**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 9, September 2014, pg.413 – 420***

**RESEARCH ARTICLE**

# AN INTELLIGENT APPROACH TO DETECT INTRUSION OVER WIRELESS

**Sonia**
Department of Computer Science & Engineering
R.N College of Engineering & Management, Rohtak
sonia.hooda92@gmail.com

**Vikram Nandal**
Department of Computer Science & Engineering
R.N College of Engineering & Management, Rohtak
vikramcse@live.com

***ABSTRACT:*** ***We use computers for banking and investing to shopping and communicating with others through email or chat programs. Computer and network of computer become the very important part of companies, organization and government sector. A lot of important information is stored in computers and transferred across networks and the internet. Unauthorized users may try to break into systems to have access to private information. This brings the need of a system that can detect and prevent those harmful activities. Intrusion detection systems (IDSs) monitor networks and/or systems to detect malicious activities. That helps us to re-act and stop intruders. There are two types of IDSs, network-based IDSs and host-based IDSs. A network-based IDS monitor's network traffic and activities to find attacks, and a host-based IDS monitors activities in a computer system to detect malicious actions. This thesis is a research on using Bayesian techniques in implementing a network-based IDS that can tell us a computer process is normal (harmless) or abnormal (harmful). We combine three techniques to build a IDS. In our system k2 algorithm is applied which main purpose is to incrementally add a node to a network, it means start with a single node than add another node to complete a network. Bayesian methods utilize a search-and-source procedure to search the space of DAGs, and use the posterior density as a scoring function and finally to construct a data structure called a junction tree which can be used to calculate any query through message passing on the tree. In a past a lot of research is done on a IDS but for a wireless network is little. We have combine three techniques to make sure that network is safe from unauthorized access and attacks.***

 

# 1. INTRODUCTION

If there are attacks on a system, we would like to detect them as soon as possible and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does. An IDS is a reactive rather than pro – active agent. Wireless network has a variety of threats; security issues are ranging from DOS to remote to local and local to root attacks. As we know that wireless network provides less security mechanisms then a wired network. So we need a wireless IDS which ensure us our network is protected from any kind of attacks.

# 2. TYPES OF IDS

## 2.1 Model Based Intrusion Detection:

The model based scheme consists of three important modules. The anticipator uses the active models and the scenario models to try to predict the next step in the scenario that is expected to occur. A scenario model is a knowledge base with specifications of intrusion scenarios. The planner than translates this hypothesis into a format that shows the behavior, as it would occur in the audit trail. It uses the predicted information to plan what to search for next. The interpreter then searches for this data in the audit trail. The system proceeds this way, accumulating more and more evidence for an intrusion attempt until a threshold is crossed; at this point, it signals an intrusion attempt.

## 2.2 Network Based Intrusion Detection:

The most obvious location for an intrusion detection system is right on the segment being monitored. Network-based intrusion detectors insert themselves in the network just like any other device, except they promiscuously examine every packet.

## 2.3 Host Based Intrusion Detection:

Host based IDs exploit vulnerabilities particular to specific operating systems and applications suites. Only host-based intrusion detection systems (The ones running as an application on a network-connected host) can correlate the complex array of system-specific parameters that make up the signature of a well- orchestrated attack.

# 3. CONTROL STRATEGY

Control strategy describes how the elements of an IDS is controlled, and furthermore, how the input and output of the IDS is managed.

## 3.1 Centralized:

Under centralized control strategies, or monitoring, detection and reporting is controlled directly from a central location (**Fig.1.1**).

 

## 3.2 Partially Distributed:

Monitoring an detection is controlled from a a local control node, with hierarchical reporting to one or more central location(s) (Fig 1.2).

## 3.3 Fully Distributed:

Monitoring and detection is done using an agent-based approach, where response decisions are made at the point if analysis (Fig 1.3).

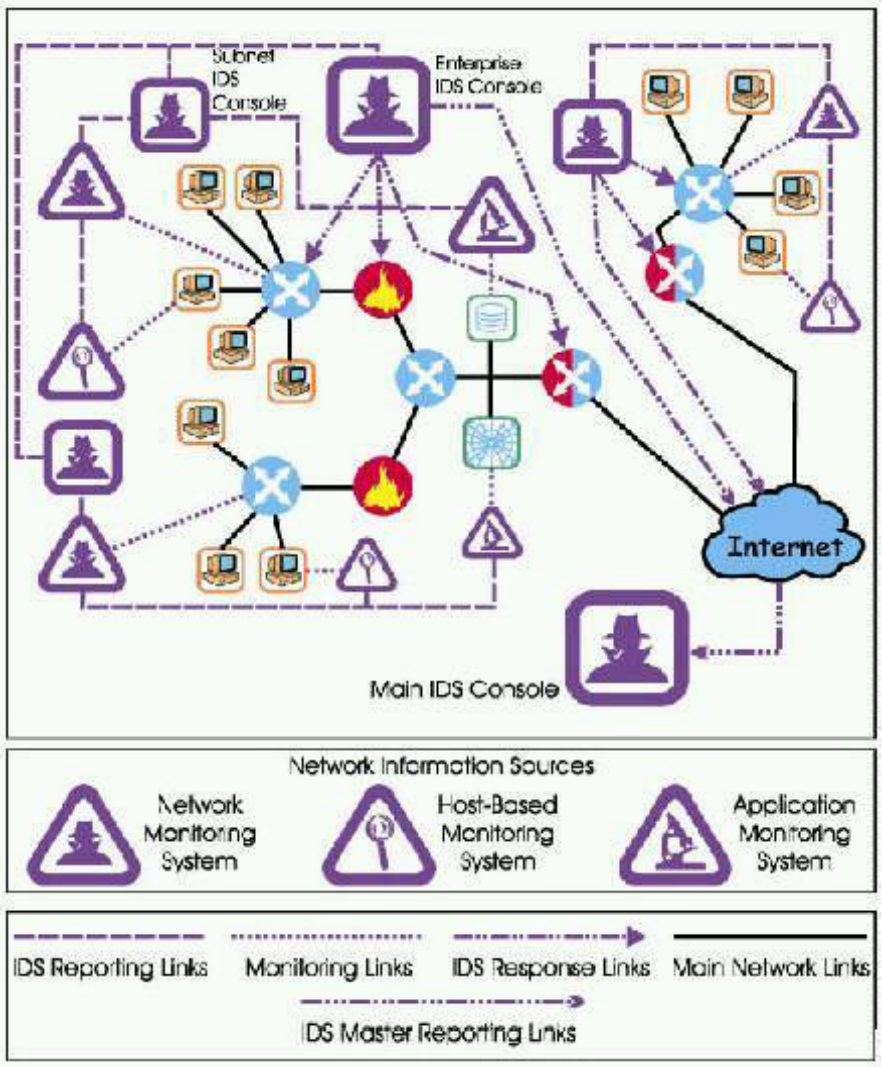


**Fig.1.1 Centralized Controls**

 

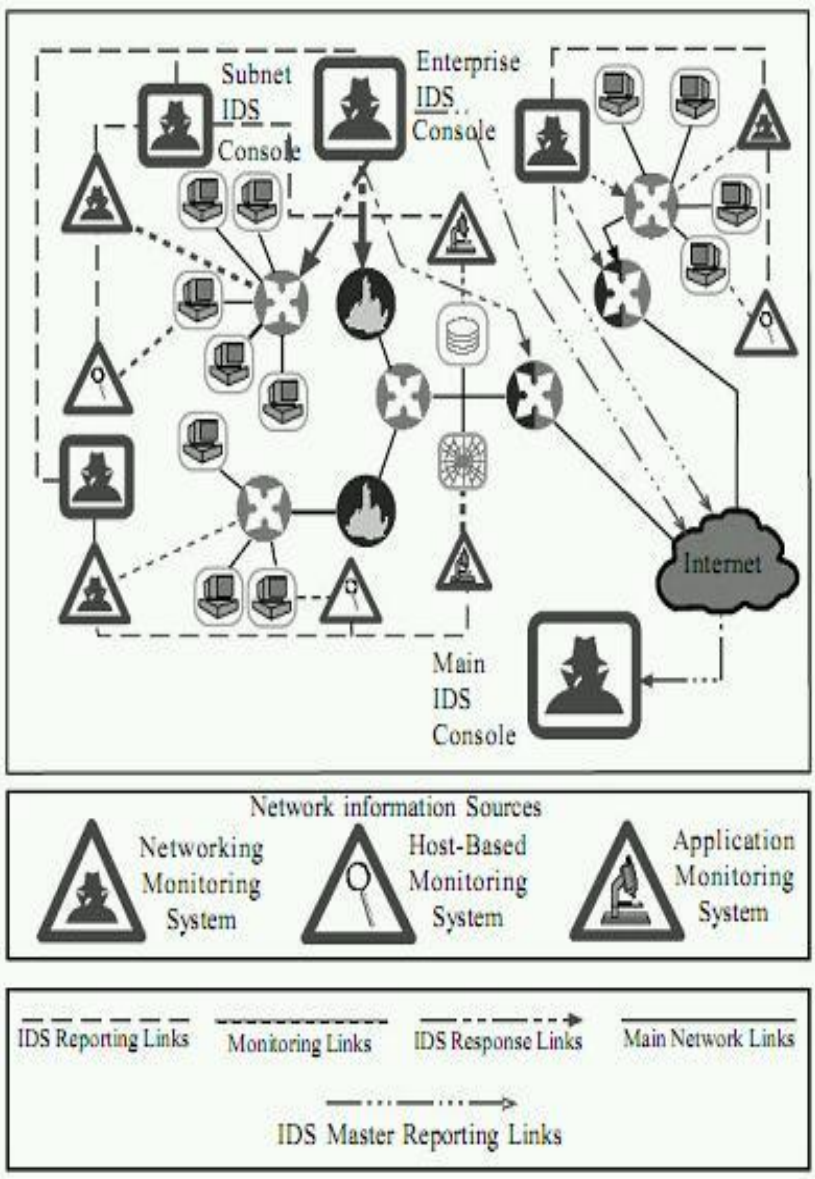


**Fig.1.2 Partially Controls**

 

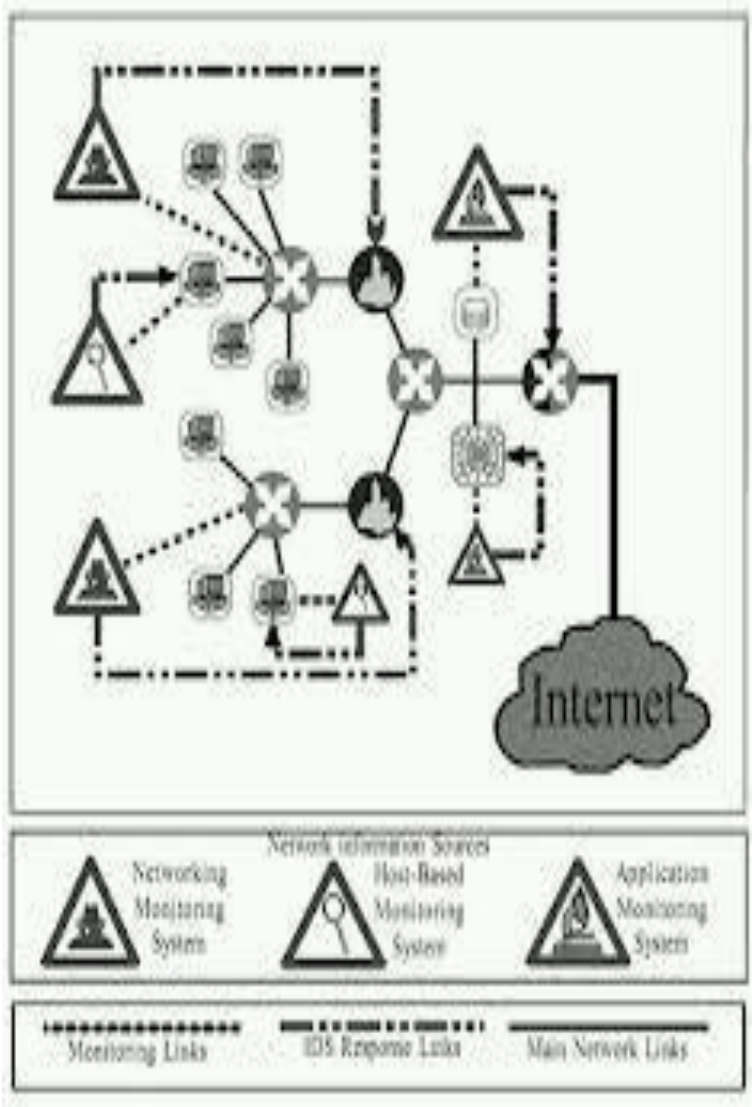


**Fig.1.3 Fully Control**

## 4. METHODOLOGY

### 4.1 K2 Algorithm:

In this thesis we are dealing with incomplete records in the database so we opted for the Bayesian approach and particularly for the Algorithm K2 used in learning step needs:

1. A given order between variables
2. The number of parents, u of the node.

K2 algorithm proceeds by starting with a single node showed high performance in many research works. (the first variable in the defined order) and then incrementally adds connection with other nodes which can increase the whole probability of network structure, calculated using the g.

### 4.2 Bayesian Recognition

These are probabilistic models very helpful when facing problems that require predicting the outcome of a system consisting of a high number of interrelated variables. A Bayesian network is used in detecting intrusion over a wireless network.

 

**Score-And-Search-Based Approach**:

It starts from initial structure generated randomly and then move to the neighbor with a maximum score in structure space or until local maximum criteria is selected. Score and search based approach for Bayesian network has three issues

**Search space:** The search space in Bayesian network structure learning is all the possible structures of directed acyclic graphs (DAGs) given the number of variables in the domain.

**Model selection criterion:** We focus on the Bayesian approach to model selection by which a model *M* is chosen according to the maximum posteriori probability given the observed data *D*:*P*(*M*|*D*) □□*P*(*M*,*D*) = *P*(*M*)*P*(*D*|*M*) = *P*(*M*)*Z*□ *P*(*D*|*M*,□)*P*(□|*M*)*d*□, where □□denotes the model parameters and □□denotes the domain of the model parameters.

## 4.3 Junction Tree Inference:

Junction tree used to calculate any query through message passing on the tree. Junction tree inference will create a network through which we can easily determine the unauthorized users or applications.

**Building Junction Trees:**

• To build a junction tree:

1. Choose an ordering of the nodes and use Node Elimination to obtain a set of elimination cliques.
2. Build a complete cluster graph over the maximal elimination cliques.
3. Weight each edge {B,C} by |B \ C| and compute a maximum-weight spanning tree.

This spanning tree is a junction tree for G.

• Different junction trees are obtained with different elimination orders and different maximum-weight spanning trees.

• Finding the junction tree with the smallest clusters is an NP-hard problem.

# 5. RESULTS AND DISCUSSION

## 5.1 K2 Learning:

A window will appear once we start intrusion detection system. It contain multiple buttons. Two browse button for selecting training and testing datasets. Firstly we have to click on the browse a dialogue box will appear on the screen so that we can select a training dataset which contain computer connection in a network. After selecting training dataset we have to select testing dataset IDS is ready to perform k2 learning process. After a click on k2 learning process what we get a different features of computer connection in a dataset, it shows the output in a record. Our system use only 9 features to detect intrusion in a network. It provides information in the form of records.

Bayesian recognition classify the systems behavior into two types:

- Normal
- Anomaly

Normal indicate that system is protected from any kind of attacks, and anomaly means that something happen wrong with system, it means some kind of attack is made by intruder. It also provide some parametric values for all features that are present in intrusion dataset, these values are very helpful in determining to which extent attack is made. The result of Bayesian recognition is a input to construct a junction tree.

 

**Table 1.1 Duration Attribute Value**

| Parameter | Normal | Anomaly |
|---|---|---|
| Mean | 0 | 0 |
| Standard Deviation | 0 | 0 |
| Weight Sum | 0.34 | 0.24 |
| Precision | 0 | 0 |

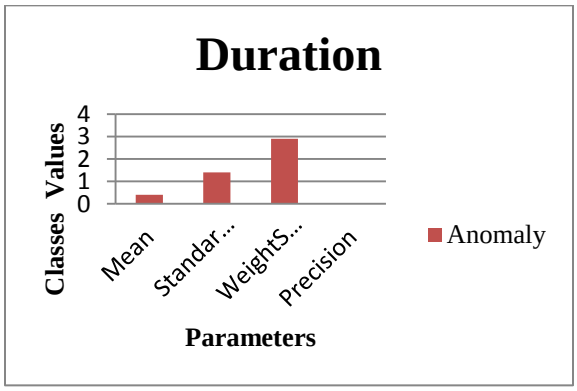


**Fig 1.4 Duration Attribute Value**

**Table 1.2 Num Failed Attribute Value**

| Parameter | Normal | Anomaly |
|---|---|---|
| Mean | 0.2 | 0.4 |
| Standard Deviation | 0.4 | 1.4 |
| Weight Sum | 3.4 | 2.9 |
| Precision | 0 | 0 |

Num_Failed_Login Attribute provides the information about the number of field logins with their corresponding values.

 

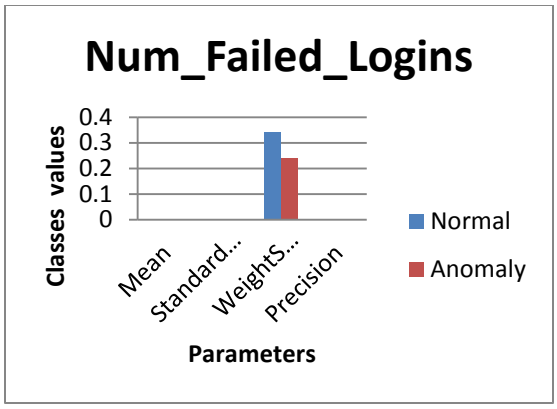


**Fig 1.5 Num_Failed_Logins Attribute Values**

### 5.3 Junction Tree:

Junction tree produce a final outcome which contain the information about all the connection or nodes respective with their Id no and it list the difference between actual and predicted class help us in ensuring whether the prediction was made correct or incorrect. By this means

we can able to determine that attack is made or not. It is the last module of our system which start working by constructing a network from DAG i.e. created by k2 learning process can also get the result of Bayesian recognition to determine the unauthorized access or application.

## 6. CONCLUSION

We have used probabilistic approach i.e. Bayesian network in detecting intrusion in network which seems to be very effective comparing with past IDS. It is a combination of three approaches: K2 Learning provides information in the form of records. The result of Bayesian recognition is a input to construct a junction tree and indicates about the system behavior either it is normal or anomaly. If system behaves normal it means system is protected from any kind of attacks and if behaves anomaly it means that something happens wrong. Junction Tree is the final outcome which is used to calculate query through message passing by this means we can able to determine that attack is made or not.

## REFERENCES:

[1] D.M. Chickering, "Learning Equivalence Classes of Bayesian Network Structure", Proceedings of the Twelfth Annual Conference on Uncertainty in Artificial Intelligence, Morgan Kaufmann, Reed College, Portland, Oregon, USA, pp. 150-157, 1996.

[2] G.F. Cooper, "An overview of the representation and discovery of causal relationships using Bayesian networks", AAAI Press and MIT Press, pp. 3-62, 1999.

[3] J. Pearl, "Probabilistic Reasoning in Intelligent Systems: Network of Plausible Inference". Morgan Kaufmann, 1997.

[4] P. Spirtes, C. Glymour, R. Scheines, "Causation, Prediction and Search (Second Edition)", MIT Press, Cambridge, MA, USA, 2000.

[5] N. Friedman, D. Koller, "Being Bayesian About Network Structure: A Bayesian Approach to Structure Discovery in Bayesian Networks", Machine Learning 50 (1-2), pp. 95-125, 2000.

[6] F .Jemili, M. Zagdoud, "A Framework for an Adaptive Intrusion Detection System using Bayesian Network" *Monuba University Tunisia, 2010*.

 