Effective and Secure vWSN Applications in a Virtualized Cloud Computing Environment

Mohammad Equebal Hussain[1], Mohammed Qayyum[2], Mohammad Rashid Hussain[3], Rashid Hussain[4]

[1]Suresh Gyan Vihar University, Jaipur, India
[2]Department of Computer Engineering, College of Computer Science, King Khalid University, Kingdom of Saudi Arabia
[3]Department of Information Systems, College of Computer Science, King Khalid University, Kingdom of Saudi Arabia
[4]Suresh Gyan Vihar University, Jaipur, India

***Abstract*:** Security is one of the key concerns in cloud computing. We are proposing Virtual Wireless Sensor Network (vWSN) which is one of the key features of cloud computing in the area of agriculture. Our main focuses are effective and secure vWSN in virtualized cloud computing environment with enhanced security to detect environmental monitoring, humidity monitoring, soil moisture, air quality (pollution) monitoring, insect monitoring, pest and disease control, which is based on virtualization and cloud computing technology, centrally managed device having flexible and configurable parameter with less maintenance and operational cost. To the best of our knowledge, vWSN is the first approach to agriculture based on extensional WSN information. WSN contains both control plane (signaling) and data plane (forwarding) coupled together.WSN is a specific purpose computer containing hardware whose main components are memory, CPU, IO, registers, Data and address bus, timer, sensor, computing logic and decision-making logic. WSN is a physical device which needs to be placed in the field in certain topology (Ring, mesh, tree, and star) which may need to be protected for damage and erosion due to various parameter including but not limited to physical theft, damage due to weather, animal and various other reason. In this paper our approach is to propose virtualized model to replace physical wireless sensor network (WSN) to virtual machine (VM) based vWSN which can be deployed on the cloud. Since security is one of the major concerns for VM in cloud computing therefore we also proposed the enhanced 3-tier security model for vWSN.

***Keywords*:** Virtual Wireless Sensor Network (vWSN); Virtual Machine (VM); Virtual Appliances (VA); Cloud Computing; Data Plane; Control Plane,Xen hypervisor; virtualization.

1. Introduction

Recent years have looked-on intensifying corrosion of the WSN predominance to the benefit of WSN's based on different applications. Our proposed unique framework vWSN adopt a similar application, which does not mean that physical approach, but rather that physical approach is a basic concept and that the instances referring to the same concept in the same application can be implement using "vWSN" to better fit the specific features of each instances. So, while WSN are still widely used in the fields of agriculture to detect environmental monitoring, humidity monitoring, soil moisture, air quality (pollution) monitoring, insect monitoring, pest and disease control using WSN. It is a valuable decision control and support tool for farmers but unfortunately in developing region where farmers are mostly using pest control legacy system (interval based), WSN technology will help them to use it on ad-hoc basis only when needed based on the decision by the sensor, vWSN framework is preferred for the same applications, because it is based on virtualization and cloud computing technology, centrally managed device having flexible and configurable parameter with less maintenance and operational cost.

Unfortunately, the absence of a unique, well approached WSN turns to a disadvantage when moving from physical application to virtual application. WSN may need to be protected for damage and erosion due to various parameter including but not limited to physical theft, damage due to weather, animal and various other reason. Network virtualization share resources from physical network among different virtual networks. One of the biggest security challenges in design of cloud computing platform is VMs interconnectivity using virtual network which significantly affects security. We approach virtualized model to replace physical wireless sensor network (WSN) to virtual machine (VM) based vWSN which can be deployed on the cloud. Since security is one of the major concerns for VM in cloud computing therefore we also proposed the enhanced 3-tier security model for vWSN. So, dedicated physical channel is the more secure way to isolate each VM. Bridge and route is used to link VMs in virtual network. As a result, isolation can be easily broken.

In this paper we propose an approach, called vWSN (virtual Wireless Sensor Network), using virtualization technique, the same can shifted to virtual machine so that the physical devices (in the field) can be replaced by virtual devices which runs as a normal application inside host machine operating system as a single process. Only picture or image is needed from the field which can be collected using high definition or high precision camera or any other similar devices. High precision camera can be placed somewhere in the field which can cover a broad area and image can be send to the server where VMs are running in order to take decision thus reducing the need of physical WSN. vWSN is beneficial in different context:

- VWSN makes economical and manageable computing solution;
- Virtualization helps migrating from hardware architecture to software;
- Since VWSN is software device hence administrator can add or reduce the size of memory, add or remove processor, add virtual disk or increase disk size, shutdown the VWSN when not in use.
- Snapshot feature will help in saving the state of machine which can be restored later.
- Patching or upgrading application when new software version is available.
- VWSN can be easily managed remotely as well as locally

by connecting to the server console.

- VWSN template can also be create, modify or delete the device when not needed.
- Flexible network configuration: integrating VA deployment in available network (IP address management) is the major task.
- Using VMware player VA can run and creates its own VM.
- WSN mainly contain measuring (sensing) unit, communication unit and computing unit. The same can be created as a virtual appliance (VA).
- This model is less expensive and more control over the device.
- vWSN framework to control the inter-communication among virtual WSN (VMs) deployed in physical machines with enhanced security.

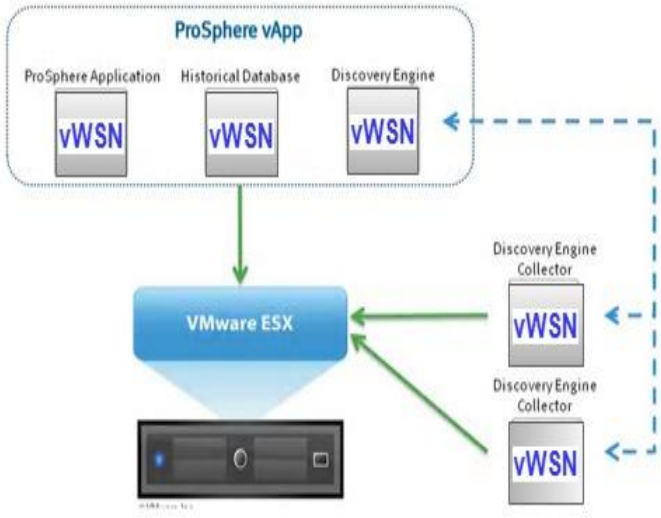

Figure 1. VA configured using VM and deployed on VMware vsphere

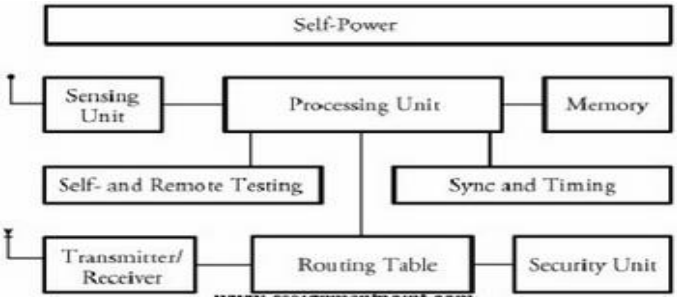

Figure 2. Wireless sensor node location using GPS

Identifying the applications of vWSN is much like building all the decision-making functionality will be done in VA configured using VM and deployed on VMware vsphere.

As far as data collection is concerned, will be done using high precision camera and information will be sent to VA. Therefore, whatever WSN can do as a physical device sitting in the field can be done by VWSN deployed on VMware at a distant location. Any number of virtual WSN can be created as described earlier. Each VWSN can run image processing algorithm to take various decision, based on that the corresponding action will take place for example to sprinkle pesticide, urea, water etc in the field at required place. In general, we wish to keep the easily manageable virtual WSN which is much simple, cost effective, efficient and configurable. There are lots of scopes to extend vWSN in the area of security, optimization, and load balancing as well as clustering techniques.

The contributions of this work are:

- An algorithm that implements a divisive approach to configure physical WSN into vWSN (Section 2)
- The concept of monitoring through Image Processing in VA (Section 3)
- The concept of Virtual Network Vulnerabilities in vWSN (Section 5)

The paper is completed by section 4, which discussed related work, section 6, which discussed about virtual network model for vWSN, and section 7, which discussed about conclusions and future works.

2. Algorithm to configure physical WSN into vWSN

Step-1: virtual appliances with customized feature can be programmatically configured in VMware studio either using web based graphical interface or command line interface (CLI).

Step-2: select the operating system (OS) and application package to include in VA, configure welcome screen, provide vendor information etc.

Step-3: configure boot script, virtual disk, virtual network card for the VA.

Step-4: in order to build and provision virtual appliance, SSH connection and daemon is required to communicate. VA in VMware has .OVA or .ZIP format.

Step-5: Once VA is created and verified or tested then can be distributed and ready for deployment on VMware hosted platform.

Step-6: Virtual Appliance Management Infrastructure (VAMI) by VMware studio includes various components which help in maintaining virtual appliance to update service, to configure network and proxy setting as well as shutdown and reboot of VA.

Due to the increasing number of Brain tumor patient, the concept of cost optimization is in priority on demand. Our Step-1: virtual appliances with customized feature can be programmatically configured in VMware studio either using web based graphical interface or command line interface (CLI).

Image processing operation can be done by any available image processing software like MATLAB. There are various proposed systems to detect pest densities by comparing images (ideal vs. infected) by continuous automatic monitoring without human intervention hence minimizing human effort and error by simple, efficient and fast solution.

3. Related Work

In this section we discuss the research area mainly related to WSN, To the best of our knowledge, vWSN is the first approach to agriculture based on extensional WSN information. In particular, in section 4.1 we summarize the approaches of vWSN, while in section 4.2 we discuss the main concepts of network security in vWSN.

Using cloud computing which is the modern as well as next generation technology to deliver various types of services

including but not limited to storage, networking, database, server, software and more over the internet ('cloud') to offer on-demand, fast, flexible, economic delivery of service. Security is one of the key concerns in cloud computing. Since one of the key feature of cloud computing is virtualization which is proposed for virtual wireless sensor network (vWSN) which is based on virtualization and cloud computing technology, centrally managed device having flexible and configurable parameter with less maintenance and operational cost

As mentioned earlier that vWSN is also a VM, by design VMs are isolated from each other (figure 3). Because of this isolation, multiple VMs can run securely while sharing same hardware. Guest OS in one VM can't detect any device other than the one which is made available to it. Failure of guest OS in one VM does not affect other VM running on the same host. Since virtual machine shares memory, CPU, IO devices and other physical resources whose access takes place through VMkernel hence VM can't avoid this level of isolation

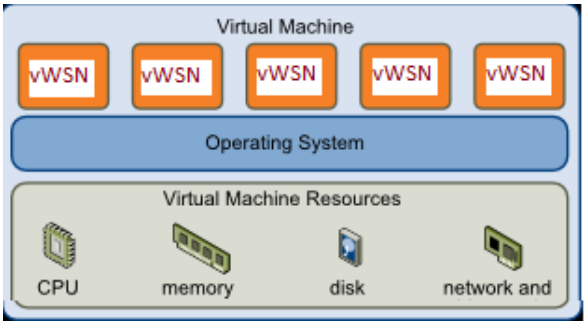

Figure 3. Virtual machine and its resources

A network card is required to communicate between two physical machines, similarly a virtual switch is required to communicate between virtual machine running in the same host (Figure 4).

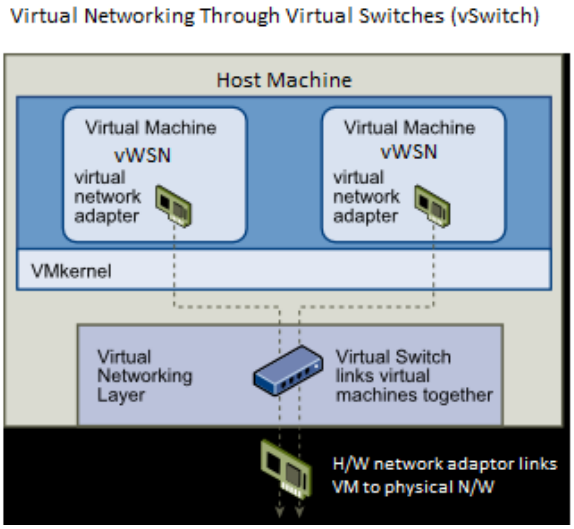

Figure 4 Virtual network through virtual switches (vSwitch)

Industries are moving towards virtualizations due to many reasons one of them is to improve the performance by providing dynamically created virtual machines within a hypervisor as scalable Internet service (Example: Amazon EC2/S3). However, security of VMs became a significant concern. MacDonald [5] pointed out, "Through 2009, 60 percent of production VMs will be less secure than their physical counterparts." Security in virtualization is complex.

Some of the security vulnerabilities analyzed by Reiser, Garfinkel and Kirch [6-9] in virtualization environment are mentioned below:

- Break of isolation: as mentioned earlier, within same host VM shares hardware resources therefore a VM can monitor or access another's one or host machine.
- Remote management vulnerabilities: administrator can manage VMs remotely using management console (Example: XenCenter) therefore vulnerabilities such as SQL injection, Cross-site scripting cannot be denied.
- Denial-of-service (DoS) attack: it is a well known type of vulnerability which takes all resources from host on which VM resides. Therefore resource unavailable to its intended users temporarily or indefinitely. Three types of DOS attacks are volume based (Example: UDP floods, ICMP floods), Protocol attacks (SYN floods, ping of death) and Application layer attack.
- Virtual machine based Rootkit (VMBR): it enables administrator-level access. VMBR runs underneath an existing OS and remains invisible. If compromised, can gain control of hypervisor. Examples of VMBR are BluePill and SubVirt [10].

Revert to snapshots: Snapshot is a mechanism to make a copy of virtual machine disk file. This is used to restore the VM to a particular state in case of failure or system error. This may cause security problems such as re-enabling disabled accounts and passwords

Isolation [11] in virtualization is one of the key issue which plays crucial role in VMs to guarantee that one virtual machine (vWSN) cannot affect other vWSN running within the same host.

Virtual network is a method to create independent logical network within shared physical network. This is true across all hypervisor. In this paper we will demonstrate how the virtual network works in Xen hypervisor through an example. Xen hypervisor is an open source standard for virtualization [12][13]. It is secure as well as widely used for virtualization solution. It supports multiple guest OS (Linux, Windows, Free BSD). Xen can host multiple guest operating systems, each one executes in its own secure virtual machine called domain. The first domain is, domain 0 which is created automatically when system boots. Domain 0 has special management privilege.

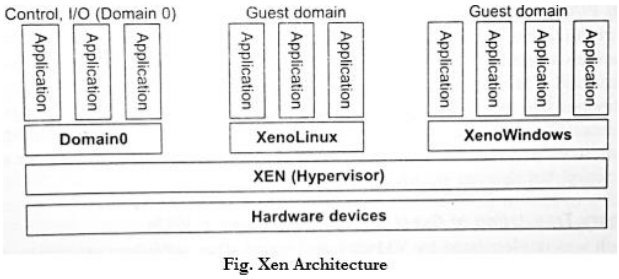

Fig. Xen Architecture

Figure 5. Xen Architecture

Network setup in Xen host can be done in three ways [9] bridging, routing and NAT

In this mode, bridging along with dom0 is used in order to permit transparency between virtual (vif) and real interface. Attach the VM's interface as shown below, directly to software Ethernet Bridge (Bridge0) connected to the physical network.

By default, when Xen starts up, Network Bridge is configured as following steps:

- Create backend domain a new bridge named Bridge0;
- To assign MAC address to virtual interface veth0, either physical interface MAC address is copied or a random sequence of bytes are used or sequence within a specified range is used (Example: 00:16:3e:xx:xx:xx)
- Rename real interface eth0 to peth0 and the virtual interface veth0 to eth0;
- Attach virtual devices interface and physical interface vif<DOMID.DEVID> and Peth0 respectively to Bridge0.
- Brought up bridge0, peth0, eth0 and VIF0.0

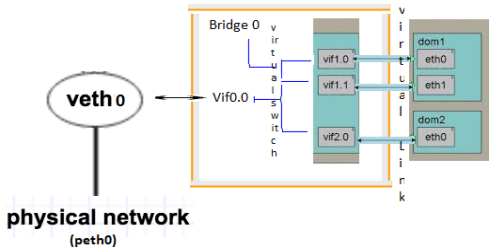

Figure 6. Network-Bridge and VIF-Bridge connectivity in Xen

When a dom starts, a script is run bringing VIF< DOMID>.0 and Bridge0 are attached and VIF< DomID.DevID> is brought up. Multiple interfaces can also be attached to a bridge.

Another mode Xen offers to configure virtual network is called routing. Unlike bridging, IP address assignment is required for each interface in guest domains and dom0. This is required to facilitate packet routing. Packets are moved from dom0's physical interface (peth<>) to virtual interface (vif<#.#> and after that XEN takes the responsibility to further route the packets.

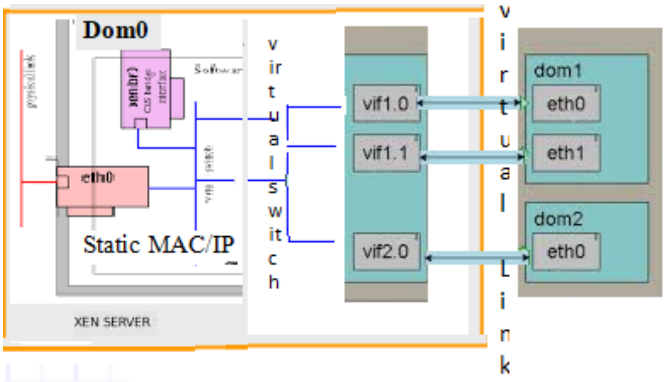

Figure 7. Route in XEN. Domo has multiple physical Interfaces

Using this method link between dom0 and each VM is created. dom0's routing table must have routes to each VM before VM starts. An available (MAC, IP) pair is assigned to each VM instance created by Xen and released when the VM is terminated. Route mode doesn't support DHCP.

Steps to configure routing in Xen:

- Enable dom0 IP forwarding.
- Bind the domU's vif to the virtual network
  vif = ['bridge=xenbr0, rate=40Kb/s']
- Copy IP address (VIF<DomID#>.0) ← IP(eth0)
- Bring up VIF<DomID>.0;
- Add static route for domU IP and MAC address of host specified in domU config file and route the traffic to interface VIF< DomID>.0.
  vif=['ip=192.168.1.1']
  for multiple devices:
  vif=['mac=00:16:3e:71:02:03,ip=192.168.14.13', 'mac=00:16:3e:71:03:02,ip=192.168.57.12']

This is another mode of routing that Xen supports. Guest domain hides behind dom0 IP for external traffic. Each VIF<#.#> is given it own IP address on a private network. Address translation is performed at dom0 to connect entire private network via a single public IP.

Configuration of NAT is almost similar to other mode except that NAT is enabled in backend domain (domU). Steps below:

- Create network bridge
  brctl addbr br0
  ifconfig br0 10.0.0.1 up
- Enable forwarding
  echo 1 > /proc/sys/net/ipv4/ip_forward
- Enable iptables in dom0 to do NAT translation.
- Setup the network interface from guest domain
  ifconfig eth0 10.0.0.2 up
  route add default gw 10.0.0.1

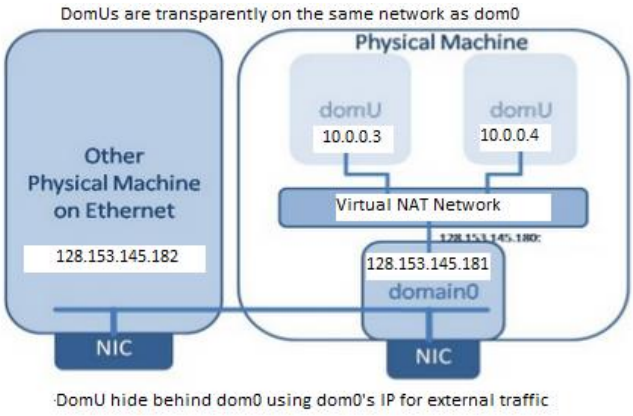

Figure 8. NAT Mode

4. Virtual Network Vulnerabilities in vWSN

Network virtualization share resources from physical network among different virtual networks. One of the biggest security challenges in design of cloud computing platform is VMs interconnectivity using virtual network which significantly affects security. Dedicated physical channel is the more secure way to isolate each VM. Bridge and route is used to link VMs in virtual network. As a result isolation can be easily broken.

The follows are the vulnerabilities existing in the current virtual network.

- Sniffing virtual network: Packet can be captured using various sniffer tools like ethereal (wire shark) because VMs share the virtual hub to communicate in bridge mode.
- Spoofing virtual network: route plays significant role in route mode. It act as a "virtual switch" which uses a dedicated virtual interface (vif) to connect each VM. Hence VM can do an Address Resolution Protocol (ARP) spoofing by redirecting packets to them and able to sniff packets between VMs.

Figure-9, illustrates how spoofing works in virtualization environment. ARP is used to convert an IP address into a matching physical address. Routing table is initialized by sending ARP command to each VM when a virtual route starts at boot time. Routing table thus update its record using the information.

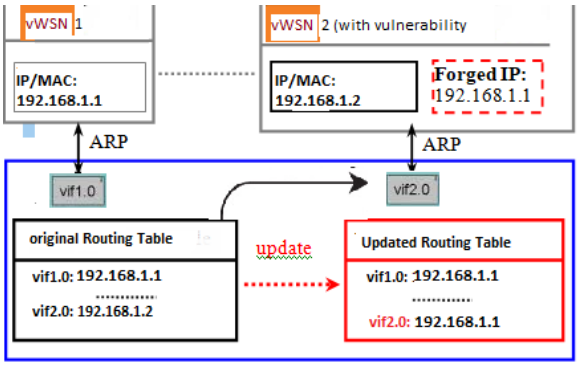

Fig. Spoofing in virtual sensor network

Figure 9. Spoofing in virtual sensor network

In figure 9, ARP spoofing attack is launched by vWSN2 (VM) by forging same IP address with vWSN1 and sent an ARP to virtual route. As a result the virtual route will get updated by the latest information received from vWSN2 VM. Because of this any traffic destined vWSN1 would be sent to vWSN2, then vWSN2 VM could sniff or modify it before forwarding.

5. Virtual Network Model for vWSN

As we discussed various vulnerabilities that exits in virtual network due to bridge and route modes hence proposing a model by combining them to make communication among VMs more secure. The proposed model consists three layers: shared network, firewall and routing layer as shown in figure below.

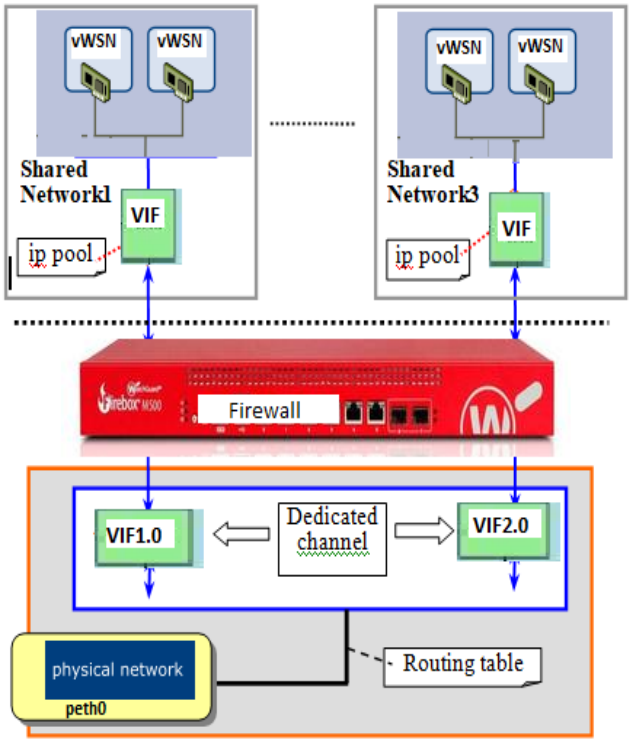

Fig. virtual network model

Figure 10. Virtual network model

5.1 Routing layer

This layer is responsible to connect between virtual and physical network using dedicated logical channel. To distinguish between various devices (vWSN) in a shared network, a unique id is stored in a configuration file. These unique IDs are then assigned to each vWSN for uniqly identifying the source during communication.

Standard of care, doctors helps to consider all the treatment options, out of which best treatments known. Different types of doctors work together, which helps them to create a patients overall treatment plan that combines different types of treatment, which is called multidisciplinary team.

5.2 Firewall (Middle layer)

Firewall is a software program which prevents unauthorized access of a private network (in this case virtual shared network). Firewall is used to inspect each inbound and outbound packet once it arrives on virtual interface (vif) either to allow, monitor or block. ACL (access control list) rules and various policies are defined at firewall layer such that no virtual interface in the routing layer can communicate to any other virtual shared network other than the one which it is suppose to. Similarly other policy can prevent those packets which can possibly modify the routing table. There can be any number of policies configured based on the requirement and use case.

5.3 Shared Network Layer

Security policies at this layer are primarily to block the communications among vWSNs within the same virtual shared network. To implement security at this layer, one possible solution is to put each virtual shared network in a unique subnet.

6. Conclusion and Future work

In this paper we have presented vWSN, physical WSN replacement by virtual WSN using VMware technique is proposed. WSN can be replaced by easily manageable vWSN which is much simple, cost effective, efficient and configurable. An approach of virtualization and cloud computing technology (Security is one of the most significant concern in cloud computing. Since virtual wireless sensor network (vWSN) is also a VM which can be hosted on the cloud) centrally managed device having flexible and configurable parameter with less maintenance and operational cost, and security of virtual network (Xen platform), without virtual network, cloud platform is not possible. We proposed three layer virtual network framework to enhance the security of virtual WSN when deployed in a physical machine and inter communication is required among various virtual WSN. The proposed model can efficiently prevent virtual WSN from various attacks. There are lots of scopes to extend vWSN in the area of security, optimization, and load balancing as well as clustering techniques.

References

[1] Mike Brown.; VMware vCenter Server™ 6.0 Deployment Guide VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com, 2015.

[2] Durairaj.M.; Kannan.P . A Study On Virtualization Techniques And Challenges In Cloud Computing, IJSTR,2014, 3,147-151

[3] Durairaj.M.; Kannan.P . A Study On Virtualization Techniques And Challenges In Cloud Computing, IJSTR,2014, 3,147-151
[4] Tanuja Jha.; Rashid Hussain. WSN CONTROLLED INSECTS MONITORING: IDENTIFICATION OF ONION THRIPS. IJCAR, 2014,6,5257-5260
[5] Neil MacDonald. Security considerations and best practices for securing virtual machines. Gartner, Inc., March 2007.
[6] Hans P. Reiser. Security Challenges with Virtualization. December 2009.
[7] Virtualization: What are the security risks? (Jan 22, 2008), http://www.zdnet.com/blog/security/virtualization-what-are-the-security-risks/821.
[8] T. Garfinkel and M. Rosenblum. When virtual is harder than real: security challenges in virtual machine based computing environments. In HOTOS'05: Proceedings of the 10th conference on Hot Topics in Operating Systems, pages 20–20, Berkeley, CA, USA, 2005. USENIX Association.
[9] J. Kirch. Virtual Machine Security Guidelines Version 1.0. The Center for Internet Security, September 2007.
[10] Introducing Blue Pill (June 2006), http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
[11] Discover the linux kernel virtual machine (April 2007), http://www.ibm.com/developerworks/linux/library/l-linux-kvm/
[12] Xen (July 2008), http://en.wikipedia.org/wiki/Xen#History.
[13] https://wiki.xenproject.org/wiki/Network_Configuration_Examples_(Xen_4.1%2B)
[14] I.F.Akyield, "wireless sensor networks: a survey" computer networks 38 (2002) 393-422.
[15] Seapahn Megerian "Exposure in wireless sensor network: Theory and Practical solution" wireless networks 8, 443-454, 2002. Kluwer academic publishers, Manufactured in the Ntherland
[16] K. Ramesh Rao "Node Activities Learning (NAL)Approach to Build Secure and Privacy-Preserving Routing in Wireless Sensor Networks" Vol. 10, No. 3, December 2018, International Journal of Communication Networks and Information Security (IJCNIS)
[17] Bongisizwe E. Buthelezi "ZigBee Healthcare Monitoring System for Ambient Assisted Living Environments" Vol. 11, No. 1, April 2019, International Journal of Communication Networks and Information Security (IJCNIS)