ResearchonIntrusionDetectionandResponse:ASurvey

[1]MEENAKSHI PANDA, *Gandhi Institute of Excellent Technocrats, Bhubaneswar,India*
[2]RANJEET KUMAR PARIDA, *Indotech College of Engineering, Khordha, Odisha, India*

Abstract

With recent advances in network based technology andincreased dependability of our every day life on this tech-nology, assuring reliable operation of network based sys-tems is very important. During recent years, number ofattacks on networks has dramatically increased and con-sequently interest in network intrusion detection has in-creased among the researchers.This paper provides areview on current trends in intrusion detection togetherwith a study on technologies implemented by some re-searchers in this research area.Honey pots are effectivedetectiontoolstosenseattackssuchasportoremailsc an-ning activities in the network. Some features and appli-cationsofhoneypotsareexplainedinthispaper.

Keywords:Detection methods, honey pots, intrusion de-tection,networksecurity

1 Introduction

In the past two decades with the rapid progress in theInternetbasedtechnology,newapplicationareasforcom-puter network have emerged.At the same time, widespread progress in the Local Area Network (LAN) andWide Area Network (WAN) application areas in business,financial, industry, security and healthcare sectors madeus more dependent on the computer networks.All of theseapplication areas made the network an attractive targetfortheabuseandabigvulnerabilityforthecommunity .A fun to do job or a challenge to win action for somepeople became a nightmare for the others. In many casesmaliciousactsmadethisnightmaretobecomeareality. In addition to the hacking,new entities like worms,Trojans and viruses introduced more panic into the net-worked society. As the current situation is a relativelynew phenomenon, network defenses are weak. However,duetothepopularityofthecomputernetworks,their con-nectivityandourevergrowingdependencyonthem,real-ization of the threat can have devastating consequences.Securingsuchanimportantinfrastructurehasb ecomethepriorityoneresearchareaformanyresearchers.

Aim of this paper is to review the current trends inIntrusion Detection Systems (IDS) and to analyze somecurrent problems that exist in this research area. In com-parison to some mature and well settled research areas,IDS is a young field of research. However, due to its mis-sion critical nature, it has attracted significant attentiontowards itself. Density of research on this subject is con-stantly rising and everyday more researchers are engagedinthisfieldofwork.Thethreatofanewwaveofcyberor network attacksisnot justa probability that shouldbeconsidered,butitisanacceptedfactthatcanoccurat any time.The current trend for the IDS is far from areliable protective system, but instead the main idea is tomakeitpossibletodetectnovelnetworkattacks.

One of the major concerns is to make sure that in caseofanintrusionattempt,thesystemisabletodetectandtorep ort it. Once the detection is reliable, next step wouldbe to protect the network (response). In other words, theIDS system will be upgraded to an Intrusion DetectionandResponseSystem(IDRS).However, no part of theIDSiscurrentlyatafullyreliablelevel.Eventhoughresearc hers are concurrently engaged in working on bothdetection and respond sides of the system. A major prob-lemintheIDSistheguaranteefortheintrusiondetection.This is the reason why in many cases IDSs are used to-gether with a human expert.In this way, IDS is actuallyhelping the network security officer and it is not reliableenough to be trusted on its own.The reason is the in-ability of IDS systems to detect the new or altered attackpatterns. Although the latest generation of the detectiontechniques has significantly improved the detection rate,stillthereisalongwaytogo.

There are two major approaches for detecting intru-sions, signature-based and anomaly-based intrusion de-tection.Inthefirstapproach,attackpatternsorthe

behavior of the intruder is modeled (attack signature ismodeled). Here the system will signal the intrusion once amatch is detected. However, in the second approach normal behavior of the network is modeled. In this approach,the system will raise the alarm once the behavior of thenetwork does not match with its normal behavior. Thereis another Intrusion Detection (ID) approach that is calledspecification-based intrusion detection. In this approach,the normal behavior (expected behavior) of the host isspecified and consequently modeled. In this approach, asa direct price for the security, freedom of operation forthehost is limited.In this paper, these approaches willbebrieflydiscussedandcompared.

The idea of having an intruder accessing the systemwithoutevenbeingabletonoticeitistheworstnightmareforanynetworksecurityofficer.SincethecurrentIDtechnology is not accurate enough to provide a reliabledetection, heuristic methodologies can be a way out.Asfor the last line of defense, and in order to reduce thenumber of undetected intrusions, heuristic methods suchas Honey Pots (HP) can be deployed. HPs can be installedonanysystemandactastrapordecoyforaresource.

Anothermajorprobleminthisresearchareaisthespeed of detection.Computer networks have a dynamicnature in a sense that information and data within themare continuously changing. Therefore, detecting an intru-sion accurately and promptly, the system has to operatein real time. Operating in real time is not just to per-form the detection inreal time,but is to adapt to thenewdynamicsinthenetwork.RealtimeoperatingIDSis an active research area pursued by many researchers.Most of the research works are aimed to introduce themost time efficient methodologies.The goal is to makethe implemented methods suitable for the real time implementation.

From a different perspective, two approaches can beenvisaged in implementing an IDS. In this classification,IDS can be either host based or network based. In thehost based IDS, system will only protect its own local ma-chine (its host). On the other hand, in the network basedIDS, the ID process is somehow distributed along the net-work. In this approach where the agent based technologyis widely implemented, a distributed system will protectthe network as a whole.In this architecture IDS mightcontrol or monitor network firewalls, network routers ornetworkswitchesaswellastheclientmachines.

The main emphasis of this paper is on the detectionpart of the intrusion detection and response problem. Researchers have pursued different approaches or a combination of different approaches to solve this problem. Eachapproach hasits own theory and presumptions. This isso because there is no exact behavioral model for the legitimateuser,theintruderorthenetworkitself.

Rest of this paper is organized as follows: In Section2, intrusion detection methodology and related theoriesare explained.Section 3 presents the system modelingapproaches.InSection4, different trends in IDS de-signarepresented.Section5describesthefeaturese-lection/extraction methods implemented in this area.InSection 6, application of honey pots in the network se-curity will be discussed. Finally, conclusions and futureworkaregiveninSection7andSection8.

2 IntrusionDetection

The first step in securing a networked system is to detect the attack.Even if the system cannot prevent theintruderfromgettingintothesystem,noticingtheintrusion will provide the security officer with valuable infor-mation. The Intrusion Detection (ID) can be consideredtobethefirstlineofdefenseforanysecuritysystem.

2.1 ArtificialIntelligenceandIntrusionDetection

Application of the artificial intelligence is widely used forthe ID purpose.Researchers have proposed several approachesinthisregard.Someoftheresearchersaremoreinterested in applying rule based methods to detect theintrusion.Data mining using the association rule is alsoone of the approaches used by some researchers to solvethe intrusion detection problem. Researchers such as Bar-bara et al.[4, 5], Yoshido [43] and Lee et al. [30] haveusedthesemethods.

Others have proposed application of the fuzzy logicconcept into the intrusion detection problem area. Worksreported by Dickerson et al. [16], Bridges et al. [8] andBotha et al.[7] are examples of those researchers thatfollowthisapproach.Someresearchersevenusedamulti-disciplinary approach, for example, Gomez et al.[18]have combined fuzzy logic, genetic algorithm and asso-ciation rule techniques in their work. Cho [12] reports awork where fuzzy logic and Hidden Markov Model (HMM)have been deployed together to detect intrusions. In thisapproach HMM is used for the dimensionality reduction.Due to its nature, the data mining approach is widelyappreciatedinthisfieldofresearch.

SomeresearchershavetriedtousetheBayesianmethodology tosolve the intrusion detection problem.The main idea behind this approach is the unique featureof the Bayesian methodology.For a given consequence,using the probability calculations Bayesian methodologycan move back in time and find the cause of the events.This feature is suitable for finding the reason for a par-ticular anomaly in the network behavior. Using Bayesianalgorithm, system can somehow move back in time andfind the cause for the events.This algorithm is some-times used for the clustering purposes as well. Reportedworks from researchers such as Bulatovic et al.[9], Bar-bara et al. [5] and Bilodeau et al. [6] are examples of thisapproach.

Although using the Bayesian for the intrusion detectionorintruderbehaviorpredictioncanbeveryappealing ,however, there are some issues that one should be concernedaboutthem.Sincetheaccuracyofthismethod

is dependent on certain presumptions,distancing fromthose presumptions will decrease its accuracy.Usuallythese presumptions are based on the behavioral model ofthe target system. Selecting an inaccurate model maylead to an inaccurate detection system. Therefore, select-ing an accurate model is the first step towards solving theproblem. Unfortunately due to the complexity of the be-havioralmodelwithinthissystemfindingsuchamodelisa very difficult task.This paper will address the systemmodelinginthefollowingsection.

ResearcherssuchasZaneroetal. [44],Kayaciketal. [23]andLeietal.[32]findtheArtificialNeuralNetwork(ANN) approach more appealing. These researchers hadto overcome the curse of dimensionality for the complexsystems problem.A suitable method is the Kohonen'sSelfOrganizingfeaturesMap(SOM)thattheyhavepro-posed. Hu et al. [20] reports an improvement to the SOMapproachusedbyKayaciketal.[23],wheretheSupportVector Machine (SVM) method has been implemented toimprove SOM. Using SOM will significantly improve thesensitivity of the model to the population of the inputfeatures.Zanero et al.[44] use the SOM to compresspayloadofeverypacketintoonebyte.

The main goal of using the ANN approach is to provide an unsupervised classification method to overcomethe curse of dimensionality for a large number of inputfeatures. Since the system is complex and input featuresare numerous, clustering the events can be a very timeconsuming task.Using the Principle Component Analysis(PCA) or Singular Value Decomposition (SVD) methodscan be an alternative solution [2]. However, if not usedproperlybothofthesemethodscanbecomecomputationally expensive algorithms. At the same time, reducing thenumber of features will lead to a less accurate model andconsequentlyitwillreducethe detectionaccuracy.

Inthecomputernetworksintrusiondetectionproblemarea,the sizeofthefeaturespaceisobviouslyverylarge.Oncethedimensionsofthefeaturespacearemultipliedbythenumberofsamplesinthefeaturespace,there-sultwillsurelypresentaverylargenumber.Thisiswhysomeresearcherseitherselecta smallsamplingtimewin-doworreducethedimensionalityofthefeaturespace.Sincethe processingtimeisanimportantfactorinthetimelydetectionoftheintrusion,theefficiencyofthede-ployed algorithmsisveryimportant.Timeconstraint maysometimesforceustohavethelessimportantfeaturesprun-ed(dimensionalityreduction).However,theprun-ingapproach isnotalways possible.Implementingdataminingmethodology,some researchers have proposed newdatareductionapproaches.Datacompressioncanbeconsidered to be an alternative approach to solve the high dimensionalityproblem.Generationofassociationrulesasitwasproposedby Leeetal.[30,31]isanalternativetoreducethesizeoftheinputdata(Rulebasedapproach).Sizeanddimensionalityofthefeaturespacearetwomajorproblemsin IDSdevelopment.Atthesametime,methodssuchasBayesianandHMMthatusestatisticalorprobabilitycalculationscanbeverytimeconsuming.

Besidesthedimensionalityreductionorthedatacompres-sion methods, there are two other methods that can dealwith the problem of computation time.These methodsareexplainedinthefollowingsubsections.

2.2 EmbeddedProgrammingandIntrusionDetection

One approach is to preprocess the network information using a preprocessor hardware (front-end processor). In thismethodsomepartsoftheprocessingisperformedpriortothe IDS. This preprocess will significantly reduce the processingloadontheIDSandconsequentlythemainCPU.Otey et al. [37] have reported a similar work by programming the Network Interface Card (NIC). This approachcan have many properties including lower computationaltrafficandhigherperformanceforthemainprocessor.Im-plementing this approach will make it easier to detect va-riety of attacks such as Denial of Service (DoS) attack.This is because the NIC is performing the major part oftheprocessingwhilethemainprocessoronlymonitorstheNICoperation.

2.3 AgentBasedIntrusionDetection

Thesecondapproachisthedistributedortheagentbasedcomputing.Inthisapproach notonly the workload willbedividedbetweentheindividualprocessors,butalsotheIDSwillbeabletoobtainanoverallknowledgeofthenetworksworkingcondition.Havinganoverallviewofthenetworkwillhelptheids todetectttheintrusionmoreaccurately and atthesame timeitcanrespondtothe threatsmoreeffectively.In thisapproach,serverscancommunicatewithoneanotherandcanalarmeachother.Inorder torespondtoan attack,sometimesitcanbesufficientenoughtodisconnectasubnet.Inthistypeofsysteminordertocontainathreat,thedistributedIDScanordersevers,routersornetworkswitchestodisconnectahostorasubnet.Oneoftheconcernswiththistypeofsystemistheextraworkloadthattheidswillenforceonthenetworkinfrastructure.Thecommunicationbetweenthedifferenthostsandserversinthenetworkcanproduceasignificanttrafficinthenetwork.Thedistributedapproachcanincreasetheworkloadofthenetworklayerswithinthehostsorserversandconsequently itmayslowthemdown.

There are two approaches in implementing an agentbased technology. In the first approach, autonomous dis-tributed agents are used to both monitor the system andcommunicate with other agents in the network. A Multi-agent based system will enjoy a better perception of theworldsurrounding it.Zhangetal.[46]reportimplementing a multi-agent based IDS where they have considered four types of agents:Basic agent, Coordinationagent, Global Coordination agent, Interface agents. Eachone of these agents performs a different task and has itsownsubcategories.Forexample,thebasicagentincludes:

Workstation agents, Network segment agents and Public server agents.These subcategory agents respectivelyworkonthe workstationsofthe network,aswellas,thesubnet level and public server level (Mail agent or FTPagent). In this way, the complex system with breakdownintomuchsimplersystemsandwillbecomeeasiertoman-age.

Inthesecondapproach,mobileagentsareusedtotravel through the network and collect information or toperform some tasks.Foo et al.[17] report an IDS de-velopment work [15] using mobile agents.They use theMitsubishi'sConcordia platform in their work to developa mobile agent based IDS. Using the mobile agent, theirIDSperforms boththeportscanningandtheintegritychecks on the critical files of the system.The proposedagent based IDS will raise the alarm if it detects any alter-ation on the critical files of the system. Mobile agents canbe sent to other systems to monitor health of the targetsystemandtocollectinformation.

Luo et al.[33] introduce a new Mobile Agent Distributed IDS (MADIDS). Authors address number of deficiencies that exist in distributed IDSs: "The overload of data transmission", "The computation bottleneck of thecentral processing module" and "The delay of networktransmission". Paper reports that one of the main goalsof the system is to improve the performance of the IDSinregardtospeedandnetworktraffic.

In a work reported by Ramachandran et al.[38] theidea of neighborhood-watch is implemented for the net-work security. There are three different types of agents in three different layers.All the agents are defined inPERL(PracticalExtractionand Report Language). Inthe front line (bottom layer) there is a Cop agent that isa mobile agent. There are different types of Cop agentsdependent on their assignments. A Cop agent is respon-sible for collecting data from various sites and reportingthem to its respective detective agent.In this system,each site will store all the important security informationabout its neighbors. This information includes checksumof critical data files and system binaries, etc. It will alsostore a list of its neighbors in the neighborhood. Thereare neighbors (hosts) within each neighborhood (subnet)whom can be inspected by the mobile agents called Cops.By voting among themselves, neighbors will decide on thecourse of action they intend to follow. This concept willbediscussedinmoredetailinthefollowingsections.

2.4 SoftwareEngineeringandIntrusionDetection

As the complexity of the IDS increases, the problem ofdeveloping the IDS becomes more and more difficult.Aprogramming language dedicated to developing IDSs canbe useful for the developer community. Such a program-ming language with its special components will improvethe programming standard for the IDS code.IDS devel-opers can enjoy the benefits of a new language dedicatedtotheIDSdevelopment.Suchalanguagewillimprove both the programming speed and the quality of the finalcode.

In a paper by Vigna et al.[41] the main attention isfocused on the software engineering aspect of the IDS.Issues such as object-oriented programming, componentreusability and the programming language for the IDS arediscussed in this paper.A new framework called StateTransition Analysis Technique (STAT) is introduced inthispaper.Intheirimplementedframework,Vignaetal.[41]proposeatypeofstatemachinesystemcalledSTATthat follows the state transition of the attack patterns.This framework is for developing signature based IDSs(The concept of the signature based IDS will be discussedlater in this paper). There is a STAT-Response class thatholds response modules. These response modules includelibraryofactionsthatareassociatedwiththepattern of the attack scenarios.All together, this language willproduceanencapsulatedobject-orientedcodewithahighreusability in the code. There is an event provider modulethat will provide the framework with the events occurringonthenetwork.

Another approach in programming languages for theIDS is to provide means to follow the state change inthe system. In this way, the IDS will have the ability tohave its behavior altered if necessary. Including this feature intheIDSwillmakeitadaptiveandreconfigurable.Possibility to alter the behavior of the IDS will provideus with a dynamically reconfigurable IDS. In a reportedwork, Sekar et al. [39] have implemented a *State MachineLanguage (SML)* approach based on the *Extended FiniteState Automata (EFSA)* to model the correct or expectedbehavior of the network. Using a well designed programin SML, the state machine will be able to follow up withtheeventswithinthenetworkandtoproduceappropriateoutputs. If no irregularities detected, then the anomalydetection part of the process will analyze the outputs andwilldetecttheanomalies.

TherearetwoapproachesinimplementinganIDS.Inthe first approach, IDS is implemented in the form ofsoftware that is deployed on a server or a host.In thisapproach the final produce is not a physical object butit is software.In the second approach the IDS is builtas a product with its own hardware platform (IDS appli-ance). In this type of IDS, once the product is installedon the network it will connect itself to the network andwillstartmonitoringandanalyzingthenetwork.IDScan perform its duties in a way transparent to the network.Such approaches could help the IDS to perform the in-trusion detection in a more successful and non-intrusiveway. At the same time, this type of products are easierto install and will introduce minimum overhead on thenetwork.Thus,theirpricemightbehigher.

2.5 SomeSelectedPapers

This section will describe selected papers in different researchareasoftheIDStechnology.

2.5.1 Bayesian(Statistical)Approach

AsanexamplefortheimplementationoftheBayesianmethodinIDS,Barbaraetal.[5]reportaworkonthesubjectofintrusiondetectionfortheanomalydetection.Authorsreportsimilarcategories(misuseandanomalydetectionforintrusiondetection),theyalsoreportthesamefeaturesforthesetwomethodologies.Inordertobeabletohandleunknownattackstheyhaveselectedtheanomalydetectionmethod.Theiraimistoimprovethedetectionandfalsealarmratesgeneratedbythesystem. Their report indicates that this work is the continuationofanongoingresearchbasedon“ananomalydetectionsystem called Audit Data Analysis and Mining” (ADAM).Theirapproachismainlydataminingorientedbut inthispaperthereportedworkisrelatedtothepseudo-Bayesestimators. The application for these estimators is to estimatetheprioriandposterioriprobabilitiesofnewattacks.Inthiswork,Naive-Bayesianclassifier isusedtoclassifynetworkinstances.Theyalsoclaimthatdue totheprop-erties of the pseudo-Bayes estimators, system won’t needany priori knowledge regarding thenewattack patterns.ADAMconsistsofthreeparts.Partoneisthepreprocessoranditsjobistocollectdatafromthe TCP/IPtraffic data(networksniffer).Thesecondpartisthedatamining engine that extracts association rules from the collecteddata.Dataminingenginesmainjobistosearchforunexpectedbehaviors.ADAMworksintwomodes:Trainingand detectionmodes.Thelastpartofthesystemistheclassificationengineanditstaskistoclassifytheassociation rules intotwo classes:Normal and abnormal.Abnormalclassescanbelaterlinkedtosome attacks.

Authors report two main advantages for the system,first the ability to work in real time (online data miningoperation) and then the strategy of anomaly detection ofthe system.In their system, rules depict behavior mod-els.These rules are saved in a database and constantlymonitored. If a rule is a new rule and not yet registered inthe database (anomaly) and its occurrences have reachedto a threshold value, then it will be labeled by the systemas a suspicious event.The mining engine works in threelevels:singlelevel,domainlevelandfeaturelevel.

Single level mining engine works in two different modes:static mining and dynamic mining. The first one is forthe normal operation time of the system when a profile ismade for the system behavior.The second one however“uses a sliding window method that implements incre-mental,on-lineassociatedrulemining”[5].

In the domain level mining engine, the source and destination IPs are monitored. The reported system may findit suspicious if both the source and destination IP’s comefrom the same subnet. In the feature selection engine, awindowing technique is implemented to record instancesof the network (every window is 3 seconds wide). In thisway,systemcollectssnapshotsfromthenetworkbehavior andthenanalyzesthem.

Thereisalsoasecondslowersamplingratethatisevery 24 hours to detect the slow occurring but long lastinganomalies.Then the system will apply the domain levelmining methods on them to capture the rules and extractfeatures.In the reported work, a selected number of at-tributes in the training data were reported to characterizeclasses.These classes reflect properties resulted duringdifferent levels of the data mining.Classifier is trainedusing thetraining data andlater on is testedusing thetestdata.

Inthereportedwork,apseudoBayesianclassifierisusedforthe classification.Theestimationpartofthisclassifier has the smoothing feature. The pseudo Bayesianestimatorisapopularmethodindiscretemultivariate analysis.Inthereportedwork,Barbaraetal.[5]useDirichletdistributionprobabilitydensityfunctionasthekernelofthe likelihood function. This method is usedtoestimatecellvaluesforthetableswithlargenumberofsamplingzeros.Inthesetables,itmayalsohappenthatduetorepeatedsampling,somecellsshowmoreze-ros thantheothers(densityofzeros)andthisiswhentheDirichletmethodwillhelpus.Thefinalstage ofclassificationiscarriedoutusingtheNaiveBayesianclassification.One ofthemostinterestingparts ofthisresearchistheuseofNaiveBayesianclassifier.Inthedescriptionoftheclassifier,Barbaraetal.haveusedtheDirichletdistri-butiontoobtaintheprobabilitydensityfunctionfortheclassifier.Dirichletdistribution[6]isagoodchoiceforthistypeofproblem.DirichletdistributionandGammadistributionaretimerelated.Forexample,Gammadis-tribution [6] will give an estimate for the time one have towait(“waitingtimeinaPoissonprocess”[6])beforegettingatleast$n$successes.Bilodeauetal.intheirbook[6]proposedthefollowingformulafortheprobabilitydensity functionusingGammaestimation:

$$f_n(t)=\lambda e^{-\lambda t}(\lambda t)^{n-1}/(n-1)!, t>0 \quad (1)$$

In comparison to the Gamma distribution, Bilodeau et al.in their book [6] have described the Dirichlet distributionas “simply the proportion of time waited”.*Analysis*:Astime and its effects on the outcomes of any IDS is subjectto a great importance in intrusion detection, addressingthis issue gives a big advantage to this paper. The conceptis very much into the linear algebra’s subject area andneeds further study.At the same time by looking at theformulas presented in either [5] or [6] reader can expect ahigh computation processing load for performing multiplemultiplications (unless we can somehow go around thisproblem).

There is still one question that remains to be answeredand thatis:“Can onebe sure that input parameters toan IDS are independent from one another?”Dependenton the answer that might be yes or no, the method of ap-proach can be different. We are doubtful about taking theparameters as independent (or conditional independent)parameters. This is because they serve the same purposethat is intrusion.However,on the contrary it can notnecessarily mean that they are not dependent either, be-causenotallof the activitiesin the networkareintrusions

and most of them are random legitimate activities. Fromour point of view, this subject deserves more study. Thisis so because during the design stage understanding thestatistical nature of these events will help us to build theoptimummodelofthesystem.

Barbara et al.[5] in their paper, present results us-ing two configurations: In the first configuration, giventraining data after Naive-Bayesian Classifier detected theintrusion, system will remove it from the DARPA 1998training data and then will apply the classifier on theDARPA 1999 test data. In the second approach however,theDARPA1999trainingdatais selectedwiththe sametestdata(DARPA1999).Thenboththetestandtrainingdata are introduced to the Naive Bayesian classifier andthe outcome is analyzed (using the test data). The presentedresultsaresatisfactorybutalthoughtheypresentagood research work, there is a concern with regard to thetestenvironment.TheproblemariseswhenBarbaraetal. [5]say:"To better evaluate the performance of pseudo-Bayes estimator, we pick a set of attacks that behavevery differently, while for the attacks that share somesimilarities,weonlyselectonecandidatestorepresentth erest".Intheirconclusionstheyalsotalkabouttheprob-lem of detecting attacks similar in nature (*Analysis*: canwe translate this to: dependent input variables?). *Analysis*:The presented results confirmed our ambitions re-gardingthechoiceofassuminginputparametersfromthenetwork as either independent or dependent parameters!Since a random variable version of the Bayes estimator isimplemented in their work and due to the following twoassumptionsinthismethod:

1) ThemultinomialdistributionassumptionintheBayesestimator.

2) TheassumptionfortheNaiveBayesianisthattheparametersareconditionalindependent.

Once the behavior of the anomalies is similar, the proposed classifier will misclassify the attacks as it is evidentin the reported results. Nevertheless this paper presentsagoodresearchworkinintrusiondetection.

2.5.2 FuzzyLogicApproach

As an example for the fuzzy logic based approach, Dick-erson et al. [16] report a research based on the fuzzy logicconcept.The paper reports a Fuzzy Intrusion RecognitionEngine (FIRE) for detecting malicious intrusion activi-ties. In the reported work, the anomaly based IntrusionDetection System (IDS) is implemented using both thefuzzy logic and the data mining techniques.The fuzzylogic part of the system is mainly responsible for bothhandling the large number of input parameters and deal-ing withtheinexactness oftheinputdata.

In the reported work, a Network Data Collection(NDC) module is implemented to take samples from thenetwork (using TCP packet data) with 15 minutes inter-vals.NDCis akindofnetworkdatasnifferandrecorder system that is responsible for reading packets off the wireandstoringthemonthedisk.Thesamplesizeissolarget hat authors were forced to use data mining technique tocreate an aggregated key composed of IP source, IP desti-nation and destination port fields to reduce the data size.Inthiswork,systemtracksthestatisticalvarianceofthe packet counts searching for any unusual increases in theirnumber. Once any unusual increase is detected, it meansthat someone is scanning the network with small numberofpackets.

There are three fuzzy characteristics used in this work:COUNT,UNIQUENESSandVARIANCE.Theimple-mentedfuzzyinferenceengineusesfivefuzzysetsforeachdata element(LOW,MEDIUM-LOW,MEDIUM,MEDIUM-HIGHandHIGH) and appropriate fuzzy rulesto detect the intrusion.In their report, authors do notindicate that how did they derive their fuzzy set. Thefuzzy set is a very important issue for the fuzzy inferenceengine and in some cases genetic algorithm approach canbe implemented to select the best combination. The pro-posed system is tested using data collected from the localarea network in the college of Engineering at Iowa StateUniversity and results are reported in this paper. The re-portedresultsaredescriptiveandnotnumericalthereforeit is difficult to evaluate the performance of the reportedwork.

Gomez et al.[18] report a work based on the fuzzylogic concept. This work is dedicated to the network in-trusion detection problem. The dataset for this work isKDD-cup'99 and 1998 DARPA datasets. In this work,theGeneticAlgorithm(GA)isusedtooptimizethefuzzyrules so that they can better fit to the purpose. In this ap-proach, fuzzy sets are normalized to fit within the bound-aryof0.0to1.0.

Thefitnessvaluefor theGAiscalculated usingtheconfidence weights of the system.This process is verysimilar to the way uncertainty problem is handled in theexpert systems. Later on in their paper, a comparison hasbeen made between the rules for the normal and abnormalbehavior (there are two main sets of rules in the system,oneisforthenormalandtheotheroneisfortheabnormalbehaviors).

In a graph presented in this paper, the false alarm rateand the detection rate of the system were input parame-ters and three curves for Normal rule, Abnormal rule andNormal-Abnormal rules (one with the confidence a andthe other one with $1 - a$) were plotted.The graph wasshowingahigherdetectionandlowerfalsealarmrates for using only abnormal fuzzy rules.The system wastested using only 1% of the original 1998 DARPA datasetswhere10.63%falsealarmsand95.47%detectionrate wasreported. Authors mention that this abstraction is pos-sible since the normalization process will produce a uni-formdistribution.*Analysis*:Selectingthe1%ratiooftheWhole dataset for the training can be an indication thathigh computationalpowerisrequiredforthistask.

In another reported work in this area, Botha et al.reportawork[7]todetecttheintrusionusingtheuser

behavior andthefuzzylogic methodology. In this pa-per, intrusion detection algorithms are similar to the twoearlier approaches introduced inprevious papers.Theoverall viewof theauthorsistoconsidersixdifferentgeneric phases for an intrusion into a network. The goalof this system is to track and monitor the current state ofthe user's behavioral profile considering these categories.Thesesixphasesare:

1) Probing phase. Intruder collects information regard-ing the operating system, firewall and the user pro-file.Knowing this information will narrow intruder'soptions in finding the weaknesses within the system(Probingcommandandillegalfirewallaccess).

2) Gaininginitial access phase. This phase includesthe following parameters: Invalid password attempt,user terminal (network address) and user networkinghours.

3) Gaining full system access.In this phase the fol-lowing activities will be encountered:Illegal pass-word file access attempt, illegal file/directory accessattempt,illegalapplicationaccess.

4) Performing the hacking attempt.In this phase in-truderisgoingtousesystemfacilitiesandinforma-

tion (Intruder'saction).

5) Covering hacking tracks. Here the intruder will eraseall the track or clues leading to the exposure of hisaccessroutesandidentity(Auditlogaccess).

6) Modifying utilities to ensure future access.In thisphase, the intruder will create a backdoor in the sys-temforhimselftouseitforhisfutureaccess(Creat-inguseraccount).

In this paper, it is assumed (authors reason was thelack of data) that the model for the transition from onestate to the other is linear. In other words, if anyone failsto access the system out of the regular working hours,thenIDSwillbe33.3%certainthat this was an intru-sion attempt.There is a separate membership functionassigned to each one of the inputs to the system. Prede-finedrulestogetherwithoutputfromtheaforementionedfunct ions are used by the fuzzy inference engine for de-riving conclusions.Results reported using only 12 testsubjectsthatlookstobeasmallnumberoftestcases.

2.5.3 DataMiningApproach

Inthedataminingapproach,Lee et al. [31] report awork based on data mining concept where initially twomain usual classes of IDS are described and compared.Later, authors have explained their way of solving prob-lemswiththesystemandbringingituptowhereitisnow.Their approach is a rule-based approach (using machinelearning techniques). In their proposed system, anomaliesaredetectedusingpredefinedrules.However,thesy stem supervisor should know the behavior pattern for a cer-tain anomaly in order to be able to update the systemwith the appropriate rules.This is how the system be-comes adaptive.Authors have designed, implemented andtested several rule sets for various attack patterns. Therule generation methodology implemented in this work isinteresting.They define an association rule (item set)with the following generic form: $X \rightarrow Y, c, s$ where X and $Y$are the item sets for the rule and $X \cap Y = \emptyset$ istherelationbetweenthem.s=$support(X \cup Y)$wheresis the support value for the rule and $c = \frac{support(X \cup Y)}{support(X)}$is theconfidence for the rule.System keeps these rules for aperiod of time and uses them as the pattern for the eventand behavior model for the users. As an example, Lee etal.[30,31]say:

"an association rule for the shell command history file(whichisastreamofcommandandtheirarguments)ofa user is:$trn \rightarrow rec.humor$, 0.3, 0.1, which indicates that30% of the time when user invokes *trn*, he or she is readingthe news in *rec.humor*, and reading this newsgroup ac-counts for 10% activities recorded in his or her commandhistoryfile."

Thereisanother rule called frequent episode rule:$X, Y \rightarrow Z, c, s, window$ where X and Y are the item setsfortheruleand$X \cap Y = \emptyset$istherelationbetweenthem. s=$support(X \cup Y \cup Z)$wheresisthesupportvaluefor theruleandc=$\frac{support(X \cup Y \cup Z)}{support(X \cup Y)}$ istheconfidenceforthe ruleand*window*isthesamplingwindowinterval.

Analysis:Theirideafortrackinguserssoundsveryin-teresting.Asitisexplainedinthepaper,applyingpropersubi ntervals, system will reduce the length of the userrecords. At the same time, system will keep the historicalrecords for the activities in its database (data reduction).Using the user records, system will generate a rule set forthe activities within the network. At this stage, systemcan notice the irregularities and identify them (if they areknown).Severaltestscenarioswherepresented.

Since for the test purposes no standard datasets suchas DARPA was used, it is hard to evaluate and compareitheir results. However, the proposed rule based approachisimplementedinagoodway.

There is an abstraction on the anomaly detection con-cept in their reported work. In the report [30] authorssay: "Anomaly detection is about establishing the nor-malusagepatternsfromtheauditdata".

Their viewpoint seems to be the following: Anomalydetection is to detect any known anomaly (or a famousanomaly pattern) in the network. However, we are notnecessarilyagreedwiththemontheknownanomalyorth esignaturebasedapproachandwouldrathertouseanyautomat icallydetectedintrusiveanomalydetectionapproach.

Adaptability of their reported system requiresthatsomeonealwayskeepthesystemrulesetsuptodat e.It could be a big challenge to include an automated adap-tationfeatureintheIDS.

Lee et al.in another paper [28] report a work to im-prove andcontinuetheirearlierworkinthefieldofintru-

sion detection.In their new approach, they have imple-mented their system in a distributed configuration.Thiswill help them to break down their workload and per-form a type of parallel processing.In this way, they canalso perform sophisticated tasks and implement compli-cated algorithms.Analyzing their work and consideringtheir background in rule based approach; one can easilyget the idea of the "Black Board" strategy as it is in theexpertsystems,outoftheirwork.

They have also indicated that they are very much in-terested in "Black Box" modeling of the system. Thisisagreatideaandhonestlyspeakingthisistheideainour minds as well.This is because attacks are not in astatic model and every now and then a novel attack pat-tern emerges. A black box approach to this problem willprovide the IDS with the ability to detect the intrusionwithoutnecessarilyknowingitstype/categoryorna me.

Leeetal.[28]notedintheirreportthat

"A major design goal of CIDFis that IDAR systemscan be treated as "black boxes" that produce and con-sume intrusion-related information".Where CIDF andIDAR respectively stand for "Common Intrusion Detec-tion Framework" and "Intrusion Detection Analysis andResponse".

Considering the above, they have also noted in the ear-lier parts of their report that: "we need to first selectand construct the right set of system features that maycontain evidence (indicators) of normal or intrusions.Infact, feature selection/construction is the most challeng-ing problem in building IDS, regardless the developmentapproach in use."[28] that is a very true statement and itis important to find right features. There are some issuestobringupinthisregard.Theseissueswillbediscussedin thefollowing.

In the experiments section of the reported work, au-thors report an experiment where in a simulated SYNflood attack the IDS has not only detected the attackbut has sent agents to the slave computers (those whowhere attacking the network or the server) to successfullykill the malicious agents there. The idea seems fine, butwhat about the legal and privacy issues?Is it legal tosendagentstopeople'scomputerswithouttheirconsent?Th ere should be a legal solution to the privacy problembefore implementing such strategies.This approach canbe feasible for the network of an organization, but notovertheinternet.

*Analysis:*Thisapproachseemsreasonablebuttherearesomeissu esthatneedtobeaddressed:

1) The reported work is heavily counting on the con-nectivity or the availability of the network structurefor their work.In some occasions,this cannot beexpected.This is because in some DOS attacks notthe server but the network switches might becomesaturated, which means that there will be no meansby which these distributed systems can communicatewithoneanother.

2) Thefeaturedetectionparthastobeautomated,this is because different attack strategies may have dif-ferent features and in an adaptive system feature ex-traction has to be automated.However, authors intheir implementation part of the report still reportthathumaninspectionisrequiredintheirsystem.

3) We believe in the Black Box (BB) approach for thistypeof problems. It is also evident that model-ing such ahuge and complicated system needs bothagreat computational powerand alarge memoryspace. Nevertheless, one has to accept the fact thatsome times cost is high! The question is not the costbut on the other hand, it is about the possibility. Inmany occasions, learning speed in BB modeling is soslow that it is practically impossible to use it in thereal world applications.However, if possible to im-plement, a BB model can never tell you how or whythissituationisanattack!Itjustknowsthatthisisanattack(s eemslikeoneorbehaveslikeone)!

No numerical results are presented in this report. Justthe experimental environment and the experiments weredescribed.

2.5.4 DifferentTendsinDataMiningApproach

InanothergroupofthefuzzylogicandGeneticAlgo-rithms (GA) related papers that are related to IDS con-cept,theonetostart withis a work from Bridges et al.[8]. They report a work where fuzzy logic is used to modelthe uncertainties in the network behavior. The GA's rolehere is to optimize the membership functions of the fuzzylogic engine.Authors also report that they have imple-mented standard S, PI, and Z functions in their work aswell.This will make themembership function tolookdifferent from just some overlapped triangles.Here, thetriangles will turn into half sine waves. Their approach isan anomaly-based approach.They are using expert sys-tems and their approach is rule-based.Association rulesand their corresponding confidence and support factorsare also implemented in the system. Their reported resultshows that by tuning fuzzy logics membership function,GA's optimization process is improving the performanceof the IDS (improves its feature extraction capabilities).Inthereportedpaper,fuzzyresultswerecompare dversusresults from a non-fuzzy system using a diagram. The de-picted diagram indicates less false positive error rate forthe fuzzy based methodology. The method is well definedand as it is indicated in the paper, the work is an ongoingworkandneedsfurtherfollowup.

InanotherreportedworkbyBarbaraetal.[4]reportsthesame workasitispreviouslymentionedinthisreport [5]and reports other researchers approaches in this area.He is not satisfied with the quality of the result reportedby Lee et al. [30]. However, two papers from Lee et al.are referenced in their paper.Regarding the weaknessesof their own method, they reason that it is due to inac-curate thresholds in their classification system.Authorsaresuggestingthatinordertoimprovetheaccu racyand

the detection rate for the proposed system, one way canbe to add more sensors to the system. This idea is sim-ilar totheone in the control systems area of research(so called multi-sensor data fusion). In their future work,authors goal is to avoid the dependency on the trainingdata(probably because it is very difficult to obtain suchadataset)forthenormalevents.

As it is evident in this last set of reported works, thefuzzy logic or Bayesian estimator based works can be in-cluded under either their own name or under the datamining category name.This is because the data miningworkareaisamulti-disciplinaryareaofresearch.

Yoshida [43] inhis paper reports a new approach tothe IDS design.In this paper, the author indicates thathis/her goal is to provide system with the ability to de-tect newly encountered attacks.However, this claim inthe paper is not supported by the experimental results.Yoshida's report is mainly descriptive and it talks aboutthe new approach without showing any proof of its per-formance.

Yoshido explains that application of the APRIORI al-gorithm that mines the association rules from the givendataset is most popular among the researchers in datamining research area.Yoshido also believes that "theresult of APRIORI algorithm involves association ruleswith contradiction"[43]. He also indicates that the resultofthisalgorithmisnoisyandinordertouseitwithinanIDS, the result needs post-processing. As for his proof, heprovides an example where in a given database there aretwo rules such that: Rule X has 100 supporting and 200contractingdataitemsinthedatabaseandruleYwhichh as 99 supporting and no contracting data items. GivenMinSup (Minimum support) value equal to 100, APRI-ORI algorithm will only find the rule X. If it is desired tohavetheYruleaswell,thentheMinSupvalueshouldbedecreasedwhichinturnwillleadtoahighernoiseintheresult. In order to improve the results, Yoshido proposesa Graph Based Induction (GBI) approach using Entropybaseddatamining.TheGBIalgorithmisasfollows: Firstthe input graph is contracted. Here "Every occurrence ofthe extracted sub-graph in the input graph is replacedby a single node in step 1"[43]. In the second step, thecontracted graph is analyzed and consequently every sub-graph consisting of two linked nodes that are called a pairis extracted. Finally satisfying a certain criteria the bestpair is selected. Later on "The selected pair is expandedto the original graph, and added to the set of extractedsub-graphs"[43]. For calculation of the Entropy he usesthefollowingformulas.

$$Informationgain(D,T) = Entropy(D) - \sum_{G_i \epsilon G} \frac{|G_i|}{|D|} Entropy(G_i) \quad (2$$

WhereTisthenewtestdatasetandDistheoriginaldatasetthatis goingtobeclassified.TheEntropycanbe calculatedusingthefollowingformula:

$$Entropy(D) = \sum_{i=1} -p_i \log_2 p_i \quad (3)$$

The $G_i$is a subset of D classified by the test T and $p_i$istheprobabilityofclass$i$.

Cabrera et al. [11] report a work in continuationof theirearlier work [10] where thefeasibility of theirapproachwasstudied.Authors use the Simple Network Management Protocol (SNMP) to build an IDS system.Theyseparate theirapproach from thecommonapproachesinthenetworksecurityareabysaying: "IDSseitherrelyon audit records collected fromhosts (host-based IDSs) or on raw packet traffic collectedfrom the communication medium (network-based IDSs).SNMP-based NMSs on the other hand rely on MIB vari-ablestosettrapsandperformpolling"[10]. Later,paperexplainsthatalthoughthesetwoapproachesdonothavemuchincommon,SNMP-basedNetwork Management Systems (NMS) relying on the Management Information Base (MIB) variables can help theIDStoset traps and perform polling. This will enableustodesignadistributedIDS. Authors intention is touseMIB variables toimprove thedetection rate of theIDS especially for those attacks that are difficult to detect.A SNMP-friendly IDScanuse the MIB to cover awide spectrum of security violations.They also believethat "MIB variables can be used not only to character-ize security violations, but also to characterize precursorsto security violations"[10].Authors say that the idea ofproactive IDS is about predicting the intrusion attack be-foreitactuallyreachestoitsfinalstage.

Cabrera et al. mainly focus on the Distributed DenialOf Service (DDOS) attack. In this type of attack, initiallya master node will install a slave program in the targetclients of thenetwork.Then after awhile it orders themtostart theattack by sending a message to them. Inthissystem,slaveswillgenerateanartificialtrafficbywhich they will cause network congestion and will bringthe network into halt.Cabrera et al.have characterizedtheirproposedsystemintotwocategories:

1) TemporalRules:

In this category in the detection rule, the antecedentandtheconsequencewillappearinacorrectorderin distinct time instances (first antecedent followedby the consequence). The time series analysis in thisworkwilldealwiththedesignoftheIDS.

2) Reportincomingdanger:

If the antecedent is true then after a certain timedelaytheattackwillcommence.

Extraction of the temporal rules is an off-line operationthat implements data mining methodologies. Extractionof therules is performed in four stages where a largedatasetfromthenetworkstatusevolutionstothehistory ofsecurityviolationsareanalyzed.Thesestagesareasfollow:

Step 1 Extracting the effective parameters/variables atthe target side within the dataset.It is very impor-tanttoknowwheretolookfortheclues.

Step2Extractingthekeyparameters/variablesattheintruder side within the dataset. IDS should be ableto model the behavior of the intruder and these vari-ables are used to detect the current state of the in-trusion process.This information may derive fromstatistical casualty tests on some candidate variablesplusvariablesfromstep1.

Step 3 Determining the evolution of the intrusion pro-cessusingthevariablesderivedfromstep2andcom-paring them versus normal state of the network. Itis clear that this work follows the anomaly detectionapproach.

Step 4In this stage the events extracted in the step 3are being verified to see if they are consistently fol-lowed by the security violations observed in variablesextractedinstep1.

Intheirdescriptionofthistypeofattacks,authorsde-pictatimingdiagramforafivestagetransfertothefinalnetworksaturationinDDOS.Thesestepsare:Masterinitiatesinstallationofslaves(T0),Mastercompletesin-stallationofslaves(T1),Mastercommandstheslavetoinitiatetheattack(T2),Slaves start sendingdisablingnetworktraffictothetarget(T3),Disabling networktraf-ficreachestheTarget(T4),Thetargetisshutdown(T5).Atthistimechart, T0 is the start of the attack andT5iswhenthenetworkwillgodown.Thetime-periodbetweenT1-T2issolelydependentonhumanfactorandonwhenthemasterwilldecidetoorderthetslavetostartthe attack. Considering this chart and by using the NMSwithintheIDS,thesystemmightbeabletopredictor reacttotheattacks.
Authors of the paper have prepared a test rig for theintrusion attack simulation and have carried out few in-teresting experiments on their test rig.The results aremonitored and recorded. In this way, they can investigatethebehavior oftheirIDS andstudythe results. Theirmainemphasis is onthedata extracted from theMIBvariables.They have included few charts from the MIBvariables within the test period in their paper and haveanalyzedthem.Inintervalsof2hoursandsamplerateof 5 seconds, 91 MIB variables corresponding to 5 MIBgroups are collected by the NMS. These charts are syn-chronized so that they can be studied. Charts will provideus with an understanding of the behavior of the systemduring the normal and under attack periods. Since thesecharts are synchronized, one can easily relate the sequenceoftheeventsfromonevariabletotheother.
Later on in their paper, authors explain how to ex-tract rules from this dataset.In their description theyhave assumed that the sampling interval is constant i.e.samples are taken in equal time intervals. The result isamultivariatetimeseries.Amongdifferentdefinitionsin thepaper,twoofthemseemveryinterestingandtheyareexplainedinbelow:

Causalrule"If$A$and$B$aretwoevents,define$A \overset{\tau}{\Rightarrow} B$astherule:If$A$occurs,then$B$occurswithintime$\tau$.Wesaythat$A \overset{\tau}{\Rightarrow} B$isacausalrule"[11].

Precursorrule"If$A$and$B$aretwoevents,define$A \overset{\tau}{\Leftarrow} B$astherule:If$B$occurs,then$A$occurred notearlierthan$\tau$timeunitsbefore$B$.Wesaythat$A \overset{\tau}{\Leftarrow} B$isa precursorrule"[11].

Bothoftheserulesarespecialcasesofthetemporalrules.As an indication of the certainty level for correctness oftherules, eachoneofthese rulescanbe associatedwithaconfidence factor.Authors mention that precursor rulesaremined,butonlycausalruleswere applied.Threeproblems for the rule extraction are addressed in this re-portandlateronsolutionshavebeensuggested[11].

3 ModelingtheNetworkasaSys-tem

Thegoaloffindingamodelforthenetworkistodefinethenormal behavior and consequently anomaly in the behav-ior of the system. In the current literature, authors havedefined the normal behavior of the network with regardto their own view points and no generic definitions arenecessarily provided. A generic definition for the normalbehaviorandanomalyisproposedinbelow.
Generic definition of the normal behavior of the sys-tem (network):The most frequent behavior of (eventswithin) the system during a certain time period is calledthe normal behavior of the system.This behavior is thedominant behavior within the system and is the most fre-quentlyrepeatedone.
Generic definition of the anomaly within the system(network): The least frequent behavior of (event within)the system during a certain time period is called anomalyorabnormalbehavior.Therepeatingperiodforananomaly event has a very long repeat period and its in-tervalisclosetotheinfinity.
The most and the least frequent events will have re-spectively the lowest and the highest variances among allthe other events. Therefore, effective parameters will be:the duration of the time period, the frequency and thevarianceoftheeventswithinthattimeframe.
As it is clear from the literature, researchers have fol-lowed different approaches to improve accuracy and per-formance of their proposed IDS. However, the executiontime constraint is always an obstacle or a challenge toovercome. Modeling a dynamic and complex system suchas the network is very difficult.Thus,abstraction andpartial modeling can be a good solution. This is why someresearchershavechosentoseparatedifferentpartsofthenetwork and model them individually.The whole net-work can be divided into three different segments: host,userandthenetworkenvironment.Theuseritselfcan

be divided into two parts:legitimate user and malicioususer (intruder). Different researchers have selected eitherof thesegroups.Assigning a behavioral model to eitherof these groups, one can derive a model of the legitimateoranomalybehaviorforthem.

To model the host, it is required to monitor the systemwithin an intrusion free working environment for a while.Using the collected data, it would be possible to derive amodel for the normal behavior of the host. Any deviationfrom this model can be considered as an anomaly behav-ior and can be used for the intrusion detection.Usuallythere is a threshold value that determines the acceptabletolerance for any deviation from this model. Any activ-ity that subjects the system to a deviation larger than athreshold value from its normal behavior model can beconsideredasananomaly.

Anotherapproachistomonitorthesystemforaperiodof time and then assign a baseline to the systems param-eters.In this approach, crossing the baseline denotes ananomaly behavior. It is also possible to assign a normalbehavior model to a host and to consider any other be-havior an anomaly. However, this approach will requireapplying limitation on the system that might not be de-sirable. This approach might be suitable for cases wheresystem performs highly repetitive tasks and within a welldefined work area. It also requires deep knowledge of thesystem. The approach is a specification based approachto the ID and Section 4.1 will provide a more detaileddiscussion on the specification based ID. Sekar et al. [39]report a work in this area where a state machine basedIDSisimplementedtofollowstatetransitionswithint hesystem. In this work, system is expected to behave in acertain way and IDS will respond to any abnormal statetransitions.

User modeling can be an alternative method to tacklethe ID problem. In this method, one can decide whetherto model the legitimate user. The anomalous behavior isusually(butnotnecessarily)anindicationofanintruderus er. This approach can be used to model the intruderand to monitor his actions and his progress. Determin-ing the normal behavior of the legitimate user can alsobe specification based that will lead to limiting the userwithinacertainboundary.Sincetheuserisahumanbe-ing and humans can be unpredictable, normal behaviormodeling of the user can be a very difficult task.Thesamecanbetruewithbuildingabehaviormodelfor theintruder. Intruder as an intelligent human being, who isaware of the usual behavior for the intruders, can slightlyalter his intrusion approach and fool the system. Model-ing the intruder can be a better alternative since it canbe assumed that intruders are a small subset of the usercommunityandwithaknownattribute(knowngoal)i.e. intrusion. On the contrary, legitimate users are a muchlarger subset of the overall users and their attribute(s)can be diverse i.e. they might have different interests anddifferentgoals.

In a reported work, Vigna et al. [41] implement a StateTransitionAnalysisTechnique(STAT)tomodelatt ack scenarios (intruder behavior modeling).Their work isespecially interesting since STAT framework has an ex-tension process that includes the extension of the attackmodeling language.Therefore, using this modeling lan-guage it would be possible to model different attack sce-narios.

Inanotherreportedwork,Bothaetal.reportawork [7] to detect the intrusion using the malicious user behav-iorandthefuzzylogic.Theoverallviewoftheauthorsis to consider six different generic phases for an intrusionintoa network. The goal of this system is to track andto monitor the current state of user's behavioral profileconsidering these categories. These six phases are respec-tively: probing, gaining initial access, illegal password fileaccess attempt, performing the hacking attempt, coveringhacking tracks and finally modifying utilities to ensure fu-ture access.One of the short comings of this work is anassumption that is made by the authors.They have re-ported that due to the lack of data, the model for thetransition from one state to the other is assumed to belinear.However, in the real world this transition is non-linear.

The network environment itself can be considered forthemodeling.Inthiscase,transactionsbetweenmembersof thenetworkcanbemonitored.Agentbaseddistributedsystem s are the main contributors to this approach. Nev-ertheless,thisapproachisverycomplicatedandthetar-get system is complex. In this approach the relationshipbetween the members of a network play an importantrole. Distributed processing will improve the time con-straints for the processing of the information within suchanenvironment.AworkreportedbyLeeetal.[28]isane xample of this approach. In the reported work data min-ing techniques and a Common Intrusion Detection Frame-work (CIDF) are deployed to build a distributed IDS.

Inthisworkconnection/sectionrecordsareusedasfeatures.

4 Some Trends inIDS Design

Before getting started with describing trends in the IDSdesign, it should be noted that IDS has a classifier ker-nel.The kernel of the IDS is responsible for classifyingthe acquired features into two groups namely normal andanomaly, where the anomaly pattern is likely to be anattack.Nevertheless, there are occasions where a legiti-mate use of the network resources may lead to a positiveclassification result for the anomaly or signature basedintrusion detection. As a result of this wrong classifica-tion, IDS will wrongly raise the alarm and will signal anattack. This is a common problem with the IDS and iscalledFalsePositive(FP).Oneoftheparameterstomea-surethequalityofanIDSisthenumberofitsFPalarms.Thes malleristhenumberoffalsepositives,thebetteristheIDS.

4.1 SignatureBased,Anomaly BasedandSpecificationBasedIDS

Signature based intrusion detection (misuse detection) isoneofthecommonlyusedandyetaccuratemethodsofintrusiondetection.Onceanewattackislaunched,theattack pattern is carefully studied and a signature is definedfor it. The signature can be a name (in characters) withinthebodyoftheattackcode,thetargetedresourcesduring the attack or the way these resources are targeted (attackpattern).Studying the attack pattern, security special-ists can design a defense against that attack.Later on,using the proposed defense method, the IDS is updatedaccordingly to recognize the new attack patterns and toresponse to them. This approach is very efficient for theknownattacksandproducessmallnumberofFPalarms. However, as the main short coming of this approach, it isnot capable of detecting novel attacks. Once the attackpattern is slightly altered, this approach will not detectthe altered versions of the old attacks.Thus, this ap-proach is only efficient in detecting previously known at-tacks. There is another approach for detecting the novelandunseenattacksthatfollows.

Another widely used ID method is the anomaly detection approach [35, 34, 22, 26]. The basic idea behindthisapproachis tolearntheusualbehavioralpatternofthe network. Consequently the attack is suspected (de-tected) once the network behaves out of its regular way(anomaly). However, network regular behavior is not sim-ilar for different networks. The network behavior is de-pendent on the date or the working conditions in the or-ganization where the network is installed.The regularbehavior model for the network can be variable. Consid-ering these working conditions, the degree of freedom forthe problem is large.One way to solve this problem isto make the IDS adaptable to the network environmentwhere it is going to be installed. To do so, IDS will startto monitor and record the network behavior just after itsdeployment.

Assuming the recorded pattern as the regular patternfor the network, IDS will use it as the normal behaviorof the network and will set a baseline.Once the net-work pattern deviates from this baseline pattern by morethanathresholdvalue,itdenotesananomaly.Asitwas mentioned earlier, not every anomaly indicates an intrusion. This is especially true in this case, where the system is very dynamic. Thus, it is not clear if the detectedanomaly should be assumed to be an intrusion or not.Asadirectresultofthisuncertainty,anomalybasedIDS will produce high FP alarms. As a remedy to this problemthere should be a pruning system to detect FP alarms andcancel them. Keeping this shortcoming in mind this ap-proach has a big benefit, that is, it is capable of detectingnovelattacksornewreleasesoftheoldattacks.

One of the problems in this field of research is findingeither the right features or the right relation between cer-tain features to monitor. May be sometime in future, theanomalydetectionmethodologybecomesmatureenough not to require a baseline anymore. Currently many commercial ID systems use a hybrid approach where anomalybased intrusion detection is used together with the signa-ture based intrusion detection method.Using the signa-ture based ID methods system can accurately identify theknown attacks with low FP alarms. If any unknown in-trusions occur then anomaly detection based ID methodscan detect the intrusion and raise the alarm. Using theanomaly detection based ID, the signature based meth-ods can also be used to refine the FP alarms raised bythis method. This approach will result in increasing theaccuracy and reliability of the IDS while keeping the num-berofFPalarmslow.

A recently introduced approach is the specificationbasedintrusiondetectionapproach.Somerepor tedworksemphasize only on the signature (misuse) based andanomalybasedintrusiondetectionapproaches[16,12,42, 22].However, there are others who talk about all threeof the approaches.The specification constraint in thisapproach is used for reducing the number of FP alarms[40,39].

Implementation of the anomaly based IDS requires indepth knowledge of the system.The specification constraints are extracted by the human expert manually.Although specifying critical resources of the system andtheir utilization may improve the security, there mightalways be some points missing in this process that mayaffect the system utilization.Specification based is notjust applicable to the host systems but they can also beapplied on the users as well.A legitimate user is ex-pected to behave in a certain way, or it can be specificthat a user should behave in this manner. This decisionwill improve the security but with the expense of a lessattractive user interface.Limiting the user actions andfreedom may lead to making the application look less ap-pealing to some users. It is expected to get better resultsby applying specification based ID methods on the systemitself.

4.2 NetworkBasedIDSandHostBasedIDS

Asitwasmentionedearlierintheintroductionsectionof this article, network based and host based systems aretwo categories of the IDSs. The network based IDS is responsible to protect the entire environment of the networkfrom theintrusion.This task asks for full knowledge ofthesystemstatusandmonitoringboththecomponentsofthe networkandthetransactionsbetweenthem.Agenttechnology playsakeyroleinthisstrategy.Networkistheinfrastructure for a distributed system. Therefore, agentsare a natural choice for this approach. Collecting informa-tion within the network and processing them, respondingtotherequestsandcommandsofthekerneloftheIDSor working as an individual, all can be accomplished using agent based technology.The network based IDS iscapable of accessing the network routers and instructingthemtoperformtasks.Usingthisfeature,systemcan ask

the router to disconnect a terminal or a subnet that hasbecomeasecuritythreat.

There are several reported works in this area.In apaper by Foo et al.[17] authors investigate the imple-mentation of the mobile agents in the IDS area. In thisway, they intend to improve the speed of program develop-mentandupdatefortheIDS.InanotherpaperbyZhanget al. [46], a new architecture for a multi-agent based IDSis proposed. Paper divides the security threats into twomain groups: those that come from Insider Intruders andothers that come from Outsider Intruders. Paper also cat-egorizes IDSs into three categories: host-based, network-basedandrouter-basedIDSs.Authorsbelievethatina multi-agent based IDS, the system should be able tohave a perception of the world surrounding it.Finally,paper proposes a model with a network architecture con-sisting of four types of agents: basic agent, coordinationagent, global coordination agent, interface agent. Consoleconsists of two agents, a global coordination agent andan interface agent. The global coordination agent is re-sponsible for all of the coordination agents in the system.This includes receiving reports and sending instructionsto them. The interface agent can provide information forthe administrator in the form of Graphical User Interface(GUI). It can also receive control commands in the formofGUI.

InapaperbyLuoetal.[33]anewMobileAgentDistributedIDS (MADIDS)hasbeenintroduced.Paperreports that one of the main goals of the system is to im-prove the performance of the IDS in regard to speed andnetworktraffic.MADIDSconsistoffourparts:EventGene ration Agent, Event Analysis Agent, Event TrackingAgent and Agent server. Data is transferred by the Gen-eralizedIntrusionDetectionObject(GIDO).Eventgen-erators are responsible for collecting data and convertingthem to the appropriate format.Event analyzers are re-sponsible for analyzing the events and generating GIDOs.Responseunitswillprocess GIDOs. Events and GIDOsare store in event servers (databases).Distributed com-puting on different computers will significantly improveMADIDSsprocessingperformance.

In a work reported by Ramachandran et al.[38] theidea of neighborhood watch is implemented for the net-work security. There are three different types of agentsin three different layers. There are different types of Copagents dependent on their assignments. A Cop is respon-sible for collecting data from various sites and report-ing them to its respective detective agent.The detec-tiveagentisresponsibleforanalyzingthereportsreceivedfro m the Cop agent.There is a Chief agent on the toplayer who will have all the detectives reporting to him.Chiefisresponsibleforthesecurityofboththehostandt he neighbors. There might be a Chief agent monitoringa number of other Chiefs. Chief will monitor and studythe reports from the detectives. If a Chief notices that se-curityofasitehasbeencompromised,thenitwillselecteither of the actions:Chief decides to further monitorthatsiteorwillorderothersitestoprotectthemselve s fromthatsite.

Ramachandran et al. [38] have proposed this approachwith the intension to distribute the decision making andthe workload of the IDS. The detective agent is responsi-ble for analyzing the reports received from the Cop agent.There is a Chief agent on the top layer who will have allthe detectives reporting to him.Chief is responsible forthe security of both the host as well as the neighbors.There might beaChiefmonitoring anumberofotherChiefs. Chief will monitor and study the reports from thedetectives.If a Chief notices that security of a site hasbeen compromised, then it will either decide to furthermonitor that site or it will order other sites to protectthemselves from that site.Paper reports that every nowand then sites start to check each other to determine thesecurity leveloftheirneighbor.Theresult willbere-portedtotheDetectives.

Mukkamala et al.[34] believe that IDS has two cat-egories:hostbasedIDSandnetworkbasedIDS.Theydefine these two types as follows: “A host based IDS mon-itors all the activities on a single information system host.Itensuresnoneoftheinformationsystemsecuritypolicie sare beingviolated. A network IDS monitors activities onawholenetworkandanalyzestrafficforpotentialsecuritybr eachesorviolations.”

ThehostbasedIDSisonlyinstalledonasinglehost/terminal and is responsible for monitoring the statusof that terminal/server only. This type of IDS is respon-sible for the security of its host and will monitor all thenetworkactivitiesinthathost[23].Oneoftheproblemswi ththehostbasedIDSisthehighprocessingoverheadthatthe yimposeontheirhost.Thisoverheadwillslow-down the host and therefore it is not welcomed.Thisapproachisquitepopularamongtheresear chers.

4.3 DifferentApproachestoIDSDesign

An active IDS will provide a predefined response to thedetected intrusions. The passive IDS is only responsibleformonitoringthesystemandtoinformtheadmi nistra-tor once an intrusion occurs or to produce an advancewarning.The response concept is related to the activeIDS.Thisresponsecanbeareactiontoasecuritybreac hin the system or a preemptive response to avoid a secu-rity breach. One of the main goals of any active IDS isto prevent the security breach and not just to respond tothethreat.

Continuing their earlier work [10], Cabrera et al. [11]reportamoreadvancedworkwherethefeasibilityoftheira pproach is studied.Authors use the Simple NetworkManagement Protocol (SNMP) to build an IDS system.In this report, authors report that the idea of proactiveIDS is about predicting the intrusion attack before it ac-tuallyreachestoitsfinalstage.ProactiveIDSisasystemthat reacts to the imposed threats, and in response it willapplypredefineddefensiveroutineswithinthesystem.

There are two types of product lines in the commer-cialIDSindustry.Inonetypeofproduction,theIDSis

produced in the form of a software package.In order toprotect a host, the IDS software has to be installed onthathost.Once theIDSisinstalled,itwill access thenetwork modules/ports of that host and will gain controlover them. Later on, using its control over the system,IDSwillmonitorthenetworktransactions andwillrespond to the threats.Although it can be used for thedistributed IDS as well, this approach is more suitable forthehostbasedIDSthanthenetworkbasedIDS.

However, industry has shown a great interest in another approach as well. In this approach, the whole IDSproduct is included in one box (IDS appliance). Both thehardware and the software modules are inside that box.Other hosts/servers can communicate with the IDS usingthe network infrastructure.Network administrator canupdatetheIDSwithnewpoliciesusingaterminalwitha network connection. Products from companies such asCISCO (CISCI IDS Sensors) and Mazu (Mazu Enforcer)areexamplesofthistypeofapproach.

The reason for the IDS appliance approach being attractive to the market and consequently to the IDS industry, is its ease of installation and flexible deployment.At the same time, administrators do not need to worryabout the high computing overhead exerted on the hostmachinesbytheIDS.Oncea network is targeted, thefirstattackisaimedontheIDSitself.Thus,inthecaseoftheh ostbased IDS, both the host and the IDS willgo under attack. This situation will increase the comput-ing overhead on the host machine at the same time willreduce itsresponse time.WiththeapplianceIDSthisproblem issolved.Another benefit of this approach isfor themanufacturer. Producing the IDS in the form ofan appliance will improve the security measures for theproduct reengineering as well.It is easy to crack a software and make illegal copies out of it, however, followingthis approach wont be feasible for the appliance IDS. Thehardware implementation of the appliance will make itharder and more expensive to make a copy of it.Thedrawback for this approach is the cost of production. Usingthehardwarecomponentswillincreasetheproductioncost and consequently the price of the product. Anotherbenefit of this approach is the guarantee for the optimumhardware setup and performance for the IDS. This is be-cause, the hardware platform and the software setup isalreadycompletedandtestedbythemanufacturerthatisfamiliarwiththesystem.

5 WheretoLookfortheFeatures?

Desired features for the IDS depend on both the methodology and themodeling approach usedin building theIDS. These features are usually numerous.Thus consid-ering the volume of data, processing all of them will takequiet awhile. In order to speed-up the process, these fea-tures are usually preprocessed to reduce their size, whileincreasing their information value.There are numerousapproachesreportedinthisarea.Mostofthereporte dresearch is concerned with the header of the packets. However, recently researchers have valued the body or thepayload of the packets as well. This part of the packetswas usually disregarded due to its large volume and theextensive processing time required for processing them.Researchers such as Lee et al.[30, 31, 28] with datamining interests tackle the problem using the associationrules. However, they extract these rules using the infor-mation in the header of the packets. Zanero et al.
[44]reportaworkwhereTCP/IPheaderandpacketspayload areusedtoextractfeatures.Inthiswork,usinganunsupervised clustering algorithm, the payload is compressedinto a single byte. In their work, Zanero et al. have usedSOM for the classification of packets. In another reportedwork,Leietal.[32]reportImprovedCompetitiveLearn-ing Network (ICLN) method based on the SOM but 75%faster(experimentedontheKDD-99dataset).

Just extracting features is not useful for the ID. Extraction should be followed with a second stage where patternsare produced using the extracted features.Using thesepatterns,intelligentkernelofthIDSwillanalyzetheworking condition of the network and will raise the alarmif necessary.Employing pattern extraction method, oneshould consider both the importance of the features andtherelationbetweentheminthefeaturespace.Theresultantpatternissomehowacompressedandabstractedver-sion of the feature space.One of essential questions is howtodeterminetheinformationvalueofthefeaturesorhowto find the relations and evaluate the importance of therelations between the features? Usually statistical meth-ods [6] are used for this purpose.Data mining methodsarealsocommonlyusedinthisarea[30,31,28,29].Th eseapproaches are not limited to using the association ruleapproach but other methods such as ANN [44, 32, 23, 20],Bayesian[5],Fuzzy Logic [8], Genetic Algorithms (GA)[8,35,22],HMM[12,3,42]andSVM[23,20]methods haveattractedmuchattentionaswell.

6 HoneyPot(HP)

Despite its effectiveness, not until recent years this approachhasbeentakenseriouslywithintheacademia.However , recently research in this area has gained somemomentum. Maybe this lag was due to the fact that thereisnotheoreticalconceptinvolvedintheHPapproach,itis just a deception. HP is mainly a heuristic approach andis based on the concept of bait and trap.Nevertheless,industry sector is very attracted to this concept. Thereare a number of products available that use the HP totrap undetected intrusion attempts.Generally speaking,HP is a deception based approach to detect actions of adeceitful enemy (the intruder).The HP concept has at-tracted much attention over the internet and there arenumerous sites dedicated to this concept [19].Some HPbasedframeworksinclude:

- HoneydprojectwithGNUGeneralPublicLicense [21]thatcreatesvirtualhostsonanetwork.

· Honeynet [36] project, is a project defined with thegoalofbuildingavirtualHoneynet.

· Specter[13]isacommercialproductandsupportsHP for different resources within the system. One oftheimportant features for this commercial productisthewidespectrumofoperatingsystemsthatitcovers.

· ProjectHoneypot[1]isaimedtoprotectwebsitesandemail serversfromthespammers.

· Back Office Friendly (BOF) [14] is a free softwarethatdeploysHPforvariousservicesinthesystem e.g.SMTP,POP3,HTTP,FTP,TelnetandIMAP2.

· Many other research projects in this area are listedin Honeypots.net site [19] that are out of the scopeofthisreport.

The overall idea behind the HP technology is to lay atrapandbaitandwaitforthehunttofallintoit.Thisisinadditi ontoalltheotherdetectiontoolsdeployedtocatch the hunt. Here HP is used as a supplement to theIDStodetectthe intrusionwhereIDSwasunabletodoso.In this way, the probability of missing some attacks un-detected is reduced. Other than detecting attacks missedbytheIDS,HPcanhelptheIDSinmanyotherways. Themain assumptioninimplementing a HP, is that,no one would ever use the selected resource for the HP.Therefore,anyattempttousethoseresourcesisexpectedto be malicious and should be monitored. Some benefitsoftheHParelistedinbelow:

· HPwillkeeptheattackerpreoccupied.Inthismethod, after detecting the intrusion attempt, sys-tem will alert the security officer immediately whilekeeping the attacker busy. This approach has severalbenefitsthatarelistedinbelow:

1) By selecting correct resources for the HP to em-ulate as bait, one can distinguish different in-terestsoftheattackers.Havingtheintruderfallenin thetrap,HP canstartstudyingtheopponent.HP will let the intruder to navigatethrough the emulated environment and will logits actions.HP or the security officer can gainmuch information by studying logged actions ofthe attacker, the targeted resources and attack-ers informationregarding thesystemsuchasusername,password,etc.

2) Keeping the attacker busy.HP will buy moretime for the response system or the security of-ficer/administrator of the system to come-upwith a proper response to the attack attempt.Response latency time is very important sinceattacks might be too fast for the response sys-tem to react to them.At the same time, pro-vidingthe systemadministratorwith sufficient time might help in finding the root of the con-nection that the attacker is using. Tracking theattackers can be very difficult and it requires agreat deal of experience and time to trace thembacktotheirorigin.

3) Another benefit gained by HP keeping the at-tacker busy is to waste attackers time and topreventhimcompromisingotherresourceswitha fast speed.For example, in a port scanningscenario keeping the attacker waiting for a replymay significantly slowdown the whole process.HPcandothisinadifferentwayaswell,thatis, by emulating a working environment, HP canconvince the intruder that he is in a real systemand let him try to perform the intrusion.Themore convincing is the HP, the more time theintruderwillspendintheenvironment.

· Within an IDS guarded system, HP will detect un-noticed attacks.In this way, HP will increase thereliability of the IDS. The detection offered by theHP is independent of the type of attack that is en-forcedonthesystem.

· Another benefit for using a HP in a system is withrespect to the overhead on the processor. In the IDSapproach every packet transaction in the system hastobemonitored and analyzed.Thus,theIDSap-proach willgenerate ahighcomputationalpowerde-mand within the system.The same is true with thedata transfer within the system. Due to the size ofthepacketstransferredwithinthesystem,datatrans-fer time will consume a large part of the processingtime. In addition to the processing time, data trans-fer will consume different data transfer related re-sources of the system. Using the HP will reduce theprocessing and resource consumption overhead on thesystem. The processing time will be provided for theHP process only when the HP monitored resourceswithin the system are utilized. In this way, the over-head enforced on the host system by the HP duringthe HPs idle period will be negligible. This scenario isvery similar to the differences between the interruptbased and the polling based IO handling methods inthecomputerhardwaredesign.

In order to improve the performance of the HP opera-tionandtoincreasethehitprobabilityoftheHP,usuallya large number of HPs are placed in a network.TheseHPsareclosetotheimportantresourcesinth enetworkandoperatebothasaguardianandadecoyforthem .Agroup of HPs that are distributed in a system is called aHoneyPotfarm.
Nowadays, intruders aware of the HP technology try toavoid the HPs or even take advantage of them. To do so,they have implemented tools to detect the HP and oncedetected, they disengage the HP. At the same time, HPsareusuallydeployedtoprotectaresourceoradata.Once

the HP is detected, it is most probable to find a valuableresourceinitsneighborhood.

Zhang et al. [45] report an investigation on the HP concept. In the reported paper, HP concept is investigatedand HP and honey nets are described. Data control andcapture for the HP are illustrated. Authors categorize theHPs into four categories: Prevention, Detection,
ReactionandResearch.Bytheprevention,Zhangetal.meant hatthe prevention HP will delay the intrusion by divertingintrudersattentiontotheHP.AsforthedetectionH P,itcan generate alert once the attack is detected. Authorsalso believe that HP can not be used individually and itis a supplement to the IDS. They define the reaction HPto be a type of companion system and trial environmentfor test systems vulnerabilities. The research honey potis to log and study the opponent (the intruder) and to re-port the result. This type of HP will act in a very flexibleway and will provide the intruder with a vast maneuverspace. The main goal of this type of HP is to determinethe purpose and the goal of the intruder. A HP can holdanyoracombinationofthesecategories.

Kuwatly et al. [27] in their paper, divide HPs into twocategories i.e. Low-interaction HPs and High-interactionHPs. Low-interaction HP are those that have limited in-teraction capabilities and can emulate certain protocolssuchasFTPe.g.Specter[13],Honeyd[21].

As the HP technology improves so does the anti-HPtechnology.Therefore, a never ending battle is alreadystarted. Honey pots have to be improved constantly oth-erwise they themselves will become a weak point in thesystem.In other words, protecting or hiding somethingshows that it is important to us.Thus, by knowing whatresources HP is protecting, the intruder can identify theenvironment and the valuables in the system in a betterand more efficient way [25]. Authors propose a design fora dynamic honeypot, capable of changing configurationtomatchthedynamicandeverchangingenviron mentofanetwork.

Khattab et al.[24] propose roaming HPs for service-levelDoSattacks(physicalroaming).Theproposedmechanis m allows the HP to randomly move its positionwithin a server pool. Interesting beneficial features in thisworkarethefilteringeffectandconnection-dropping.Thefilteringeffectiswhentheidleserverthatisactin gasaHP detects addresses of the attackers and filters them outor blacklists them.The connection-dropping occurs at arandom displacement time when the server is switchingfrom idle (HP mode) to active.At this time server dropsall the connections (attacker connections).This connec-tion dropping in turn will open space for the legitimaterequests before a new wave of attacks start again. In theirpaper, authors define the logically roaming honey pots inthefollowingway.

Logically roaming honey pots are similar to the IP hop-ping, where legitimate clients coordinated by the serversrandomly change the destination address in their packets.Inthisway,theunwelcometrafficthatisnotupdatedw iththecorrectdestinationaddresswillberendered.They also claim that although logical roaming of the HPs ismore cost effective, the physical roaming is still necessaryto protectthenetworkagainsttheinternal attacks.

7 Conclusions

Considering the surveyed literature, it is clear that in order to be able to secure a network against the novel attacks, the anomaly based intrusion detection is the bestway out.However, due to its immaturity there are stillproblems with respect to its reliability.These problemswillleadtohighfalsepositives in any anomaly-basedIDS. In order to solve this problem, usually a hybrid ap-proach is used.In the hybrid approach, the signature-based approach is used together with the anomaly-basedapproach.In thisway,thesecond approach is mostlyused for the novel tactics while the accuracy of the firstapproach (signature based approach) will provide a reli-able detection for the known attacks. Specification-basedapproach is only good when system specifications and de-tails are known and applying limitations on the user isacceptable. The generic definition of the normal behaviorand the anomaly behavior in the system are presented inthis paper.The intension for introducing these genericdefinitionswastohelpresearcherstoconvergeonthede f-initionofthenormalbehaviorofthenetwork.

Innetwork-based IDS,agentbasedsystemsplayanessential role.In such systems a distributed processingarchitecture is a must and system has to collect informa-tion from different components within the network.Im-plementingsucharchitecture,oneshouldavoidincreasingthe networktraffic.

Large volume of data and non-deterministic normal be-havior of the network are two major challenges in IDS de-sign. As the volume of data using the header of the pack-ets is already very large, using information in the payloadwill make the process even slower.However, there
areworksreportedbysomeresearchersinthisareathatshowgo odprogressinusingpacketspayloadfortheanalysis.

The intrusion detection products were analyzed withrespecttothesoftwareorappliancebasedproductionandt hebenefitsofeitherofthedesignswerediscussed.Build-ing hardware appliances can be more difficult for compa-nies with lower development budget. However, appliancebased IDSs are more appreciated in the market. From theconsumer point of view, appliance based IDS is easier toinstall and to maintain. In manufacturers view, appliancebased IDS is a more secure design to manufacture but asthesametimemoreexpensivetoproduce.

Another aspect of the IDS design is the issue of themissed attacks. If some attacks are not detected by theIDS, there are no means to notice them. This is especiallythe case with the novel attacks. In addition to all otherbenefits, HP technology can help to expose these attacks.TheaccuracyoftheHPtechnologydependsonthenu m-ber of HPs distributed in the system (population of theHPfarm).ThelargerthepopulationoftheHPsthemore

accurate is the detection rate. Increasing the accuracy isnot the only benefit for implementing the HP technology,but it can be used for other purposes as well.For ex-ample, HP can be used for studying or slowing down theintruder.

8 FutureWork

As for the future work, intension is to produce an IDScapable of anomaly and signature based intrusion detec-tion. There are two options in front of us, i.e. host basedornetwork basedIDS.The host based IDS can be eas-ier to implement, though the network based IDS needsmore timeand effort for its implementation and design.In return, the network based IDS will provide a more re-liable and more accurate IDS. The network IDS needs tohave environment awareness.Thus, the network basedIDS needs special sensors for its work. Agent based tech-nology is one of the essential blocks in this distributedarchitecturedesignmethodology.

The selected approach for our future work is the net-work based software product.However, the host basedapproach will be considered as well.The project time-frame and the budget are main issues with regard to thisdecision.Nevertheless, accepting the expenses, it is al-ways possible to convert a software based IDS to the ap-plianceversionofit.

From the theoretical point of view, it is intended toimprove the accuracy of the anomaly based intrusion de-tection.One way to do so is to use the payload of thepackets.Therefore, it is necessary to envisage a methodeithertoreducethesizeofthedataortoprocessthedata more quickly. The main idea is to find a method to handlehigh volume of data with less information loss.For thesamereason,featuresshouldbeevaluatedwithrespecttoth eirinformation value. In this way, every feature willbe associated with a coefficient of importance that deter-mines its overall effectiveness in comparison to the otherfeatures.Efficient algorithms and programs can provideagreathelpforthispurpose.

References

[1] Unspam;LLCaChicago-based anti-spamcom-pany.“Websitefortheprojecthoneypot,”.http://www.p rojecthoneypot.org/.

[2] M. Analoui,A. Mirzaei,and P. Kabiri,“Intrusiondetection using multivariate analysis of variance al-gorithm,”in*ThirdInternationalConferenceonSys-tems, Signals & Devices SSD05*, vol. 3, Sousse,Tunisia,Mar.2005.IEEE.

[3] A. Zhong and C.F. Jia,“Study on the applicationsof hidden markov models to computer intrusion de-tection,” in *Proceedings of Fifth World Congress onIntelligent Control and Automation WCICA*, vol. 5,pp.4352–4356.IEEE,June2004.

[4] D. Barbara, J. Couto, S. Jajodia, and N. Wu, “Spe-cial section on data mining for intrusion detectionand threat analysis: Adam: a testbed for exploringtheuseofdataminingintrusiondetection,”*AC MSIGMODRecord*,vol.30,pp.15–24, Dec.2001.

[5] D. Barbara, N. Wu, and S. Jajodia, “Detecting novelnetwork intrusions using bayes estimators,” in *Pro-ceedingsoftheFirstSIAMInternationalConferenceon Data Mining (SDM 2001)*, Chicago, USA, Apr.2001.

[6] M. Bilodeau and D. Brenner, *Theory of multivari-ate statistics*.Springer - Verlag : New York, 1999.Electroniceditionatebrary,Inc.

[7] M.BothaandR.von Solms, “Utilising fuzzy logicand trend analysis for effective intrusion detection,”*Computers & Security*, vol. 22, no. 5, pp. 423–434,2003.

[8] Susan M. Bridges and M. Vaughn Rayford, “Fuzzydata mining and genetic algorithms applied to intru-sion detection,” in *Proceedings of the Twenty-thirdNational Information Systems Security Conference*.National Institute of Standards and Technology, Oct.2000.

[9] D. Bulatovic and D.Velasevic,“A distributed in-trusion detection system based on bayesian alarmnetworks,” *Lecture Notes in Computer Science (Se-cure Networking CQRE (Secure) 1999)*, vol. 1740,pp.219–228,1999.

[10] J.Cabrera,L.Lewis,X.Qin,W.Lee,R.Prasanth, B. Ravichandran, and R. Mehra, “Proactive detec-tion of distributed denial of service attacks using mibtrafficvariables-afeasibilitystudy,”in*Proceedingsof the 7th IFIP/IEEE International Symposium onIntegrated Network Management*, pp. 609–622, Seat-tle,WA,May2001.

[11] Joao B. D. Cabrera, L. Lewis, X. Qin, W. Lee, andRaman K. Mehra, “Proactive intrusion detection anddistributed denial of service attacksa case study insecurity management,” *Journal of Network and Sys-temsManagement*,vol.10,pp.225–254,2002.

[12] S. B. Cho, “Incorporating soft computing techniquesintoaprobabilisticintrusiondetectionsystem,”*I EEETRANSACTIONS ON SYSTEMS, MAN,AND CYBERNETICSPART C: APPLICATIONSANDREVIEWS*,vol.32,pp.154–160,May2002.

[13] NETSEC-Network Security Software Co. “Specter,”.http://www.specter.com/.

[14] NFRCo.“Websiteofnfrco.,”.http://www.nfr.net/.

[15] Mitsubushi Corporation.“Concordia mobile agentdevelopmentkit,”.Software,1999.

[16] John E. Dickerson and Julie A. Dickerson, "Fuzzynetworkprofilingforintrusiondetection,"in*ProceedingsofNAFIPS19thInternationalConferenceoftheNorth American Fuzzy Information Processing Society*,pp.301–306,Atlanta,USA,July2000.

[17] Simon Y. Foo and M. Arradondo, "Mobile agentsfor computer intrusion detection," in *Proceedings oftheThirty-SixthSoutheasternSymposiumonSystemTheory*,pp.517–521.IEEE,IEEE,2004.

[18] J. Gomez and D. Dasgupta,"Evolving fuzzyclassifiers for intrusion detection," in *Proceedings of the2002IEEEWorkshoponthelnformationAssurance*,WestPoint,NY,USA,June2001.

[19] honeypots.net.
"Websiteforhoneypot,".http://www.honeypots.net/.

[20] P. Z. Hu and Malcolm I. Heywood, "Predicting intrusions with local linear model," in *Proceedings of theInternational Joint Conference on Neural Networks*,vol.3,pp.1780–1785.IEEE,IEEE,July2003.

[21] Website is maintained by:Niels Provos."Honeydframework,".http://www.honeyd.org/.

[22] J. Guan,D.X.Liu,and B. G.Cui,"An inductionlearning approach for building intrusion detectionmodels using genetic algorithms," in *Proceedings ofFifth World Congress on Intelligent Control and Au-tomation WCICA*, vol. 5, pp. 4339–4342. IEEE, June2004.

[23] H.GunesKayacik,A.NurZincir-Heywood,andMalcolm I. Heywood, "On the capability of an som basedintrusion detection system," in *Proceedings of theInternational Joint Conference on Neural Networks*,vol.3,pp.1808–1813.IEEE,IEEE,July2003.

[24] SherifM.Khattab, C. Sangpachatanaruk,D.Mosse, R.Melhem,and T. Znati, "Roaming honeypotsfor mitigating service-level denial-of-service attacks,"in *Proceedingsof the 24thInternational Confer-ence on Distributed Computing Systems (ICDCS04)*,pp.328–337. IEEE, IEEEComputerSociety,Mar.2004.

[25] N.Krawetz,"Anti-honeypottechnology,"*IEEESECURITY & PRIVACY*, vol. 2, pp. 76–79, Jan.-Feb.2004.

[26] C.Kruegel,T.Toth,andE. Kirda, "Service spe-cific anomaly detection for network intrusion detec-tion," in *Proceedings of the 2002 ACM symposium onApplied computing*, pp. 201–208. ACM, Symposiumon Applied Computing, ACM Press New York, NY,USA,Mar.2002.

[27] I. Kuwatly, M. Sraj, Z. Al Masri, and H. Artail, "Adynamichoneypotdesign for intrusion detection,"in*ProceedingsoftheIEEE/ACSInternational Con-ference on Pervasive Services (ICPS04)*, pp. 95–104.IEEE,IEEEComputerSociety,July2004.

[28] W. Lee, Rahul A. Nimbalkar, Kam K. Yee, Sunil B.Patil,Pragneshkumar H. Desai,Thuan T. Tran,and Salvatore J. Stolfo, "A data mining and cidfbased approach for detecting novel and distributedintrusions,"in*ProceedingsofRecentAdvancesin Intrusion Detection, 3rd International Symposium,(RAID2000)*(H.Debar,L.M.,andS.F.Wu,eds.),
pp. 49–65, Toulouse, France, October 2000. LectureNotes in Computer Science, Springer-Verlag Heidel-berg.

[29] W. Lee and Salvatore J. Stolfo, "A framework forconstructing features and models for intrusion detectionsystems,"*ACMTransactionsonInformationandSystemSecurity(TISSEC)*,vol.3,pp.227–261,Nov.2000.

[30] W. Lee, Salvatore J. Stolfo, and Kui W. Mok, "Min-ing audit data to build intrusion detection models,"in*ProceedingsoftheFourthInternationalConference on Knowledge Discovery and Data Mining(KDD'98),*,NewYork,NY,USA,Aug.1998.

[31] W. Lee, Salvatore J. Stolfo, and Kui W Mok, "Adap-tive intrusion detection: A data mining approach,"*ArtificialInteligenceReview*,vol.14,no.6,pp.533–567,2000.

[32] J.Z.LeiandAliGhorbani,"Networkintrusiondetection using an improved competitive learning neuralnetwork," in *Proceedings of the Second Annual Con-ference on Communication Networks and ServicesResearch (CNSR04)*,pp. 190–197. IEEEComputerSociety,IEEE,May2004.

[33] G. Luo, X. L. Lu, J. Li, and J. Zhang, "Madids:Anovel distributed ids based on mobile agent," *ACMSIGOPS Operating Systems Review*, vol. 37, pp. 46–53,Jan.2003.

[34] S. Mukkamala, G. Janoski, and A. Sung, "Intrusiondetection using neural networks and support vec-tor machines," in *International Joint Conference onNeural Networks IJCNN02*, vol. 2, pp. 1702–1707,Honolulu, HI USA, May 2002. IEEE, IEEE.Source:IEEEXplore.

[35] F. Neri,"Comparing local search with respect togenetic evolution to detect intrusions in computernetworks," in *Proceedings of the 2000 Congress onEvolutionary Computation*, vol. 1, pp. 238–243, Mar-seille, France, July 2000. IEEE, IEEE. Source: IEEEXplore.

[36] WebsiteoftheHoneynetProject."Honeynetproject,".http://www.honeynet.org/.

[37] M. Otey, S. Parthasarathy, A. Ghoting, G. Li, S. Nar-ravula, and D. Panda, "Towards nic based intrusion detection," in *Proceedings of the ninth ACMSIGKDDinternationalconferenceonKnowledgedis-covery and data mining*, pp. 723–728. ACM, ACMPress, NY, USA, Aug. 2003. Poster Session: Indus-trial/governmenttrack.

[38] G.RamachandranandD.Hart,"Ap2pintrusiondetection system based on mobile agents," in *Proceed-ings of the 42nd annual Southeast regional confer- ence*, pp. 185–190. ACM Press New York, NY, USA,Apr.2004.

[39] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari,H. Yang,and S. Zhou,"Specification-basedanomalydetection:anewapproachfordetecting

network intrusions," in *Proceedings of the 9th ACMconference on Computer and communication security*, pp. 265–274, Washington D.C., USA, Nov. 2002.ACMPress.

[40] T.Song,J.Alves-Foss,C.Ko,C.Zhang,andK. Levitt, "Using acl2 to verify security properties ofspecification-based intrusion detection systems," in*Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July2003.

[41] G.Vigna, F. Valeur, andRichardA.Kemmerer, "Designing and implementing a family of intrusion detection systems," in *Proceedings of the 9th Europeansoftwareengineeringconferenceheldjointlywith10 thACM SIGSOFT international symposium on Foundations of software engineering*, pp. 88–97, Helsinki,Finland,2003.Source:ACMPortal.

[42] N.Ye,"Amarkovchainmodeloftemporalbehavior for anomaly detection," in *Proceedings of the 2000IEEE Workshop on Information Assurance and Security*,UnitedStatesMilitaryAcademy,WestPoint,NY,June2000.

[43] Ken. Yoshida, "Entropy based intrusion detection,"in*ProceedingsofIEEEPacificRimConferenceon Communications, Computers and signal Processing (PACRIM2003)*,vol.2,pp.840–843.IEEE,Aug. 2003.IEEEExplore.

[44] Ste. Zanero and Sergio M. Savaresi, "Unsupervisedlearning techniques for an intrusion detection sys-tem,"in *Proceedingsofthe 2004 ACM symposiumon Applied computing*, pp. 412–419, Nicosia, Cyprus,Mar.2004.ACMPress.

[45] F.Zhang,S.Zhou,Z.Qin,andJ.Liu,"Honeypot:a supplemented active defense system for network security," in *Proceedings of the Fourth InternationalConferenceonParallelandDistributedComput-ing, Applications and Technologies (PDCAT2003)*,pp.231–235.IEEE,IEEE,Aug.2003.

[46] R.Zhang,D.Qian,C.Ba,W.Wu,andX.Guo, "Multi-agentbasedintrusiondetectionarchitecture,"in *Proceedings of 2001 IEEE International Confer-ence on Computer Networks and Mobile Computing*,pp.494–501, Oct.2001.