScienceIandINetwork

SecurityI(IJCSNS),IVol.8,INo.2,IFebruary,Ipp.I27-32.

InternationalIJournalIofIDistributedIandIParallelISystemsI(IJDPS)IVol.4,INo.2,IMarchI2013

47

[11]IW.ILuI&II.ITraore,I(2004)I“DetectingINewIFormsIofINetworkIIntrusionIUsingIGenetic

Programming”,IComputationalIIntelligence,Ivol.I20,Ipp.I3,IBlackwellIPublishing,IMalden,Ipp.I475-

494.

[12]IMohammadISazzadulIHoque,IMd.IAbdulIMukitI&IMd.IAbuINaserIBikas,I(2012)I“AnIImplementation

ofIIntrusionIDetectionISystemIusingIGeneticIAlgorithm”,IInternationalIJournalIofINetworkISecurity

andIItsIApplicationsI(IJNSA)