Green Wireless Computing: An Overview

**Dr. A. Haja Abdul Khader**

Assistnat Professor of Computer Science

Khadir Mohideen College

(Affliated to Bharathidasan University, Tiruchirappalli)

Adirampattinam – 614 701

Tamil Nadu, INDIA

*ahaja@ymail.com*

**Ms. A. Gomathi**

Assistnat Professor of Computer Science

Khadir Mohideen College

(Affliated to Bharathidasan University, Tiruchirappalli)

Adirampattinam – 614 701

Tamil Nadu, INDIA

*gomathimurugan566@gmail.com*

ABSTRACT

Presently green computing technology has made a great impact in the surroundings, which makes it more cost-efficient and proper use of network resources and less consumption of energy. The conception of Green computing technology in communication network is explained Greek deity. The computing technology is considered over communication network and this communication network is broadly categorized as infrastructure (wired) and wireless networks, also called as ADHOC network in which ambulatory nodes and sensor nodes are responsible for communication. In this work there many different technologies are unrepentant which accentuate on green computing, related to both the type of communication network and also provide a summary of abstraction system energy saving studies in diametric areas which are involved in data transformation.

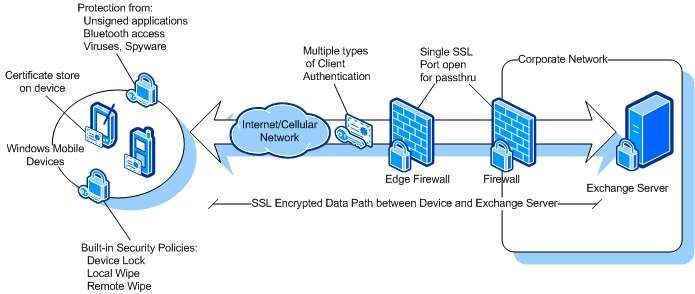
**Keywords**— Green Computing, Wireless Sensor Network, Honeypot, Network Access Control

**I INTRODUCTION**

Green Wireless computingconsists of the insurance policy and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network- accessible resources. Green Wireless engineering science involves the authorization of access to data in a network, which is possessed by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Green Wireless computingcovers a variety of computer networks, both public and private, that are used in unremarkable jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Green Wireless computing is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Green Wireless computing starts with Authentication, commonly with a username and a password. Since this requires just one detail manifest the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan).

Anti-virus software or an entry prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account. Communication between two hosts using a network may be encrypted to maintain privacy.



**Figure 1: Green Wireless Computing Architecture**

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though impelling to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. **Honeypots**, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these accomplice resources are studied during and after an flak to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A Protea cynaroides can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's playing can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.

### II TYPES OF ATTACKS

Networks are subject to attacks from cattish sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, an"Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral occurrence to find and gain access to assets procurable via the network.

Types of attacks include:

### Passive

* + - * Network
      * Wiretapping
      * Port scanner
      * Idle scan
      * Encryption
      * Traffic analysis

### Active

* + - * Virus
      * Eavesdropping
      * Data modification
      * Denial-of-service attack
      * DNS spoofing
      * Man in the middle
      * ARP poisoning
      * VLAN hopping
      * Smurf attack
      * Buffer overflow
      * Heap overflow
      * Smurf attack
      * Format string attack
      * SQL injection
      * Phishing
      * Cross-site scripting
      * CSRF
      * Cyber-attack

**III GREEN WIRELESS COMPUTING ACCESS CONTROL**

Not every user should have admittance to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint disposition or give them only limited access. This process is network access control (NAC).

### Antivirus and antimalware software

"Malware," short for "malicious computer software," includes viruses, worms, Trojans, ransom ware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

### Application security

Any software you use to run your commercial enterprise needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software package, and processes you use to close those holes.

### Behavioral analytics

To detect abnormal network behavior, you must undergo what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

### Data loss prevention

Organizations must make sure that their staff does not send light-sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

### Email security

Email gateways are the number one threat variable quantity for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

### Firewalls

Firewalls put up a barrier between your trusted intragroup network and un trusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both. Cisco offers unified threat management (UTM) devices and threat-focused next-generation firewalls.

### Intrusion prevention systems

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and re infection.

### Mobile device security

Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

### Network segmentation

Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

### Security information and event management

SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, including physical and virtual appliances and server software.

### VPN

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

### Web security

A web security solution will control your staff’s web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

### Wireless security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

**IV CONCLUSION**

This chapter aimed an up-to-date interrogation on Green computing over communication network which talk about how green computing used in both wired and wireless networks. All these plan of action explain about how green computing technology can be used over scheme to mainly decrease power activity which is a major concern for network operators to not only reduce the operational costs, but also to reduce their biological science effects.

**REFERENCES**

[1] Aruna Prem Bianzino, Claude Chaudet, Dario Rossi, and Jean-Louis Rougier, ―A Survey of Green Networking Research‖ IEEE communications surveys & tutorials, vol. 14, no. 1, first quarter 2012

[2] Doron Ezri, Shimi Shilo Greenair Wireless Ramat Gan, Israel, ―Green Cellular - Optimizing the Cellular Network for Minimal Emission from Mobile Stations‖ IEEE communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011

[3] Yan Chen, Shunqing Zhang, and Shugong Xu, ―Fundamental Trade-offs on Green Wireless Networks‖ IEEE Communications Magazine • June 2011

[4] Jianhua He, Pavel L oskot, Tim O’Farrell, Vasilis Friderikos, Simon Armour, John Thompson, ―Energy.Efficient Architectures and Techniques for Green Radio Access Networks‖ – Invited Paper – IEEE

[5] S.V.S.S. Lakshmi, Ms. I Sri Lalita Sarwani, M.Nalini Tuveera, ―A Study On Green Computing: The Future Computing And EcoFriendly Technology‖ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622

[6] http://unfccc.int/resource/docs/convkp/kpeng.pdf - Kyoto protocol to the united nations framework Convention on climate change

[7] http://www.hp.com/hpinfo/globalcitizenship/environment/pdf/leadposition.pdf - HP’s Compliance with Restriction of Hazardous Substances (RoHS) Legislation

[8] http://www.termpaperwarehouse.com/essay-on/Senior-Management/51117 - Senior Management in Computers and technology

[9] Lin x. Cai and h. Vincent poor, Princeton university, ―Dimensioning network deployment and resource management in green mesh networks‖ - IEEE Wireless Communications • October 2011

[10] Falcom Electronics (Pvt) LTD (Measurement of Data center Power consumption - http://www.fe.co.za/products/ans/documents/DataCenterSolutionsSection.pdf

[11] Energy Logic: Reducing Data Center Energy Consumption by Creating Savings that Cascade Across Systems - A White Paper from the Experts in Business-Critical Continuity – EMERSON Network Power

[12] A. Li, X. Yang, S. Kandula, and M. Zhang, ―CloudCmp: comparing public cloud providers,‖ in Proc. 2010 IMC, pp. 1–14.

[13] Vinh The Lam, Sivasankar, Radhakrishnan, Amin Vahdat, Rong Pan and George Varghese – ―NetShare and Stochastic NetShare: Predictable Bandwidth Allocation for Data Centers‖ - ACM SIGCOMM Computer Communication Review Volume 42, Number 3, July 2012

[14] Mrs.V.Kavitha Chandrakanth, S.Gayathri ―Examining bandwidth provisioning on cloud computing and resource sharing via web‖ - [IJESAT] International journal of engineering science & advanced technology Volume- 2, Issue-5, 1372 – 1376

[15] Anirban Kundu, Chandan Banerjee, Sutirtha Kr. Guha, Arnab Mitra, Souvik Chakraborty, Chiranjit Pal ―Memory Utilization in Cloud Computing using Transparency‖ - IEEE Computer Sciences and Convergence Information Technology (ICCIT), Nov. 30 2010-Dec. 2 2010

\_\_\_\_\_\_\_