PROBABILISTIC AND DETERMINISTIC CRYPTO ANALYSIS

M. Thiyagarajan[1], S. Samundeeswari[2]

[1] Professor, School of Computing, SASTRA University, Thanjavur
[2] Senior Faculty, School of Computing, SASTRA University, Thanjavur
E-mail: m_thiyagarajan@yahoo.com, samu_sivi@yahoo.com

ABSTRACT

In Network Security various attacks have been identified at different stages of intrusion and attempts. Security measures are designed for overcoming individual attacks. These attacks are random in nature and an attempt is made to the multi scale autoregressive model to combine all attempts to attack a network and to measure the total damage done to the machine or network.

Keywords: *Multiscale auto repressive process, Detailed Coefficients, Cryptographic attacks, Linear Model, Discrete Wavelet Transform*

1. INTRODUCTION

A Significant security problem for networked systems is hostile, or at least unwanted, trespass by users or software. User trespass can take the form of unauthorized logon to machines or in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized. Software trespass can take the form of a virus, worm or Trojan horse. One of the two most publicized threats to security is the intruder (the other is viruses), generally referred to as a hacker or cracker. In an important early study of intrusion, Anderson [1] identified three classes of intruders

1. Masquerader
2. Misfeasor
3. Clandestine user

Inevitably, the best intrusion prevention system will fail. A system's second line of defense is intrusion detection, and this has been the focus of much research in recent years.

We identified the following approaches to intrusion detection [2]

2. STATISTICAL ANOMALY DETECTION:

Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observe behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

3. RULE BASED DETECTION:

Involves an attempt to define a set of rules that can be used to divide that a given behavior is that of an intruder.

The requirements of Information Security in an organization have undergone two major changes for automated tools for protecting files from hackers is computer security. Network security measures are needed to protect data during their transmission between terminal user and computer, between computer and computer. There are no clear boundaries with in these two forms of security. Each attack and its damage to a system is being modeled and studied separately by different users under various platforms and systems designs. The simultaneous and over all damage and ultimate halt of an operating system is to be given in such a way that the inter dependency between various attacks is to be studied. The attack by different hackers can be viewed as a time series with different scales and different origins. As such we are led to give a multi-scale auto regressive time series model for the over all damage by different hackers. Each one is probabilistic in nature and we need to estimate the coefficients of the partial regression of one and the ultimate.

The ultimate damage experienced by an organization through different types of attacks is to be designed so as to make measures for controlling such attacks, the joint covariance are considered. Here we take up four major attempts to attack an organization. A model of the form

$$\bar{Y} = A\ \bar{X}$$

is derived where $\bar{Y}$ is the ultimate damage vector (y_1,y_2,y_3,y_4) and A is covariance matrix

with $$a_{ij} = E\left\{ (x_i - \bar{X}_i)(x_j - \bar{X}_j) \right\}$$

and $\bar{X} = (x_1,x_2,x_3,x_4)$. This in turn put in to wavelet transmission to refine the coefficients to origin and scaling.

Thus we obtain a multi scale auto regressive model along with wavelets refining the coefficients. This gives a measure of approximation to the ultimate damage to the network through different attacks. This model can be generalized to any number of individual attempts and thus giving a better service after the control.

4. BASIC CONCEPTS

4.1 MAR PROCESS

Multi Scale autoregressive (MAR) process [3] are tree - indexed stochastic process. We can consider only dyadic trees. Our notation for referring to nodes of a dyadic tree is indicated in (figure). The root node represents the coarsest scale which we denote as scale zero. The children of the root node represent the first scale. Continuing leaf nodes constitutes the finest scale which we denote as the jth scale. We will denote by x_j the stacked vector consisting of $x_j(n)$ for n=0,1,…2j-1 that is the finest scale-sub process.

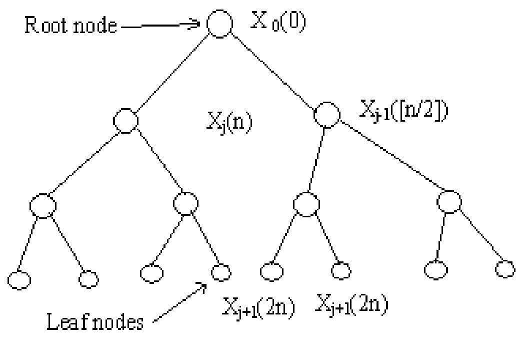

Figure1. A MAR process on a dyadic Tree. The root node state is $X_0(0)$. The parent of state $X_j(n)$ Is $X_{j-1}([n/2])$ while its children are $X_{j+1}(2n)$ and$X_{j+1}(2n)$

$$x_j(n) = A_j(n)\, x_{j-1}([n/2]) + W_j(n) \qquad (1)$$

We have showed that through a particular definition of the state vector $x_j(n)$, the MAR dynamics can be chosen to match the reconstruction algorithm associated with any compactly supported orthogonal or biorthogonal wavelet.

Given the statistics of a random signal which we view as indexed by the leaf nodes of a tree, we focus on building a MAR model to capture those given statistics with high fidelity [4]

An important property is that MAR process possesses is wide-sense Markovianity. This MAR "Markov property" as we shall call it is a generalization of the wide-sensee Markovianity of state-space processes. For a state-space process, the present is a boundary between the past and future in that it conditionally décorrelates them, Analogously, for a MAR process, the node (j, n) is a boundary between the sub-trees extending away from it; the value of the MAR process indexed by these sub trees are mutually conditionally décorrelated by $x_j(n)$, the Markov property means that $x_j(n)$ summarizes all the relevant stochastic properties of one sub-tree leading from (j, n) for optimal statistical reasoning about the other sub-trees leading from(j, n) and therefore justifies our terminology in calling $x_j(n)$ a MAR state.

4.2 ADVANTAGES OF INTERNAL MAR PROCESS

An internal MAR process is one for which the state at every node (j, n) is a linear functional of the states which reside at the fine-scale nodes which descend from (j, n) in general there are no constraints on how the MAR states should be defined but internality is a property which is very useful for many reasons.

Internal models are intellectually important in the context of statistical modeling and are widely used in stochastic realization theory for time - series.

In many applications there is need to fuse measurements taken at different scales. Frequently, the non-local coarse-scale variables (example tomographic measurements). Since internal MAR models include as coarse states non-local functions of the finest scale, they allow efficient fusion of non-local and local measurement with no increase in complexity as compared to the case of fusing only fine scale data. Internality provides a convenient parameterization of the information content of the MAR states. Using this parameterization leads to the MAR dynamics that incorporate a powerful optimal prediction of a child state from its parent. This optimal prediction will have important and significant consequence for out ability to accurately models signals using MAR processes based on wavelets.

4.3 WAVELET-BASED INTERNAL MAR PROCESSES [5]

We use the statistics of the process to be modeled to derive the dynamics of our internal MAR - wavelet models. While wavelet have nice de correlation properties, the de correlation that provide is not exact in general therefore, our MAR models based on wavelets are approximate.

1. In the internal models, we assumed that prediction errors are white. This assumption is the reasons that white noises are children of the *Brownian motion.*

2. Another property that MAR process must posses is low state dimensionality.

We will see that the state dimension of our MAR - wavelet models grows only linearly with the lengths of a support of the scaling functions, which are related in some cases, such as orthogonal wavelets, to the number of vanishing movements of analyzing wavelet. However the fact that wavelets with a large number of vanishing moments do a good job of whitening and stationarization a large class of process does not imply that the degree of statistical fidelity of our internal models necessarily increases with the number of varnishing movements.

With internal MAR - wavelet models it is possible to build accurate models using wavelets with fairly short supports and thus without dramatically increasing the state dimension. We use the fine-scale statistics of the process to be modeled to derive the dynamics of the MAR model.[6]

The first decoupled dynamics wavelet system that support a fast estimation algorithm whose structure takes the form of a set of monadic trees in scale. The second generalize the work in to wavelet packets and develops a fast estimation framework whose structure takes the form of a set of dyadic trees. They assumed that the detail co-efficients are white.

In our models, we make no such assumption to perform estimation in the frameworks of the data must be transformed into the wavelet domain. Therefore, there no way to handle sparse or irregular measurements which our framework can handle easily.[7]

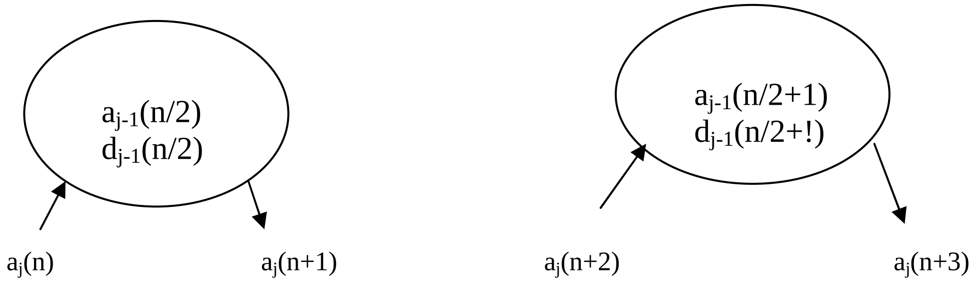

Figure 2. The Haar dependency graph is a dyadic tree. Harr n is even

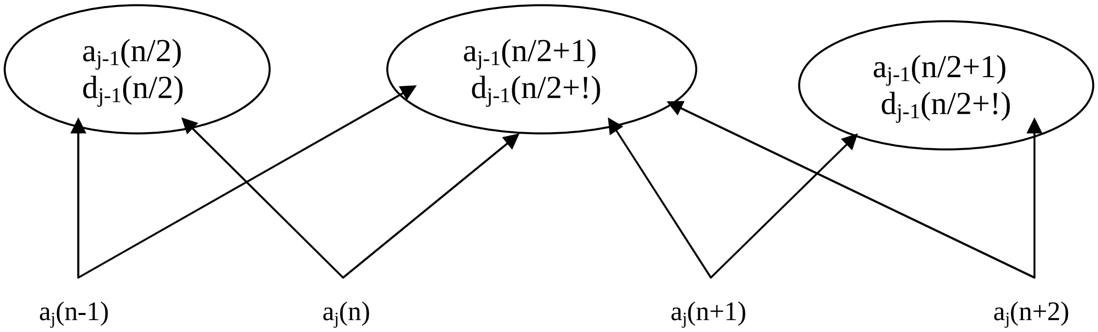

Figure 3. Dependency graph for the Daubechies 4-tap filter. Here n is even

The following diagram is the example of the internal MAR – Wavelet process with the Daubechies 4-tap filter, Scaling coefficients in bold illustrate the necessary transmitted from one scale to the next. The boxed coefficients are a linear function of the coefficients of the children by the wavelet decomposition algorithm.

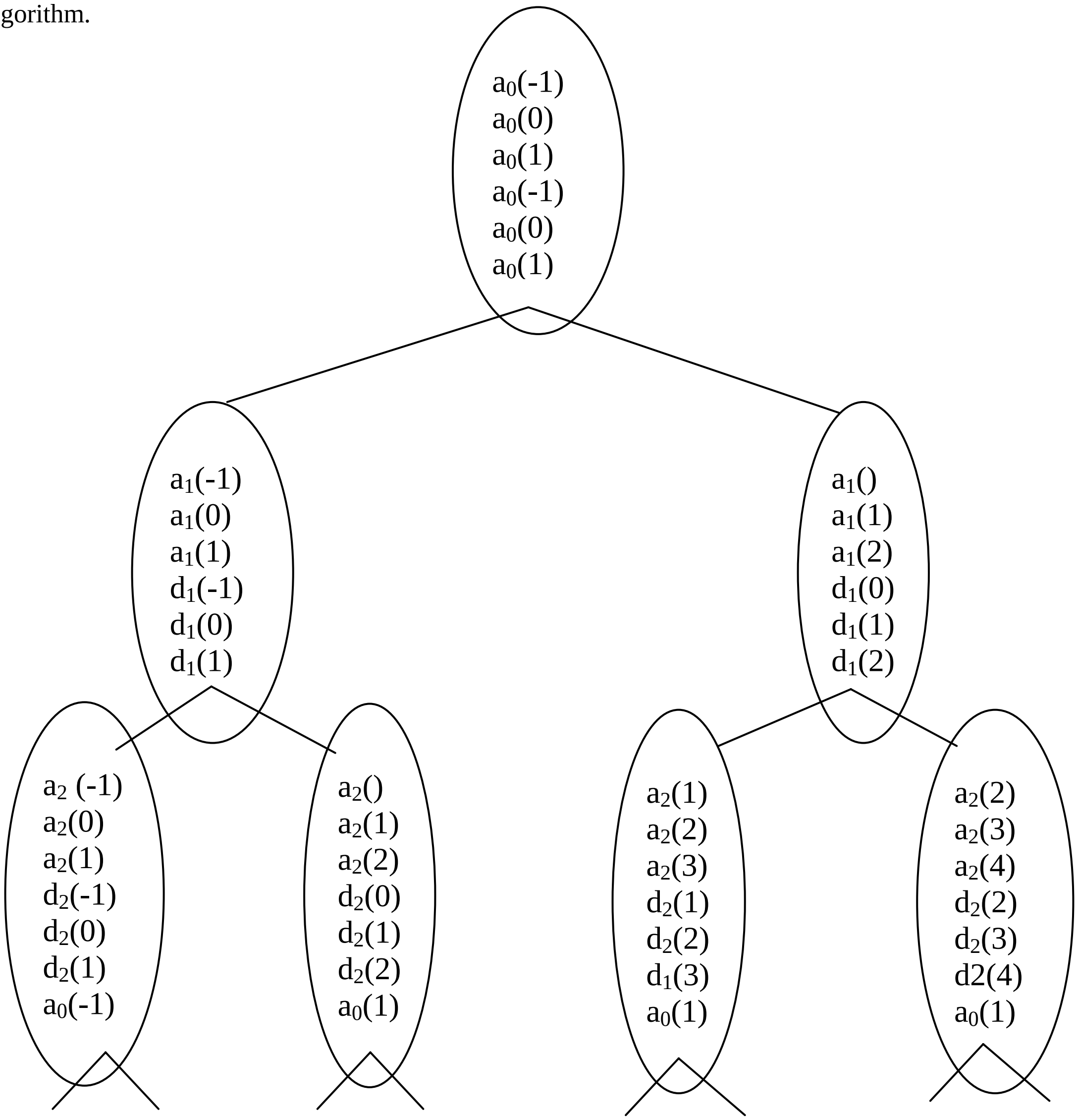

Figure 4. Example of Internal MAR-Wavelet process

5. PROBLEM FORMULATION

We consider for our discussion the three major types of attacks namely interruption, modification and fabrication. As the attempts are random in nature we take them as the outcome of a periodic Markov chain sending to limiting distribution which is uniform. We consider the covariance matrix of the joint attack of the three and these coefficients are subjected to convolution product of discrete wavelet transform to adjust for location and scaling. We fit the model in the refined form

$$\bar{Y} = \mathrm{c}\ \bar{X}$$

6. DATA AND ANALYSIS

X_1 = 73,35,3,11,57,30,2,17,21,38,6,2,5,8,4,3
X_2 = 4,4,16,26,8,1,9,7,8,3,7,13,4,2,2,2
X_3=19,55,12,17,76,90,2,33,30,29,154,48,3,12,24,4
X_4 = 22,9,56,82,66,11,32,59,12,9,55,9,1,2,19,11

$$\begin{pmatrix} C_{11} & C_{21} & C_{31} & C_{41} \\ C_{12} & C_{22} & C_{32} & C_{42} \\ C_{13} & C_{23} & C_{33} & C43 \\ C_{14} & C_{24} & C34 & {}^{C}44 \end{pmatrix} \begin{pmatrix} X1 \\ X2 \\ X3 \\ X4 \end{pmatrix} = \begin{pmatrix} Y1 \\ Y2 \\ Y3 \\ Y4 \end{pmatrix}$$

Where

C_{11} = 1,
C_{21} = -0.234911,
C_{31} = 0.164347,
C_{41} = -0.0488822,
C_{12} = -0.234911,
C_{22} = 1,
C_{32} = -0.104447,
C_{42} = 0.602825,
C_{13} = 0.164347,
C_{32} = -0.104447,
C_{33} =1,
C_{43} = 0.187686,
C_{14} = -0.0488822,
C_{24} = 0.602825,

$$\bar{Y} = \mathrm{CX}$$

Values of discrete wavelets are

$$\begin{pmatrix} 0.34151 \\ 0.59151 \\ 0.15849 \\ -\ 0.\ 09151 \end{pmatrix}$$

7. OUTPUT

For $X_1 = 73$, $x_2 = 4$, $X_3 = 19$, $X_4 = 22$

$Y_1 = 74.1$, $Y_2 = -1.870503$, $Y_3 = 34.6934$, $Y_4 = 24.4072$

8. CONCLUSION

We have followed the analysis given by Khalid Daoudi, et al, on the Multi Scale Auto Regressive Model and wavelets to our problem. This results obtained give a better understanding of the joint impact of major attacks to a crypto system. The combined effect will be given by a linear non in inner product space of these vector.

9. REFERENCE

[1] T W Anderson – The Statistical Analysis of Time Series, Wilay – New York, 1971

[2] William Stallings - Cryptography and Network Security- Pearson education press, New Delhi, 2003.

[3] Khalid Daoudi, Austin B.Frakt, Student member IEEE and Alan S.Willsky, Fellow, IEEE - Multiscale Autoregressive Models and Wavelets- IEEE Transaction on Information Theory ,Vol 45 ,Number 3 ,April 1999.

[4] I.Daubechies-Ten Lectures on Wavelets - SIAM -USA, 1992

[5] P.Flandrian .Wavelet analysis and Synthesis of fractional Brownian motion,. IEEE Trans. Inform Theory, Volume 38, pp 910-917, March 1992

[6] P. Abry and F.Sellan, -The wavelet- based synthesis for fractional Brownian motion proposed by F.Sellan and Y.Meyer: Remarks and fast implementation,. - Appl. Computational Harmonic Anal., vol .3, pg377. 383, 1996

[7] J.Medhi -Stochastic Process.-Wiley Eastern Ltd –New Delhi, 1984