PROTECTION OF THE MIL-STD-1553 WITH DISCRETE WAVELET ALGORITHMS

Aaron Fansler
Ampex Chief Technologist

Ampex Intelligent Systems
4040 E. Bijou
Colorado Springs, CO 80909
afansler@ampex.com
303-909-8669

Abstract

This paper reviews at a high level Ampex's Black Lightning capability. The Black Lightning capability tool was developed to be the first cyber defensive tool specifically designed to work at the field device component level of a Control System (CS). BLACK LIGHTNING is a passive, real-time monitoring and detection tool designed and built specifically for control systems professionals. The BLACK LIGHTNING capability uses a patent pending detection algorithm, which scans SCADA specific protocols for any anomalous activity within the customer defined component thresholds. In doing this BLACK LIGHTNING is able to alerting operators of any abnormal activity for further investigation faster than anything currently on the market.

One can look at the internals of an aircraft as multiple layers of control systems working together. As defined, "A control system is a collection of mechanical and electrical equipment that allows an aircraft to be flown with exceptional precision and reliability". An aircraft has many control systems. These systems consist of fuel, heat, speed, altitude, hydraulics, navigation, communications, sensors, actuators, servos, multiple computers just to name a few as examples.

At Ampex, we view a control system as what it is, a control system. The process(es) above that the control system(s) is transparent to us. If you protect the system and subsystems below the process then by default you will protect the process above regardless if it's an industrial power plant, nuclear power plant, water facility, manufacturing plant or an aircraft. At Ampex we protect the process by monitoring and protecting the systems below.

Introduction

MIL-STD-1553 is a military standard developed by the US Department of Defense (DoD) for the purpose of military platform integration [6] which has served as the backbone of military and aerospace avionic platforms (e.g., F-15, AH-64 Apache, F-16, V-22, X-45A, F-35) for more than 40 years. It is primarily used for mission-critical systems that require a high level of fault tolerance, since it is deterministic and dual redundant; it also uses a reduced cable topology, connecting all devices on a single bus in a multipoint topology, as opposed to point-to-point topologies.

MIL-STD-1553 is considered deterministic, because it is based on a master/slave methodology in which the master issues messages based on a predefined order and timing. Although other modern, reliable and deterministic data buses have been introduced MIL-STD-1553 remains the most widely used standard in military aviation as it has been for the last 40 years, and is expected to be used in the future. The main reason that alternative deterministic communication buses are not used in existing platforms is the difficulty of modifying an entire operational platform and replacing the main data transmission topology. Moreover, subsequent standards are based on the communication protocol defined by MIL-STD-1553. For these reasons, MILSTD-1553 will likely be an integral component of critical military platforms for many more years to come.

MIL-STD-1553 was developed long before the notion of cybersecurity was familiar and even basic cyber-attacks, such as denial-of-service (DoS) attacks, had not yet been introduced. Research regarding DoS attacks initially reported in the early 1980s, several years after the release of the most recent version of MIL-STD-1553 in 1978, and focused mainly on DoS in operating systems, rather than computer networks.

Much like the present monitoring systems of control networks such as power systems, relies a lot on state estimation, which is based on SCADA data collected from field devices such as Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs) and sent up to the control system. If one looks at an aircraft and views it as multiple integrated subsystems it is very easy to see that there are a lot of similarities of an integrated control systems, it is easy to tackle the problem of protecting an aircraft in a similar manner of protecting a ground based control system.

The potential vulnerabilities of both an aircraft and electric power control system are inherently different but the result of the attack or effect are very similar. In both cases, the operator / pilot has no ability to detect an intrusion or malicious attack at the time it occurs and is only able to speculate that there may have been an event if the particular event yields distinguishable changes to the network. Attacks such as Stuxnet would never have been detected on the operator display modules.

There are three (3) major problems with the lack of defensive capabilities for control systems:

1. Industry has not developed many defensive capabilities ***specifically*** for control systems
2. Majority of capabilities only protect at the management level of a ICS (i.e. Operator Console or HMI (Human Machine Interface))
3. Most available capabilities are signature based

In the case of an aircraft control system(s) it's only true defense being so called "air gapped" or being a fast moving target and not allowing an attacker enough dwell time to conduct an attack. Most experts would disagree that protection via these statements. The MIL-STD-1553 is public knowledge, papers and books have been printed on the topic. The question now should be not how can we protect this but how can we detect this. You must be able to monitor and detect long before you can ever protect.

The biggest problem of the three is the reliance on signature-based tools. In signature-based techniques a sequence of instructions unique to a malware is used to generate a malware signature, which is captured by researchers in a laboratory environment. In order for a signature-based capability to be effective during an attack, the research community must have already discovered the specific attack scenario, developed the set of instructions necessary to yield this particular attack ineffective, relayed this information to industry, industry must have already updated their tool and the ICS network in question must have updated their signature-based tool appropriately such that it contains the current library of signatures.

Ampex plans to address all three problems with BLACK LIGHTNING.

BLACK LIGHTNING

Einstein is attributed with having said "If I can't picture it, I can't understand it". Information assurance today is ineffective because decisions are based on an incomplete picture with security gaps. Effective protection of a network can only occur if decisions are based on an integrated contextual picture resulting from real-time awareness of the network components

and especially network traffic. BLUE LIGHTNING was designed with this specific point in mind, to be able to help operators identify and quickly respond to threats and risks in their automation systems and gain a clear view of the activities occurring within their environments.

AMPEX presented "Embedded Endpoint Protection" at the TechConnect Defense Innovation Technology Acceleration Challenges in Tampa last fall. The point of the presentation was that the AMPEX BLUE Lightning capability for industrial control system cyber protection could be adapted to protect military systems, such as aircraft.

The capability is based on a patented algorithm and specialized software that monitors the operation of control protocols and detects the behavioral changes in the protocol stream. These changes are indicators of process abnormalities which can be due to equipment pending failure, misconfigurations, or in the worst case, injection and operation of malware on a bus or in a network. Blue Lightning is deterministic, not heuristic or based on machine learning. It does not employ malware signatures. First marketed this year and going operational with installations at DOE Laboratories PNNL and INL, the target is commercial energy system operators. An adjacent opportunity is to adapt the algorithm to aircraft control protocols to detect system abnormalities, malware, and prevent data spoofing while providing process resiliency. Inherent in the product is the ability to counteract the effects of malware based on predetermined decisions. In a larger view, this detection technique can serve as the basis for cooperative detection, automatic analysis, and countermeasures among the aircraft in a strike package or similar interconnected formation.

AMPEX has modified and adapted Blue Lightning to detect malware and especially spoofing attempts in MIL-STD-1553B, the bus standard that dominates avionics control and the control systems and subsystems associated with an aircraft. We call this new modification “Black Lightning”.

The BLACK LIGHTNING is made up of both software and distributed hardware components. The logical evolution was to bring BLACK LIGHTNING to aircraft as a SWAP optimized appliance, a miniaturized component, application software of other systems already aboard aircraft. The first step is to run that algorithm against experimental data sets of MIL-STD-1553B data to optimize the algorithm for effective operation in this protocol’s respective. Called BLACK Lightning, it is an aircraft version of BLUE Lightning. BLACK LIGHTNING can be hosted on a standard aircraft Network File Server (NFS) or mission recorder and that host can fit into the available space, whether as a TS 282, TS 480, TS 640, TuffCORD, or other device tailored to a specific SWAP budget. This obviates any need to add equipment to an already cramped airframe. Once loaded, the core complex mathematical algorithm creates a “digital fingerprint” of all associated and programed network data. This algorithm has been determined to be very useful for detecting anomalous activity in CS network traffic both analog and digital.

The detection algorithm that works specifically as a SCADA traffic anomaly detector operated in real-time by passively monitoring data objects inside of a SCADA protocol stack as it’s passed from one device to another device. BLACK LIGHTNING collects and statistically analyzes the normal protocol patterns of the data object for sudden changes and then calculates to determine if the current traffic is behaving in an unordinary manner based on our initial baseline. We use this technique to detect anomalies in protocol network traffic behavior.

Software

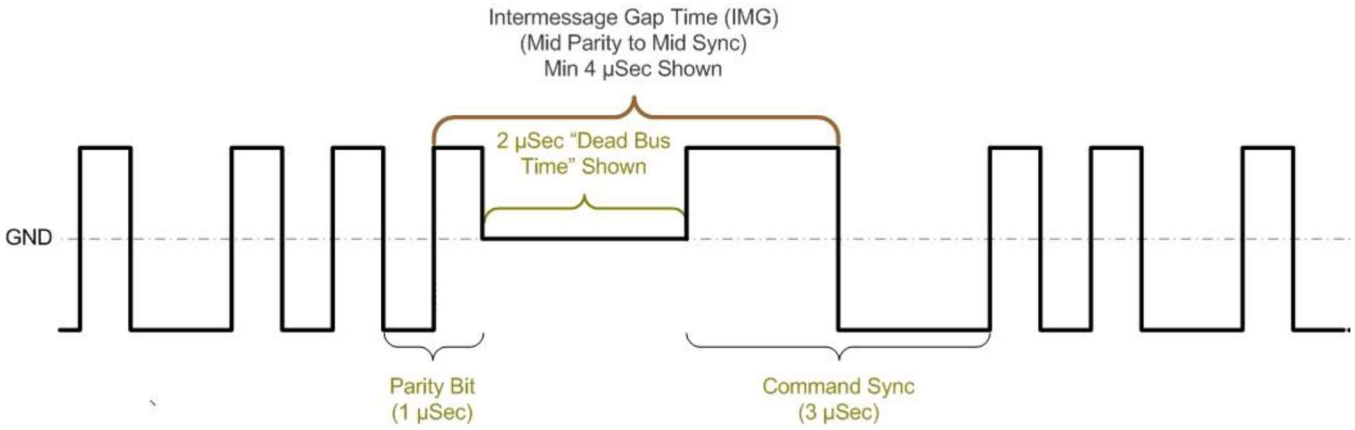
The network traffic is collected by the BLACK LIGHTNING sensor and the algorithm breaks the identified traffic (data) into its wavelets, which are then scaled and shifted versions of a single waveform. The signal is then reconstructed only from those wavelet coefficients that reach the alert thresholds which are determined based on the specific customer requirements for their specific network. By extracting local information regarding the signal in time and frequecy domains, malicious attacks may be detected using the changes in data charceteristics.

This type of analysis is suitable for non-stationary signals produced by control systems. The irregularity in shape and compactly supported nature of wavelets make wavelet analysis an ideal tool for analyzing signals of a non-stationary nature.

A 1553 network (or “data bus” in older terms) is a heterogeneous architecture where the various computers (terminals) on the network have a master/slave relationship. Message communication is controlled by one master terminal/computer called the Bus Controller (BC). The BC initiates all communications between computer-network end points, which are called Remote Terminals (RTs). There can also be passive Monitor terminals (“Bus Monitor – BM”) that “sniff” or record bus traffic (message packets).

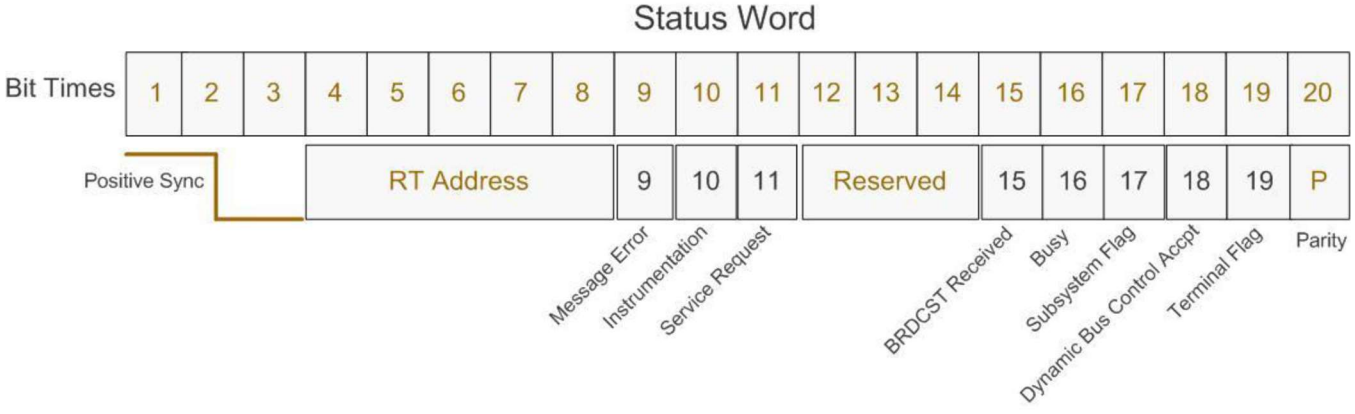
A 1553 network is time division, half duplex communications where all transmissions are on a single cable (unlike full-duplex Ethernet, RS-232/422 or ARINC-429 where separate transmit and receive wires are utilized). Only one computer terminal can talk/transmit at any given time (time division) and the other computers listen/receive (full duplex systems like Ethernet and RS-232 allow simultaneous transmit and receive on different wires).

BLACK LIGHTNING can monitor both analog and digital signals. 1553 does allow for Broadcast option (like an Ethernet UDP multi-cast) of certain message types to allow data or Mode Codes to be simultaneously issued to multiple RTs. The 1553 protocol does not implement any CRC or Forward Error Correction, just a simple “command-response” protocol to handshake data. We know that all 1553 words are 20 µSecs in time, one bit per µsec and there are 16 bit words with 3 bits of sync and one bit of odd parity. This is an example of a variable we can monitor for and develop a baseline against for protection.



We also know structure of a 1553 Data Word which is the information passed between the computers (BC and RTs) on the 1553 network. The figure below shows a Data Word Format. With analyzers, Data Words are usually shown in standard hex nibbles.

Words are the data structure used for transmitting commands, data, and status over the bus. A collection of words defines a message used for receiving or transmitting data. Messages can be periodic or aperiodic. Periodic messages are sent at fixed time intervals (i.e., time cycles). A major frame is a predefined time frame in which all periodic messages are transmitted at least once (derived from the periodic message with the longest time cycle). Aperiodic messages are event-driven and therefore are not sent in fixed time cycles. However, they have a fixed time slot in the major frame.



Hardware

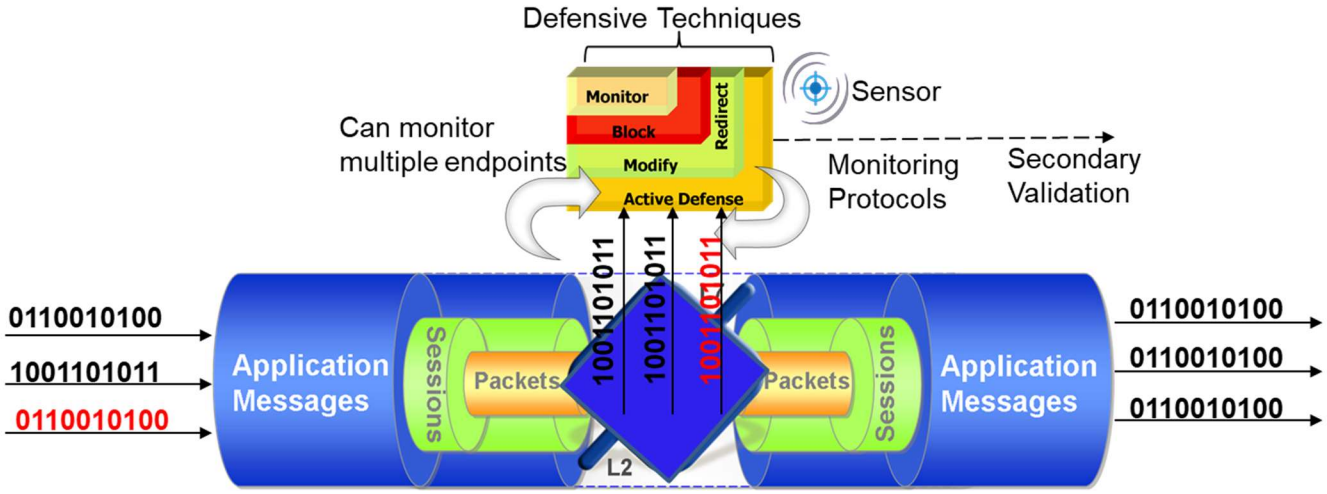
The BLUE LIGHTNING hardware consists of a server which operates as the master controller for the mesh sensor network. However, BLACK LIGHTNING will be hosted on a standard aircraft Network File Server (NFS) or mission recorder and that host can fit into the available space, whether as a TS 282, TS 480, TS 640, TuffCORD, or other device tailored to a specific SWAP requirements.

Algorithm

We developed a Discrete Wavelet Transforms (DWT) algorithm that scans control specific protocols for signs of abnormal and/or malicious of network data. This technique will be very useful for intrusion detection including third party interference.

Our algorithm takes the raw packet traffic and breaks the signal (data stream) into its wavelets, which are scaled and shifted versions of a single waveform known as the mother wavelet. We selected to build on wavelet analysis due to its suitable for non-stationary signals produced by infrastructural systems. The irregularity in shape and compactly supported nature of wavelets make wavelet analysis an ideal tool for analyzing signals of a non stationary nature. Their fractal nature allows them to analyze signals with discontinuities or sharp changes, while their compactly supported nature enables temporal localization of a signal's features. We selected to develop our detection algorithm upon Wavelet Transforms because:

- Wavelet Transforms are very good tools to extract local information regarding a signal in time and frequecy domains. This property of the wavelets can be used to detect the malicious attacks using the changes in data charceteristics.
- The wavelet analysis is capable of revealing aspects of data that other signal analysis techniques miss, aspects like trends, breakdown points, discontinuities in higher derivatives, and self similarity.
- Because wavelet analysis gives different views of data, it can compress or denoise a signal without appreciable degradation of the signal.
- Wavelet transforms decomposes a given signal into shifted (translation) and scaled (dilation) versions of the mother wavelets represented by different coefficients called "Approximations" and "Detail Coefficients".
- The different approximations and detail coefficients represent the signal at different resolutions. A given signal is decomposed using low pass filters giving approximations and high pass filters giving the detail coefficients.



In order to minimize redundancy we have used Discrete Wavelet Transform (DWT). In this method the discrete scales as well as corresponding sampling intervals differ by a factor of two (dyadic sampling).

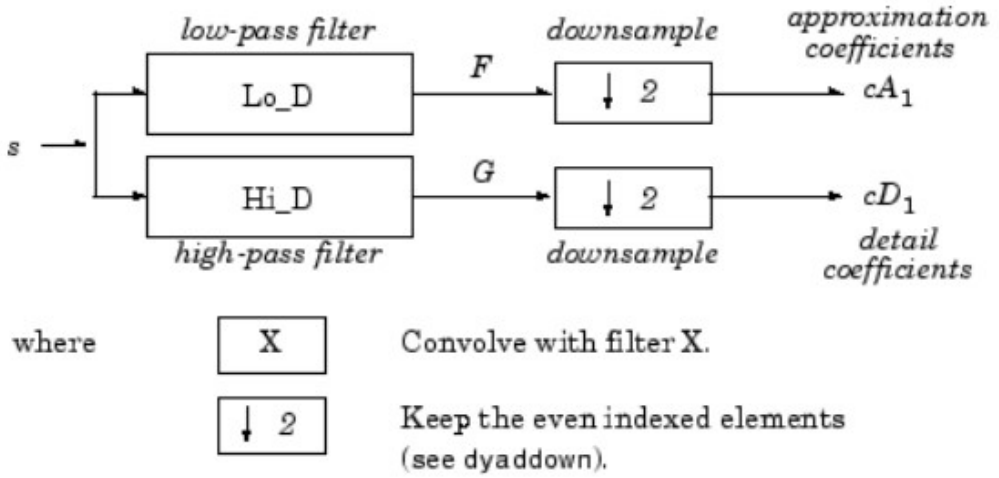
From our evaluation we selected to use DWT which produces two sets of constants termed as approximation and detail coefficients. The approximations are the high-scale, low frequency components of the data stream. The detail coefficients are the low-scale, high-frequency components. The dialation function of the discrete wavelet transform can be represented as a tree of low and high pass filters, with each step transforming the low pass filter. The signal is passed through a series of high pass and low pass filters to analyze respective functions at each level.

Discrete Wavelet Transform:

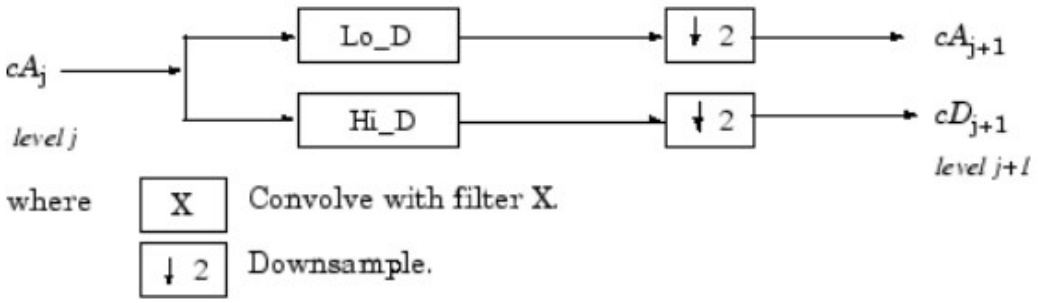
DWT is any wavelet transform which wavelets are sampled discretely. The main advantage of DWT is to capture both frequency and location information.

Decomposition

For a given signal s, by convolving with low-pass filter and high pass-filter, followed by down sampler we can obtain approximation and detail, respectively. The first step is shown below:



The next step we obtain new approximation and detail coefficients by splitting the previous approximation coefficient and so on.



At each decomposition level, the half band filters produce signals spanning only half the frequency band. This doubles the frequency resolution as the uncertainty in frequency is reduced by half

In accordance with Nyquist's rule if the original signal has highest frequency of ω, which requires a sampling frequency of 2ω radians, then it now has a highest frequency of ω/2 radians.

- It can now be sampled at a frequency of ω radians thus discarding half the samples with no loss of information.
- This decimation by 2 halves the time resolution as the entire signal is now represented by only half the number of samples.
- Thus, while the half band low pass filtering removes half of the frequencies and thus halves the resolution, the decimation by 2 doubles the scale.

Wavelet analysis starts by selecting basic wavelet function, called the mother wavelet (e.g., Haar Wavelet), wavelet representation of a signal can be given by:

$$f(t) = \sum_{k=-\infty}^{+\infty} a_{0,k}\,\phi(t-k) + \sum_{k=-\infty}^{+\infty}\sum_{j=0}^{j-1} d_{j,k}\psi(2^j t - k)$$

Scaling Function:

$$\phi(t) = \begin{cases} 1 & ,0 \le t < 1 \\ 0 & otherwise \end{cases}$$

Wavelet Function:

$$\psi(t) = \begin{cases} 1 & ,0 \le t < \frac{1}{2} \\ -1 & ,\frac{1}{2} \le t \le 1 \\ 0 & otherwise \end{cases}$$

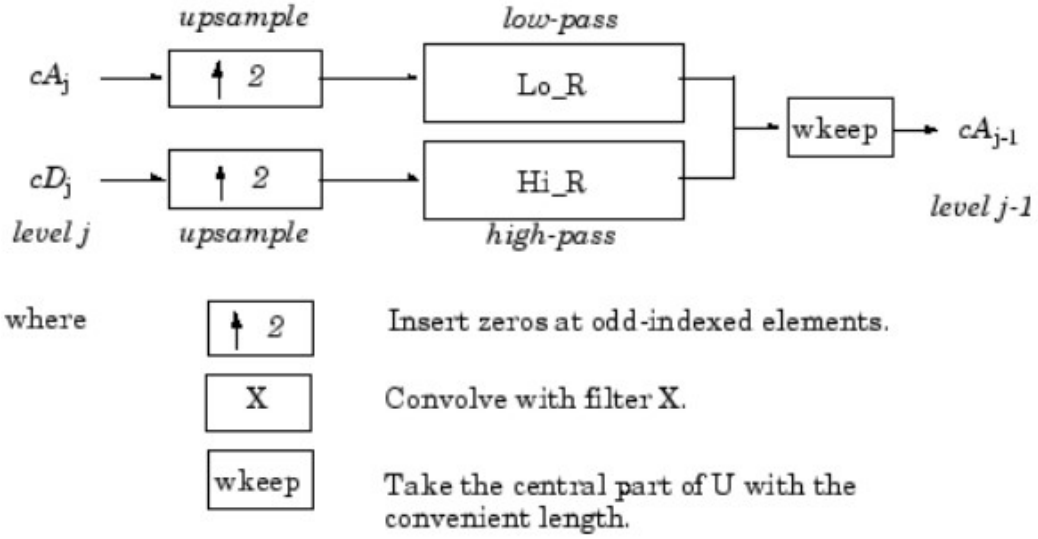
This signal is passed through a series of high pass and low pass filters to analyze the respective function at each level. Low-pass and high-pass filters are respectively:

$$\{\mathrm{h}(0), \mathrm{h}(1)\} \longrightarrow h(0) = \frac{1}{\sqrt{2}}, h(1) = \frac{1}{\sqrt{2}}$$

$$\{g(0), g(1)\} \longrightarrow g(0) = \frac{1}{\sqrt{2}}, g(1) = -\frac{1}{\sqrt{2}}$$

Reconstruction

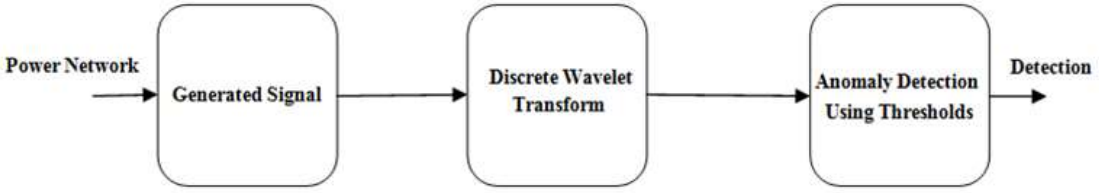
We reconstructed the approximation coefficient, Inverse Discrete Wavelet Transform (IDWT) by inverting the decomposition step by inserting zeros and convolving the results with low-pass and high-pass filter. The procedure is shown below:



Anomaly Detection

Intrusion detection using our DWT algorithm consists of three parts:

1. Targeted network protocol generated signal
2. DWT algorithm to analyze the signal
3. Anomaly detection using thresholds



The algorithm takes the reconstructed signal only from those wavelet coefficients that reach the alert thresholds. Through the sampling of historic traffic, we establish the threshold value in each level of decomposition. By setting a high threshold at each level, anomalies can be detected with high confidence. Varying the window size may possibly lead to changes to these threshold values.

The BLACK LIGHTNING detection algorithm upper and lower thresholds are is tuned to detect at $P(\mu-\sigma < X < \mu+\sigma)$ where μ is the mean of the detailed coefficients and σ is the standard deviation also of the detailed coefficients. We found that this is approximately 98% detection rate with a 2% probability that it will be a false positive. Based on beta testing at the Pacific Northwest National Laboratory, we were able to tune the determine the optimal scalar for the algorithm.

Our approach is different from traditional network defensive tools which are based on signatures of the threat after the fact. Our approach scans at the protocol level in near real-time and is based on historical and statistical analysis of the targeted network and network traffic.