ISSN: 2278 – 1323
*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*
*Volume 2, Issue 4, April 2013*

# A Design of an Efficient, Robust, Autonomous and a well Coordinated Distributed Network Monitory System for Large Computer Networks

**Quist-Aphetsi Kester**

***Abstract*— Information security assurance over networks is one of the key major issues facing the network infrastructure of organizations and information systems in today's world. Data security and access control to information are issues of great importance in large scale networks. Network performance tracking and tracking of malicious activities over networks are of key importance in network management and network security. Because most organizations do not have a coordinated and autonomous network monitory centers at nodes within large computer networks, remote tracking of data becomes a challenge for them. Some organizations do real-time monitory over large networks from a centralized system and this affects the performance of the entire network and in some cases turned to be inefficient. Monitory and analysis of large data passing through nodes becomes a challenge if it is supposed to be done remotely over the network.**

**This paper seeks to propose a method for designing efficient, robust, autonomous and a well coordinated distributed network monitory system for large computer Networks. The system consists of units or centers. These monitory centers are designed to have the capability of monitoring large amount of data passively and autonomously. They will also have the capability of collecting and analyzing data of interest as well as passing of information over to a parent monitory center for analysis if necessary. They can be used to monitor network performance and to passively monitor activities of targeted systems over the network.**

***Index Terms*—design, architecture, passive monitory, autonomous, distributed network, network-centric.**

## I. Introduction

Information and communication are two of the most important strategic issues for the success of every enterprise. Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster and easier than other facilities [1]. With the right and updated information in today's world, institutions and individuals can acquire and share information effectively. It is therefore important to establish communication among people so everyone can have access to the information. Computer network is a key in the communication field.

With the computer networks, the world of communication has experienced a tremendous growth [2]. However, when accessing the network, a user can experience some difficulties: It is right of the users of the network to get smooth working network system, without any interruption or experience slow communication between computers due to malicious activities over the network. This is done by taking administrative measure to maximize the security on ones network against multiple threats (hackers, viruses, denial of service, worms etc). [3]

Moreover, to fight these threats, network monitory is a key solution for determining sources and tracking of malicious activities. Network administrators lack the tools they need to understand and react to their changing networks. This makes it difficult for them to make informed, timely decisions regarding network management, capacity planning, and security. These challenges will only increase as networks continue to gain in throughput, become more complex, and encrypt more and more of their traffic [4].

A lot of companies whose information systems are efficient today are using a monitoring systems to better secure their IT infrastructure and Information systems.

In this paper, we have used a passive approach for the network monitory units. Independent and Autonomous monitory units (child units) are designed to monitor and keep track of activities at each vital node and feed information back to the parent unit based on predefined rules or request from the parent unit. This reduces traffic and increases efficiency over the entire network infrastructure. The paper has the following structure: sections II consist of related works, section III of the methodology, section IV The approach, section V consist of the analysis and section VI concluded the paper.

## II. Related works

In today's world, computer networks need policing. Computer systems needs to be monitored and malicious activities tracked to control fraudulent activities. [5].Network monitoring is more strategic when it comes to its implementation over large networks where large volumes of traffic are being generated every second. It involves 24/7 monitory and it is also about optimizing data flow and data access in a complex and changing environment. Tools and techniques for network monitory are numerous and they vary as the environments they guard and analyze evolve over time [6].

The availability of electronic resources increased the new

*Quist-Aphetsi Kester, MIEEE, Faculty of Informatics, Ghana Technology University College Accra, Ghana, +233 209822141*

form of criminal activity that takes advantage of electronic resources, namely computer crime and computer fraud. Computer crime poses a daunting task for law enforcement agencies because they are highly technical crimes. In banking, the growth of online banking presents other opportunities for perpetrators of economic crime. Funds can be embezzled using wire transfer or account takeover. Customers can submit fraudulent online applications for bank loans. Hackers are able to disrupt e-commerce by engaging in denial of service attacks and by compromising online banking payment systems [8].

Networks, like any other complex system need to be continuously monitored for many reasons. The day to day operations present challenges that need a precise response, whether human or automated, including anomalous or heavy traffic and threats to quality of service. Unfortunately, information residing on systems as well as sent over the internet can be accessed by unwanted or unauthorized users. [9][10] Hence network policing through monitory is of key importance. But the use of appropriate monitory system or technique utilized should not affect the performance of the network by adding more loads to it.

Directions of computer systems architecture is a key thing to consider when focusing on designing robust information systems. From 1960-1980, systems architecture was focused on organizations structure. This is purposely for internal usage and it was mainframe centric. The data definition was also unique and vendor dependent. From 1990-2000, the focus was on processes and client server architecture was a major consideration. Partial connectivity and Electronic data interchange (EDI) file transfer was paramount. EDI is a method for transferring data between different computer systems or computer networks [11]. It is commonly used by big companies for e-commerce purposes, such as sending orders to warehouses or tracking their order. It is more than mere e-mail; for instance, organizations might replace bills of lading and even cheques with appropriate EDI messages [12]. From 2010-2050, system architecture is and will be driven by distrusted functions concepts, real-time connectivity considerations and universal interoperability of systems within an IT infrastructure irrespective of the vendor and languages used. Data centricity will be a major focus within a distributed systems environment. Figure 1 provides a summary of the directions of the systems architecture [11].

Computer-centric solutions are being and will be replaced by network-centric services. Hence network policing and monitory should also have the capacity to analyze large data over large networks efficiently. Monitory centers around the world should have the capacity of sharing resources, cooperating and coordinating effectively and in some cases autonomously so that the monitory of Information systems across geographical areas can be effective.

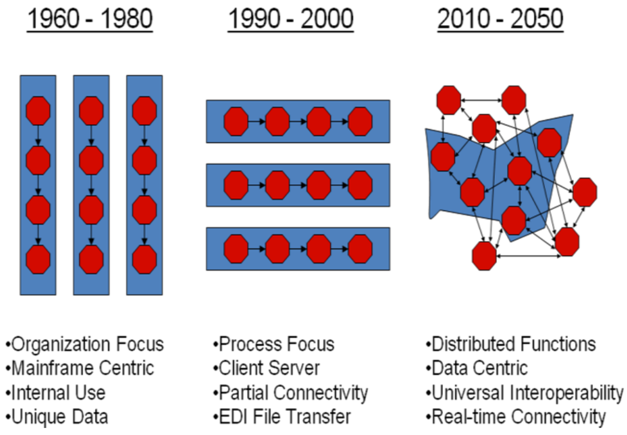

Figure 3: Directions of System Architecture

Because the network provides the wires that connect a grid, understanding the performance provided by a network is crucial to achieving satisfactory performance from many grid applications. Monitoring the network to predict its performance for applications is an effective solution, but the costs and scalability challenges of actively injecting measurement traffic, as well as the information access and accuracy challenges of using passively collected measurements, complicate the problem of developing a monitoring solution for a global grid. Bruce B. Lowekamp wrote a paper on combining active and passive network measurements to build scalable monitoring systems on the grid. His work was a preliminary report on the Wren project, which was focused on developing scalable solutions for network performance monitoring. By combining active and passive monitoring techniques, Wren was able to reduce the need for invasive measurements of the network without sacrificing measurement accuracy on either the WAN or LAN levels. Specifically, they presented topology-based steering, which dramatically reduces the number of measurements taken for a system by using passively acquired topology and utilization to select the bottleneck links that required active bandwidth probing. Furthermore, by using passive measurements while an application was running and active measurements when none was running, they preserved their ability to offer accurate, timely predictions of network performance, while eliminating additional invasive measurements. [13]

In Grid environments, high-performance applications have to take into account the available network performance between the individual sites. Existing monitoring tools like the Network Weather Service (NWS) measure bandwidth and latency of end-to-end network paths. This information is necessary but not sufficient. With more than two participating sites, simultaneous transmissions may collide with each other on shared links of the wide-area network. If this occurs, applications may obtain lower network performance than predicted by NWS. Den Burger, M., Kielmann, T., & Bal, H. E, described TOPOMON, a monitoring tool for Grid networks that augments NWS with additional sensors for the routes between the sites of a Grid environment. Their tool conforms to the Grid Monitoring Architecture (GMA) defined by the Global Grid Forum. It unites NWS performance and topology discovery in a single monitoring architecture. Their topology consumer process collects route information between the sites of a Grid environment and derives the overall topology for utilization by application programs and communication libraries. 14]

Monitoring is the act of collecting information concerning the characteristics and status of resources of interest. Monitoring grid resources is a lively research area given the challenges and manifold applications.

Zanikolas, S., & Sakellariou, R. worked on a taxonomy of grid monitoring systems. Their aim was to advance the understanding of grid monitoring by introducing the involved concepts, requirements, phases, and related standardisation activities, including Global Grid Forum's Grid Monitoring Architecture. Based on a refinement of the latter, their paper proposes a taxonomy of grid monitoring systems, which was employed to classify a wide range of projects and frameworks. The value of the offered taxonomy lies in that it captured a given system's scope, scalability, generality and flexibility. 15]

The Remos architecture is designed to provide the information needed by Grid applications across many diverse environments. Remos provides resource information to distributed applications. Its design goals of scalability, flexibility, and portability are achieved through an architecture that allows components to be positioned across the network, each collecting information about its local network. To collect information from different types of networks and from hosts on those networks, Remos provides several collectors that use different technologies, such as SNMP or benchmarking. By matching the appropriate collector to each particular network environment and by providing an architecture for distributing the output of these collectors across all querying environments, Remos collects appropriately detailed information at each site and distributes this information where needed in a scalable manner. Prediction services are integrated at the user-level, allowing history-based data collected across the network to be used to generate the predictions needed by a particular user. Remos has been implemented and tested in a variety of networks and is in use in a number of different environments.[16]

## III. Methodology

Network technologies play an important role in the survival and competitiveness of most organization today. It is therefore indispensable to make sure the network is reliable. Designing network monitory system is a step forward to securing a network and enhancing its reliability.

This paper proposes a method for designing efficient, robust, autonomous and a well coordinated distributed network monitory system for large computer Networks. This monitory system is designed to have the capability of monitoring large amount of data passively and autonomously. This system have units that have the capability of collecting and analyzing data of interest as well as passing of information over to a parent monitory unit for analysis if necessary. They can be used to monitor network performance and to passively monitor activities of targeted systems over the network. The ultimate aim of this paper is to propose a new system design to improve security in the monitory of large computer networks.

This work move monitory of the network systems from computer-centric environment to network centric environment. With the computer centric situation, the central computer has to provide high computing power, large memory, high dependability, fault tolerance management, and too many input/output connections (This makes analysis of data solely to be done by a single system pulling traffic towards a central point for analysis).With the network centric approach, distributed monitory centers are situated at key points to monitor and analyze traffic. This distributed unit then feed vital information to the main monitory centre based on predefined rules of engagement of the units though they function autonomously. The units can cooperate in analyzing traffic on specific routes as well.

The unit systems will have the capability of interoperability and cooperation as well as reporting to the main centre. The proposed system will function passively, though it can be actively engaged. This way of monitory will reduce load on the network as well as make monitory efficient and more successful.

## IV. The Approach

The network-centric monitory model is presented in figure 2 below. An illustration of seven nodes of monitory centers has been connected to effectively coordinate and monitor activities effectively. Each node cooperates with its neighbor nodes in monitory of traffic between two points and a node monitors traffic arriving at a particular point. In choosing of the position of the monitoring units, considerations were given suitable points that can be monitor without affecting the performance of the network.

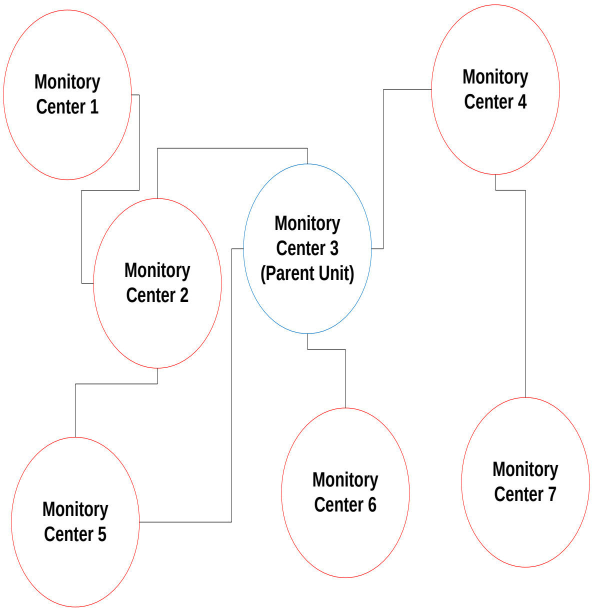

Figure 2: Network monitory center model

From the model, center 1 may monitor traffic coming from a region or a section of the entire network that may connect say a community, city, town or an institution. Autonomously, it gathers data on systems that are targeted or filter traffic passively to analyze contents. It can cooperate with centre 2 in monitory of traffic between two points from each side over the network. Reports can then be generated and forwarded to the Parent unit (Monitory center 3) based on predefined rules and service contracts.

Figure 3 represent a set of routers within a large network. These routers connect cities to towns as well as institutions and other systems. All of them contribute to the building of the entire network but only seven of them are connected to a monitory centers as shown in figure 4. Here, router C is connected to the parent center. Router I and F are not monitored because the packet passing through them will irrevocably go to one of the routers connected to a center before reaching any computer on the network. The monitoring units are strategically positioned and connect to major routing points and every packet can therefore be analyzed.

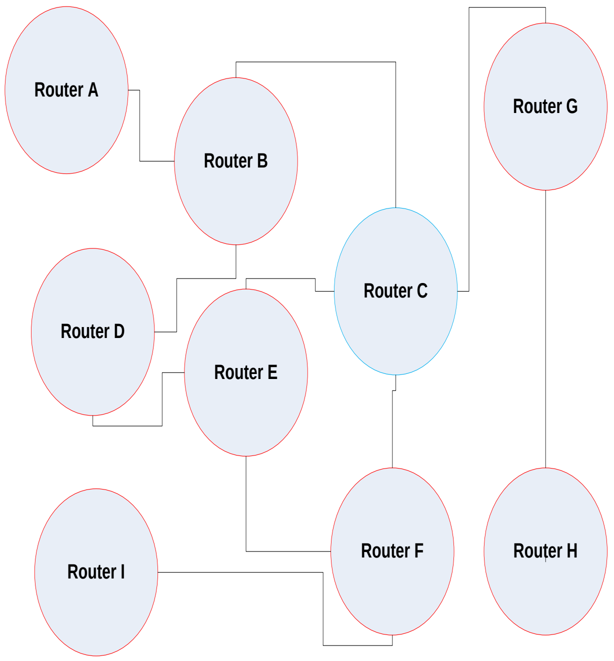

Figure 3: The routing nodes

The figure 4 shows a typical network-centric monitory systems architecture with monitory centers. There are communities, institution and cities all connected to the internet through nodes. The network connects cities, town, individuals and other institutions to the internet. For better understanding, numbers have been assigned to every center. Also, letters has been given to the routers. The model of the monitory centers is shown in figure 1. The monitory center model is composed of seven centers. One of these monitors is considered to be the main or parent center. The others are called child centers. The child centers operate independent on the main center. They will automatically send information to the main center according to some predetermined rules. This will require end-to-end network performance information. Every packet passing through the centers will be stored based on classification criteria. Data mining techniques will be used as well as artificial intelligent approaches to effectively control and coordinate all activities on the child centers from the parent unit. Irrespective of the path taken by the packets to reach a certain destination, they will always be analyzed by one of the monitory centers.

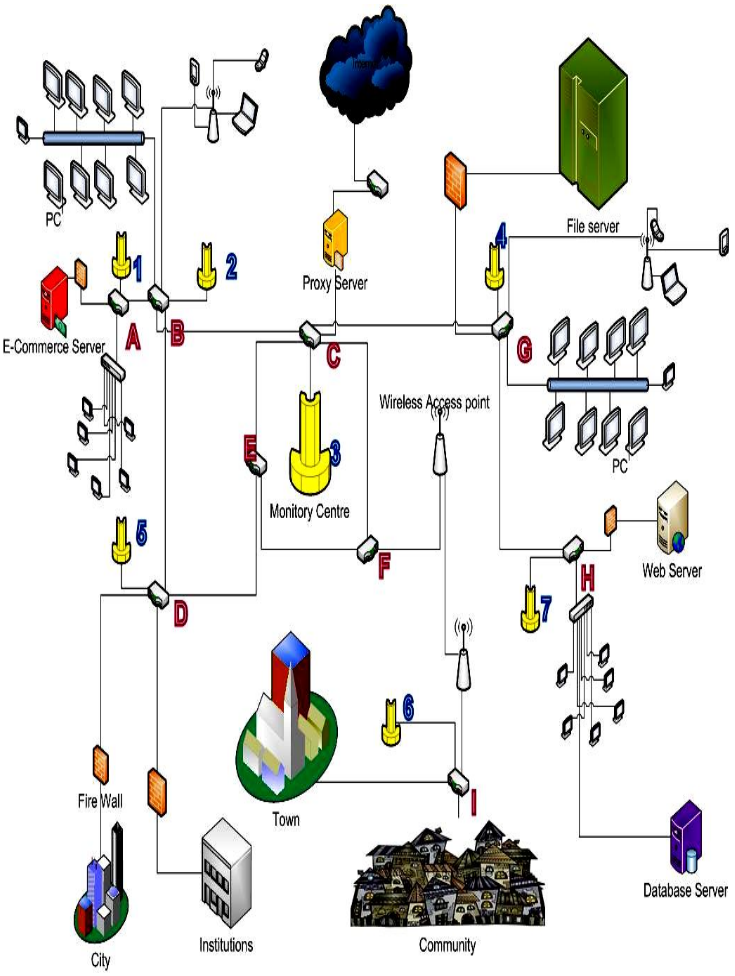

Figure 4: network-centric monitory systems architecture

To access the internet from the community, one has to communicate through a process involving router I connected to monitory center 6. Then the router will forward traffic to router F through two wireless access point as seen in the figure 4. There is no need to connect a monitory unit to router F because every packet passing through it will be going to either router D or router C.

## V. Analysis and Results

Let v be vertex and let it denotes the nodes of the monitory points and e be the eccentricity between the monitory points. The eccentricity \e (v) of a vertex v is the greatest geodesic distance between v and any other vertex. It can be thought of as how far a node is from the node most distant from it in the graph. The eccentricity e (v) of a point v in a connected graph G (V, E) is max d (u, v), for all u v.

Let all units be v in fiigure1, then e (v) will yield

Let MC=Monitory center

Table 1: Eccentricity of v

| | MC1 | MC2 | MC3 | MC4 | MC5 | MC6 | MC7 |
|---|---|---|---|---|---|---|---|
| MC1 | 0 | 1 | 2 | 3 | 2 | 3 | 4 |
| MC2 | 1 | 0 | 1 | 2 | 1 | 2 | 3 |
| MC3 | 2 | 1 | 0 | 1 | 1 | 1 | 2 |
| MC4 | 3 | 2 | 1 | 0 | 2 | 2 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| MC5 | 2 | 1 | 1 | 2 | 0 | 2 | 3 |
| MC6 | 3 | 2 | 1 | 2 | 2 | 0 | 3 |
| MC7 | 4 | 3 | 2 | 1 | 3 | 3 | 0 |

Table 2 provides the values of the eccentricity such that e (v) of a point v in a connected graph G (V, E) is max d (u, v), for all u v. It can be seen that the further the monitory centers are apart from each other the greater the value of the eccentricity. Hence the most efficient point that can effectively receive data at a low cost from all nodes is the one with the minimum values of eccentricity.

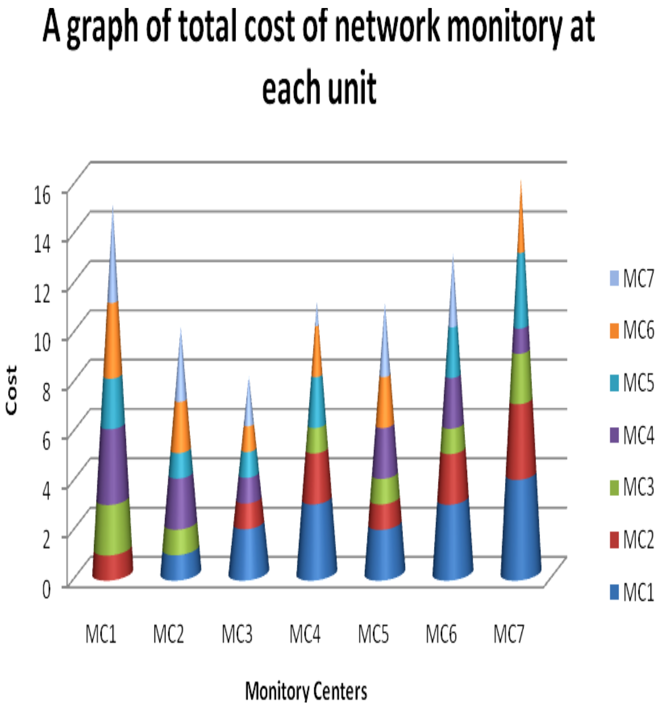

Figure 5: a graph of total cost of network monitory for each unit

From figure 5, it is clearly seen that monitory center 3, which is the parent unit, is the one with the minimal cost. This means that it is cost effective as well as efficient to place the parent unit at the MC3.

Table 2: Nearest neighbor of v

| | MC1 | MC2 | MC3 | MC4 | MC5 | MC6 | MC7 |
|---|---|---|---|---|---|---|---|
| MC1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| MC2 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| MC3 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| MC4 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| MC5 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| MC6 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| MC7 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |

Table 2 consists of monitory units and data on their neighbors. The value 0 incated that they are not neibors and 1 indacated that they are neighbors. The more the neighbor of a unit the more efficient and less cost rffective it is to put a main unit there.

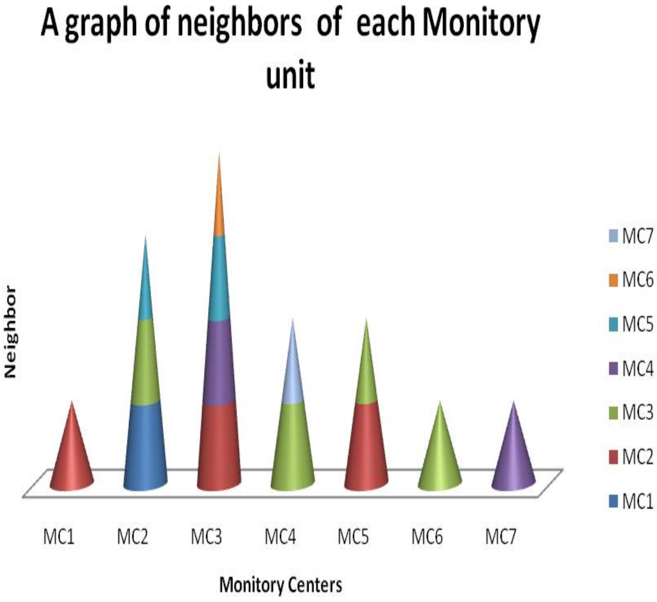

Figure 6: a graph of neighbors of each monitory unit

From figure 6 it clearly seen that monitory center 3 is more connected to adjacent nodes than the others hence it is advisable to put the parent unit there.

## VI. CONCLUSION

With the proposed model, huge traffics can be analyzed on a network efficiently. Geographical activity monitory and system tracking can also be done by units. System policing and surveillance can effectively be carried out autonomously to track suspected activities as well as automated network live network forensics can actively be used. These systems design approach can be engaged in the future for network policing and monitory can easily be done on a national and international scale.

## REFERENCES

[1] ICT Global (2012). The Importance of Computer Networks. Retrieved from http://www.ictglobal.com/imp_networks.html

[2] Midkiff, Scott F., Network (computer science). Microsoft Student 2008 [DVD]. Redmond,WA: Microsoft Corporation, 2007.

[3] WiFinotes (2012. Computer Network security, Security Issues and Solutions, Security Policies http://www.wifinotes.com/computer-networks / computer-network-security.html

[4] Schultz, M. J., Wun, B., & Crowley, P. (2011, October). A Passive Network Appliance for Real-Time Network Monitoring. In Architectures for Networking and Communications Systems (ANCS), 2011 Seventh ACM/IEEE Symposium on (pp. 239-249). IEEE.

[5] WiseGeek. What is Network Monitoring? Retrieved from http://www.wisegeek.org/what-is-network-monitoring.htm

[6] By Kim S. Nash, Alyson Behr (2012). Network Monitoring Definition and Solutions retrieved from http://www.cio.com/article/133700/Network_ Monitoring _Definition_ and_Solutions

[7] Matthews, W., Cottrell, L., & Salomoni, D. (2001). Passive and Active Monitoring on a High Performance Research Network. Passive and Active Monitoring (PAM).

[8] LEXIS-NEXIS The Growing Global Threat of Economic and Cyber Crime,(December 2000)

[9] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advnaced Communication Technology, 2004.

[10] Alabady S. , "Design and Implementation of a Network Security Model using Static VLAN and AAA Server," In Proceedings International Conference on Information & Communication Technologies: from Theory to Applications, ICTTA'2008

[11] Prof. Paul A. Strassmann(2007) .What is a Service Oriented Architecture - George Mason University, November 19, 2007

[12] Wikepedia,(2012).Electronic data interchange. Retrieved from http://en.wikipedia.org/wiki/Electronic_data_interchange

[13] Lowekamp, B. B. (2003). Combining active and passive network measurements to build scalable monitoring systems on the grid. ACM SIGMETRICS Performance Evaluation Review, 30(4), 19-26.

[14] Den Burger, M., Kielmann, T., & Bal, H. E. (2002). TOPOMON: A monitoring tool for grid network topology. In Computational Science—ICCS 2002 (pp. 558-567). Springer Berlin Heidelberg.

[15] Zanikolas, S., & Sakellariou, R. (2005). A taxonomy of grid monitoring systems. Future Generation Computer Systems, 21(1), 163-188.

[16] Dinda, P. A., Gross, T., Karrer, R., Lowekamp, B., Miller, N., Steenkiste, P., & Sutherland, D. (2001). The architecture of the remos system. In High Performance Distributed Computing, 2001. Proceedings. 10th IEEE International Symposium on (pp. 252-265). IEEE.

**Quist-Aphetsi Kester, MIEEE:** is a global award winner 2010 (First place Winner with Gold), in Canada Toronto, of the NSBE's Consulting Design Olympiad Awards and has been recognized as a Global Consulting Design Engineer. Currently the national chair for Policy and Research Internet Society (ISOC) Ghana Chapter, a world renowned body that provides international leadership in Internet related standards, education, and policy. He is the Chairman for the Centre of Research, Information Technology and Advanced computing-CRITAC. He is a law student at the University of London UK. He is a PhD student in Computer Science. The PhD program is in collaboration between the AWBC/ Canada and the Department of Computer Science and Information Technology (DCSIT), University of Cape Coast. He had a Master of Software Engineering degree from the OUM, Malaysia and BSC in Physics from the University of Cape Coast-UCC Ghana.

He has worked in various capacities as a peer reviewer for IEEE ICAST Conference, IET-Software Journal, lecturer, Head of Digital Forensic Laboratory Department at the Ghana Technology University and Head of Computer science department. He is currently a lecturer at the Ghana Technology University College.