International Journal of Parallel Programming (2020) 48:280–295
https://doi.org/10.1007/s10766-018-0580-z

A Novel Security Model for Cooperative Virtual Networks in the IoT Era

Salah A. Alabady[1] · **Fadi Al-Turjman**[2] · **Sadia Din**[3]

Received: 29 January 2018 / Accepted: 5 June 2018 / Published online: 30 July 2018

Abstract

The Internet of Things (IoT) has particular applications in public safety as well as other domains such as smart cities, health monitoring, smart homes and environments, smart industry, and various types of pervasive systems. The attacker can simply attack the IoT device in such applications, because it is randomly distributed, dynamic topology and not reliable due to energy and communication limitation. Moreover, the threat to confidentiality and security is increasing as the number of devices connected in IoT is increasing. As the numbers of devices connected to the Internet is expanding, the threat to confidentiality and security is increasing. The aim of this paper is design a typical network security model for cooperative virtual networks in the IoT era. This paper presents and discusses network security vulnerabilities, threats, attacks and risks in switches, firewalls and routers, in addition to a policy to mitigate those risks. The paper provides the fundamentals of secure networking system including firewall, router, AAA server and VLAN technology. It presents a novel security model to defense the network from internal and external attacks and threats in the IoT Era. A testbed is built to investigate the proposed model, and the performed assessment show an effective security performance with a good network performance.

Keywords Network security policy · Attacks · Internal and external threats · Configuration weaknesses · Security of IoT

✉ Fadi Al-Turjman
fadi.alturjman@antalya.edu.tr

Salah A. Alabady
eng.salah@uomosul.edu.iq

Sadia Din
saadia.deen@gmail.com

[1] Computer Engineering Department, College of Engineering, University of Mosul, Mosul, Iraq

[2] Department of Computer Engineering, Antalya Bilim University, Antalya, Turkey

[3] Kyungpook National University, Daegu, Korea

1 Introduction

Recently, with the growth of wireless sensor networks (WSNs), developments have been made in Internet of Things (IoT) with extensive and different applications. There are awesome expectations of advancement and application in IoT, that applied in many features of human life, such as public health, environmental monitoring, Intelligent Transportation System (ITS), etc. [1]. Data, images, and videos exchange over IoT is a requirement in various applications, including smart industry, smart structures, and smart transportations that include aerospace and automotive. Any disclosure of these sensitive messages in those applications is unacceptable [2]. IoT is affecting every aspect of our life, the aerospace and automotive industries are no exception, and both fields are making huge strides in their application in the IoT era [3]. In [4], the authors present a review fundamental concepts, recent developments and critical design factors under IoT-specific constraints and objectives. The review covers some of the current and future concepts of networking such as WSNs and IoT. In addition, the future research for routing protocols includes the integration of sensor networks with wired networks in IoT is providing. By way of IoT being increasingly applied, the life is becoming more and more convenient and comfortable. However, with the rapid development of networks and communications technologies, the problems of privacy and security are becoming serious. In spite of the fact that Internet security architecture model has been extremely exceptional, there are yet huge numbers of assault. For instance, a great number of malicious nodes send information in the meantime; it will lead to DoS attack. Therefore, the particular network should be built for suitable IoT transmissions. Even though the current internet has security protection methods, there are still some common threats including illegal access networks, integrity damage, DoS attack, eavesdropping information, confidentiality damage, Man-in-the-middle attack, virus invasion, exploit attacks, etc. How, to ensure that is convenience and reduce the risks at the same time seems to be a long-term work. From this viewpoint, the paper studied the reasons of privacy security risks, and explained some related IoT risk prevention methods. For IoT security, the IoT should have three characteristics: intelligent processing, complete intuition, and reliable transmission [5].

In the automotive area, the application of sensors has been one of the largest development areas. Several significant numbers of sensors within vehicles are used for engine operation, system monitoring, and emission control. Utilizing Vehicle to Infrastructure (V2I) communication permits better movement stream in various conditions [6]. V2V communication defines a communication between vehicles, through technologies such as Dedicated Short Range Communication (DSRC), long-term evolution for vehicles, and Visible Light Communications [2]. Nevertheless, these protocols were designed for safety and efficiency rather than security [7]. The attacks useful from some remote vehicular vulnerabilities, for example, physical endpoint devices, and outside communications, such as, Dedicated Short Range Communication (DSRC) and Bluetooth [2].

The authors in [8] emphasize the importance of safety in the aviation industry, at least 28 aircraft accidents or complications are linked to suspected unapproved parts (SUP), which are counterfeit aircraft parts, which do not meet the level of approved aircraft parts. In addition, the authors in [8] claim that IoT can be reliably used to identify counterfeit products and elements, and hence improving the safety and security of the products. One way used to identify original parts is by examining the accompanying documents, however, this is a tedious and time-consuming task, therefore, an electronic system can be developed to document the origin and safety–critical events of specific parts during their lifecycle. This information is stored in a decentralized database and Radio-Frequency Identification (RFID) tags and attached to the aircraft parts. Therefore, before installation of any parts, we can get an authentication by getting a digital signature and comparing the information from the RFID tags with the one found in the database. By doing this, we significantly improve the safety and operational consistency of the aircraft. The automotive industry has taken a new turn with the introduction of IoT, the authors in [8] remark that we are equipping cars, buses, bicycles, and trains with advanced sensors and actuators with processing power to improve their performance and efficiency. Smart things were used in automotive to monitor and record parameters such as pressure in tires and the proximity of other vehicles. Moreover, RFID was used to advance logistics, increase quality control and improve customer services in automotive production [2, 9].

Furthermore, RFID technology is used to provide real-time data in the manufacturing industry and in the maintenance operation, offering new ways of managing recalls more efficiently. The authors in [2] also talk about Vehicle-to-Vehicle (V2V) and vehicle-to-infrastructure (V2I) communication which will have significant improvement in the Intelligent Transportation Systems (ITS) applications such as traffic management and the safety of the vehicles, according to [2], this will completely integrate the transport infrastructure to IoT.

On the other hand, increasing the demand of the Internet in home and work environments has radically increased the vulnerabilities of networks systems to attack from a wide variety of threats. Without satisfactory network security, many persons, and administrations are at risk. Therefore, the need to vital solution for secure network is becoming more significant and imperative to design a high-performance network security infrastructure [5, 10]. In addition, many services enabled by the default configurations of network devices are always vulnerable to network attacks. Consequently, it is inevitable to re-configure and all unnecessary services should be disabled.

Although most secure plans can restrain and reduce the impacts of attacks, attack detections and avoidances are still requirement for framework security [11]. Saturation attacks, denial of service (DoS) attacks, and Man-in-the-middle attacks are still as opens security challenges [12].

In [12] the authors provide a survey of security challenges in the software defined networking (SDN). The authors exhibited investigate security threats to application, control, and information planes of SDN. Salah and Chaudary [13] propose a network security model based middle boxes with intrusion detection systems, network firewalls, and email spam filters. The authors [13] show the performance of a certain security depends on the middlebox processing capacity and type of hardware it is built on.

Bechtsoudis and Sklavos [14] present a penetration test procedure (planning, discovery, exploitation and reporting) to depiction possible useable vulnerabilities in every network layer. The authors show that although the vendor updates not enough for an effective security strategy, but it is still necessary. In [15] a method for detecting malicious and infected nodes on external Internet and monitored networks is presented. Carter et al. [15] show the effectiveness of probabilistic threat propagation on the tasks of detecting malicious web destinations. In addition, they present a method for producing statistical probabilities through iterative propagation.

In [16], the attack survey and evaluate existing solutions designed to mitigate several attacks is described. The authors [16] propose a mitigation solution based on a dynamic fair IP addresses allocation algorithm to mitigate the problem of DHCP starvation attacks. In [17], the authors presented an efficient firewall query processing algorithm to use as core data structure. The work in [18] presents a new idea of network security virtualization (NSV). NSV used to create a virtual version for security resources or security functions to network administrators or users. In addition, it offers security response functions from network devices.

In [19] an advanced method to modeling network designs in order to quantify their ability to mitigate the impact of denial of service attacks on end-user services is describes. The authors in [20] present a survey of game theoretic solutions to increase network security and classifications of existing game theoretic approaches to network security. The work in [20] compares different game theory solutions and shows that the game theoretic approaches are powerful tools for solving network security problems.

In this article, a network security model using firewall, router, Virtual Local Area Networks (VLANs), in addition to the AAA (Authentication, Authorization, Accounting) server is presented. The aim of this work is to construct a valid network security model that can be used to protection data and suggest a solution to alleviate the problem of several attacks. The paper details issues such as switch and router weaknesses, including a list of some attack types and common security policy and configuration weaknesses that should be avoided.

This paper is organized as follows. Section 2 provides VLAN technology background. We presented threat and attacks on layers two and three in Sect. 3. Section 4 presents the security policy. Creating and implementing a security policy was presented in Sect. 5. Section 6 presents network security testing configuration. Finally, the paper is concluded in Sect. 7.

2 VLAN Technology Background

In this section, an overview of Virtual Local Area Networks (VLANs) is presented. The capability to create VLANs is consider the one important feature of the Ethernet switching. A VLAN is a virtual cluster of network nodes and devices that connected to the Ethernet switching [21]. The basic function of a switch is either to forward a unicast, multicast, or a broadcast traffic on VLAN segments and this can lead to significant improvement in terms of the network performance [22].

Broadcasts and segment a broadcast domain can contain when a VLAN is implemented and a switch logically divides its ports into isolated segments. In this manner, the nodes on a VLAN cannot communicate with nodes on another VLAN. Consequently, to communicate between VLANs, a router is required. The router forwards packets between VLANs through the VLAN trunk port. Routers offer connectivity between various VLANs, traffic flow management, broadcast filtering, and security. In addition, the routers are an imperative part of a network and their security is a fundamental part of the general security for the networks they serve [23]. Correctly planned and designed VLANs are influential tools for network administrators. The benefits of VLANs are allowed network administrators to organize their LANs virtually instead of physically and enable administrators to cluster the network users according to the network services they use most frequently. This allows network administrators to perform several tasks for network management such as, easily move or add nodes to the LAN, easily control network traffic, easily change the network configuration, decrease broadcast traffic and improve security [23, 24].

Three types of VLAN memberships, including Protocol-based VLANs, dynamic VLAN, and static VLAN. In this work, the static VLAN is used where End-user devices become members in a VLAN based on which physical switch port they are connected. VLAN technology is not just utilized as an essential part of the LAN environment. VLAN is currently likewise being utilized as assets of providing WAN/MAN services. Regular issues related with this technology and a poor VLAN configuration cause to reduce the overall network security and expose the network to attacks. Therefore, network administrator shall take this into consideration when implementing VLAN to protect network against threats and attacks [22, 23].

3 Threats and Attacks in Layers Two and Three

Internet applications keep on growing exponentially. For example, private, management, administration, and industry serious applications become extra comprehensive on the Internet. Nonetheless, there are several benefits, these information resources, services and applications may be exposed to many risks and attacks. The common goals and objectives of network security are commonly regarded to be assuring availability, maintain integrity, protect confidentiality, accountability and assurance [13].

In the network security filed, three common terms are used, attack, vulnerability, and threat. Usually, the threats use a multiplicity of tools, and programs to presentation attacks opposite to networks. On the other hand, four major categories of threats to network security, internal, external, structured, and unstructured threats [24]. Internal threats consider a main source of damaging network security [25]. These threats normally root from either unprincipled or dissatisfied employees. On the other hand, external threats, usually mentioned to as hackers, they are sometimes similarly and riskier than internal threats. Normally, the hackers use a few some applications and tools to discover significant information or a way to access into a network. Examples for those tools are; password sniffers, IP snooping, E-Mail attacks. Usually, these threats are continuing because of vulnerabilities that can occur because of miss-configured software or hardware, low quality network design and policy, characteristic technology weaknesses, or end-user carelessness. Recently, many threats have become cunningly applied attacks causing committing larceny or damage. The common threats on firewall and router include session hijacking, re-routing, and denial of service (DoS), unauthorized access, information theft, and eavesdropping. Attack methods and technologies include: simple network management protocol (SNMP) attacks, routing protocol attacks, password guessing, rerouting attacks, session replay attacks, smurf attack, TCP SYN attack, land attack, IP fragmentation attacks. Illustrations of DoS attacks are Packet fragmentation, E-mail bombs, Ping of death, reassembly, miss-configuring routers, malicious applets, SYN flood attack, CPU hogging, and the chargen attack [24].

A weakness that is characteristic in every network and device called Vulnerability. This includes firewall, routers, switches, servers and desktops. The vulnerability can originate from mis-configured software and hardware, poor network design, characteristic technology weaknesses and end-user neglecting. Three primary vulnerabilities or weaknesses; technology weaknesses, configuration weaknesses, and security policy weaknesses.

In general, there are two main categories of attacks whose ambition to compromise the network security: active and passive attacks. During active attacks, the attackers adapt information, disturb services and target to advance unauthorized access to the network systems. Supplementary, an active attack goals to effect disruption and is normally easily recognized. On the other hand, in a passive attack, the attacker basically, observers the communication between two stations and captures information that was sent and received. During a passive attack, the attacker does not aspire to interject the service or cause an effects, he only read the information [14]. With this in mind, it is imperative that all information and communications must encryption.

Attacker purposes separated into four fundamental classes: reconnaissance, fabrication, break or interruption and modification. The first class is reconnaissance attacks, where the attacker attempts to achievement unauthorized access, detection and planning of network systems, services, or vulnerabilities. The examples of this attack are snooping on a communication link where important data are transmitted, ping sweeps, packet sniffers, port scans, and Internet information queries.

The second class is the fabrication attacks that ambition to avoid authenticity checks by imitator or impersonator information [14]. An interruption attack cause to be network resources unavailable. Denial of service (DoS) attacks is a simple example [23]. DoS attack is the greatest common attack in WSN and Internet. It causes loss of network resources, and makes the service unavailable. DoS attack is an attempt to make network resources unavailable to authentic users. DoS attacks include slowing the system down to the point that it is unusable or crashing the system. In addition, DoS attacks can be as straightforward as erasing or corrupting data. For the most part, performing the attack includes running a hack or script. The attacker does not require prior access to the target. For these reasons, DoS and distributed DoS attacks are the most feared and the most threatening security challenges [12]. Finally, the fourth class is modification attacks purpose to change data that is transferred during a communication session of two or more nodes. Network spoofing attack is a simple example of that attack [26].

Switches as routers are vulnerable to many of the same layer 3 attacks. One kind is VLAN hopping attacks. In this kind, an attacking system sends out packets destined for a system on a different VLAN that cannot usually reached by the attacker. Switch spoofing and double tagging are two diverse types of VLAN hopping attacks. Private VLAN vulnerabilities, private VLANs work by constraining the ports within a VLAN that can communicate with different ports in the same VLAN. Spanning-Tree Protocol vulnerabilities, the network attacker plans to spoof his system as the root bridge in the topology and after that, the network attacker can change the network topology. In this case, the attacker offers the idea that the attacking host is a root bridge with a higher priority. When the Content addressable memory (CAM) table limit is achieved, the switch works as a hub and simply floods traffic out all ports. DHCP starvation attacks work by broadcasting DHCP requests with spoofed MAC addresses [15, 16]. MAC spoofing normally used the known MAC address of another host that is authorized to login the network. One example of the man in the middle attacks is the MAC spoofing.

In IoT there are numerous sensing/communication devices and technologies, such as RFID, sensors, Global Position System (GPS), gas inductors, laser scanners, and infrared sensors. These technologies represent the main equipment in the perception layer. The wireless network transmission is the way of information transmission after the data are collected. In this case, the information signals are bare in the public place, and the signals can be observed, captured, and easily troubled. Because the most of sensing devices are installed in the unmanned monitoring sites, the attackers can easily achieve an access to the equipment, control and/or physically damage it. For instance, the Differential Power Analysis (DPA) is a very effective attack in these scenarios.

Like a computer, any security vulnerabilities in the IoT devices could make the information stored on or transmitted through that device at risk. Consequently, as users install and use more smart devices in their works and houses, the numbers of vulnerabilities are increased, which could enable intruders to access and misuse private information and transmitted to or from the device. Denial of Service attacks, message replay attacks, and false information attack, these attacks are all present in Vehicular Ad hoc Network (VANET) and in modern vehicles. In as much as IoT devices increase, vulnerabilities could enable these attackers to use large numbers of devices in such attacks. Accordingly, we should assure that devices in IoT applications are secured. A portion of the security threats of IoT devices is same as those in the conventional Internet. New cars these days are equipped with various types of sensors, such as global positioning system (GPS) can give data about wherever a client visits. An attacker or a hacker can steal the user's information and identity, which can cause serious problems. If the GPS of a car is compromised, the attacker can get the data about the area of the user, which can cause a significant privacy issue for him.

4 Security Policy

Security policy is the meaning of security purpose against a network interruption and intrusion. Security engine gives security functions of a packet filtering, an authentication, an access control and an intrusion investigation and analysis [17, 25]. In this section security policy for firewall, router and AAA server that used in the network security model are presented. AAA is the abbreviation from ("authentication, authorization, accounting"). Authentication controls access by requiring valid user identifications, which are regularly a username and password. Authentication defined is the technique for identifying users before enabling access to a network. Authorization is the technique used to define a user that has the privilege to do once he has authenticated to the network, and controls the administrations and commands available to each confirmed user. Accounting is the part that takes into consideration log and trailing of user and traffic activities on the router, which can be utilized for resource tracking. AAA can be managed from a central server running RADIUS (Remote Authentication Dial In User Service) or TACACS + (Terminal Access Controller Access Control System Plus) protocols or can be applied on a device locally [23].

The most practically server kind is the TACACS + Server and it was chosen in this paper for that reason. TACACS + encrypts the complete TACACS + packet, whereas RADIUS only encrypts the shared secret password portion. AAA security is essential parts of the general network security policy of an institute. AAA is fundamental for secure remote access and management for the network devices. Utilizing AAA offers three principle advantages; supports standardized protocols, allows multiple backup systems and provides scalability.

Router is considered a vital part in networks and Internet, that defines the best path in the network to reach a destination and controls the data packet flow. In addition, router provides good security solutions when the administrator applies a good security policy. Routers provide different functions, such as forwarding traffic between two or more local networks, filtering, encrypting, relaying, and observing information streams. Actually, these functions influence the confidentiality, integrity, and availability of information connections in security is critical network mechanisms. However, configuring the router for good network security is not easy to task. Similarly, to other network devices and many computers, the router has many services and protocol enabled by default. Several services and protocols are needless, and an attacker can use it for data collecting or for exploitation. Therefore, it is better to deactivate all unnecessary protocols and services in the router configuration to avoid the attacker from using it in case he plans to harm the network and network devices configuration or to steal the significant data. Because of the router is generally used to manage network traffic and connects at least two different networks, the security is essential to rule of an illegal network intrusion, and an unauthorized router access. Secure router innovation has security capacities, for example, intrusion discovery, access control and IPsec, that applied to inheritance router for secure networking [15, 23].

Firewalls are considering vital elements in network security, which are hardware, or software that applied an access control policy between at least two networks. Firewall provides stability between security and simple outbound access to the Internet, which is frequently used for e-mail and Web servicing. Firewalls are hitherto another measure used to increasing the level of security in a network [17]. The first and most important function that all firewalls must perform is to control and manage the network traffic that is allowed to access the protected network. The purpose of firewall is investigative each outgoing and incoming packet and decides whether to accept or to reject the packet based on its security policy.

In addition, packet-filtering are a positive step in increasing network security. Packet filtering or packet inspection is the process of interrupting and processing the data in a packet to decide whether it should be allowed or denied based with the access list policy. Packet inspection can look at any or all of the elements such as source IP address, source port, destination IP address, destination port, IP protocol and packet header information to making a filtering determination. In that case, a firewall examiner all packets of a message try to pass through the network and deny the packets that do not satisfy the security policy. However, it does not secure the transmitted information. Most firewalls have been afflicted with security policy errors because the deficiency of tools and analyzing firewall policies. A firewall policy error either makes security breaks that will enable malicious traffic to sneak into a private network or blocks authentic traffic [18, 19]. Firewall and routers are exceptionally parts of network security. Attentive administration and persistent review of routers and firewalls operations reduce network interruption, avoid the authorized users, and decrease network threats [16].

Hackers and attacks exploit some protocols and services in network devices to discover the weakness in the network. Samples for these protocols and services are following; Cisco Discovery Protocol (CDP), Simple Network Management Protocol (SNMP) Services, Internet Control Message Protocol (ICMP) messages (i.e., IP Unreachable, Redirects, and Mask Replies), UDP and TCP small servers, finger server, HTTP server, Bootp server, IP source routing, proxy ARP, and IP directed broadcast. A more exhaustive description for these protocols and services can be found in [23, 24].

The general threats on switch, router and firewall included but not limited are session replay attacks, DoS, unauthorized access, session hijacking, rerouting, masquerading, eavesdropping, land attack, Distributed Denial of Service (DDoS) attacks, TCP SYN attack, smurf attack, and information theft. The attack methods include: SNMP attacks, redirect (address) attacks, password guessing, routing protocol attacks, IP fragmentation attacks—to bypass filtering, Ping of death, E-mail bombs, SYN flood attack, circular redirect for DoS, and packet fragmentation and reassembly.

5 Security Policy Implementation

This section presents and mentions the necessary setups that must be considered applied in switch, router, access points and firewall to achieve an effective security policy performance and to prevent several kinds of threats and attacks. The configuration of proposed network security model is shown in Fig. 1. The core objective of proposed network security model is to defend against the stated categories of threats and attacks in Layers 2 and 3 of the TCP/IP model. The important thing that must be taken in the consider, added security techniques should not influence extremely on the network performance and management.

Detection threats and attacks can be implemented by multiple methodologies, such as intrusion detection system (IDS) or monitoring techniques [27, 28]. In monitoring, when threats are detected, they give us a good idea about the essential network configuration strategy needs to eliminate ongoing attacks. The principal security matter with VLAN technology is inefficient configuration. Therefore, there are several configurations' matters requirement for the configuration procedure in switching security policy. The idea of the proposed security solutions is constructed on using several security methods and it divided to collections of procedures that explained as followed:

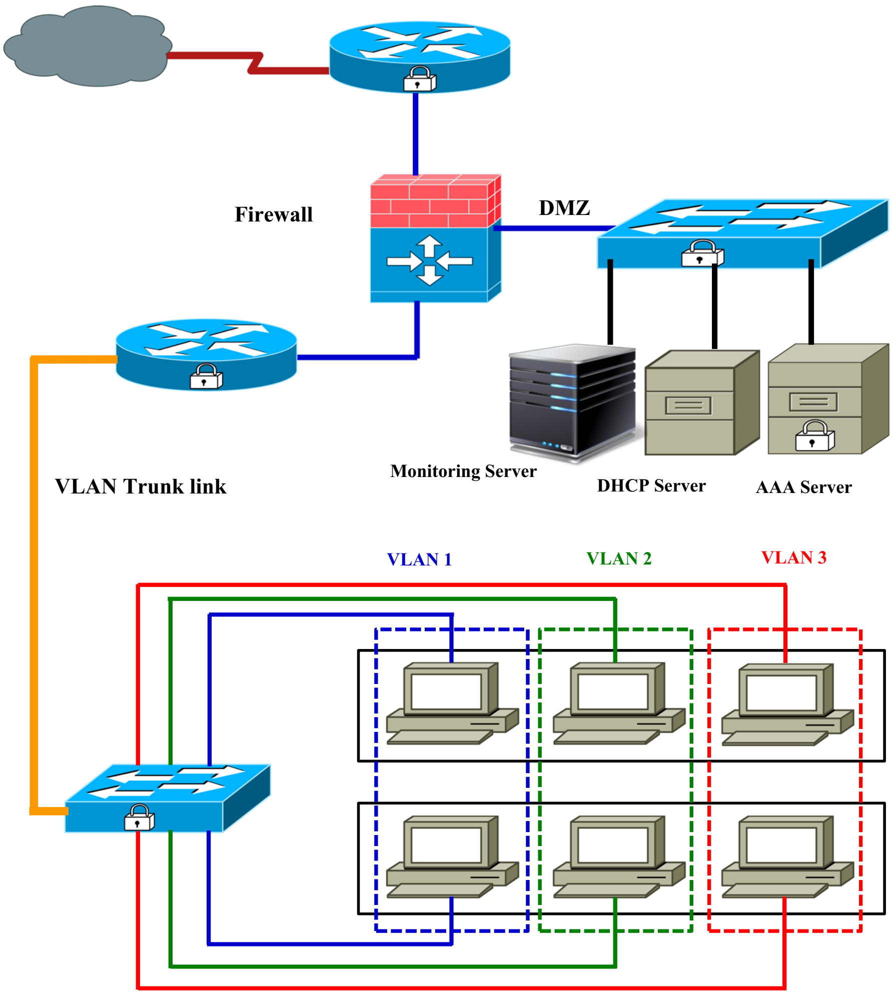

Fig. 1 Structure of proposed network security model

5.1 Physical Security, Password and Remote Access Policies for All Network Devices

1. Create and build physical security policy is an important point through considered who is authorized and have a permission to set up, uninstall, add or change network devices, change physical connections for all network devices.
2. Description authorizers that are have permission to log in and access to network devices by the direct access or console port connections and define the password policy.
3. Identify who are authorized and approved to remotely access to network devices using Telnet and SSH services. On the other hand, restrict use remote management and monitoring services.

4. Change the default password on all network devices and enable secret password for auxiliary port, virtual terminal lines (VTYs) ports, and console port.
5. Encryption all passwords for all network devices using service password encryption facility. This action will prevent the unauthorized from recovery the secret password and disable the recovery password service.
6. To improve the performance of security access to network device, it is important specify a minimum password length.
7. Restrict the connections via the VTYs ports to accept connections with protocols needed, and configure VTY timeouts, and adjustment VTYs to receive only Telnet sessions.
8. Apply the encryption for all communications between the administrator's computer and network device using SSH or IPSec encryption. This action will stop session hijacking and several other network attacks types to collect network traffic during remote access and capture the password.
9. The AAA server checks the entire connection request, authorized and official users can admission to the network based to their security policies. All the connections and access between VLANs requirement pass through the AAA server.

5.2 Disabling Unnecessary and Unneeded Services

1. Disabling IP source routing on the router.
2. Disabling any unnecessary and unneeded features services in network devices such as TCP and UDP small services, http server, IP directed broadcasts, and bootp server.
3. Deactivating some protocols (CDP, ICMP, finger protocol requests, proxy ARP protocol, (NTP) Network Time Protocol) without influence or reduce network performance to deprivation hackers, unauthorized and attacks from utilization it.
4. Using IP Security encryption (IPSec), SSL, or SSH for all remote access to network devices instead of TELNET.
5. Shutdown idle interfaces on network devices, this benefit dishearten unauthorized use extra interfaces to add new network connections to network devices.

5.3 Applied Access Control Lists

1. Extended access control lists (ACLs) was applied in network devices (firewall and router) to block and filter the malicious traffic packets, and inspect all outgoing and incoming packets. This will protect a network opposite to unauthorized access and attacks. Typically, the filtering can do based on three conditions: First, source and destination IP addresses. Second, source and destination ports. Third, type of traffic (protocol).
2. Using the ALCs, all traffic with a source or destination address was declined belonging to any illegal address range or reserved.
3. Apply the VLAN ACLs to filter the traffic routed between VLANs or in the same VLAN.

4. Authentication and Access Control, Apply the ACLs to permit TACACS + traffic to the internal interface of the server.

5.4 Switch Security Polices

1. Deactivate all unused switch ports, and use dedicated VLAN IDs for all trunk ports to avoid VLAN hopping attacks.
2. Turning off DTP on user ports for non-trunking mode.
3. Use the root guard and the BPDU guard features to assure the placement of the bridge in the network and to prevent Spanning tree manipulation.
4. To alleviate and block CAM table overflow attacks, port security applied on the switch. Three ways to apply port security: Sticky secure MAC addresses, Static, and Dynamic secure MAC addresses.
5. To avoid MAC and ARP spoofing attacks spoofing, a port security interface was applied.
6. To alleviate DHCP starvation attaches, a port security applied on the switch.
7. Apply VLAN ACLs (VACL), and IP source guard to limit DHCP replies.

5.5 Router Security Polices

1. Accurate router configuration avoids several kinds of attack such as DDoS attacks.
2. Configure local AAA on router and firewall to controlling logging and access user activities.
3. All user authentications used TACACS + or RADIUS protocols instead of local user accounts.
4. Using NAT (Network Address Translation), in that case the router hides the network structure through translating all IP addresses transparently and coalescing the distinct IP addresses into a single one.

6 Security Testing and Evaluation

Experimental testbed is built in order to test proposed network security model included firewall, routers and switches. Several packet sniffing and network hacking tools involves (Ethereal, Nmap, Password Cracking, Snort, Super Scanner, Port Scanner, DHCP gobbler, Packer Sniffer, Arpspoof tools, Dsniff tools, Nessus program and Kiwi Syslog program) were used and applied on the network security model to intrusions the network and simulate a real scenario that hacker does. The testbed is implemented as shown in Fig. 2. The results represent the network robustness against different types of attacks and performance of the proposed network model. The testbed is consisted from the Cisco switch 2960, Cisco firewall (PIX) 516E, Cisco routers 2811, access point, TACACS + protocol with AAA server and 2 workstations work as attacker. Table 1 illustrates samples of network security testing for differences types attaches and hacker's tools.

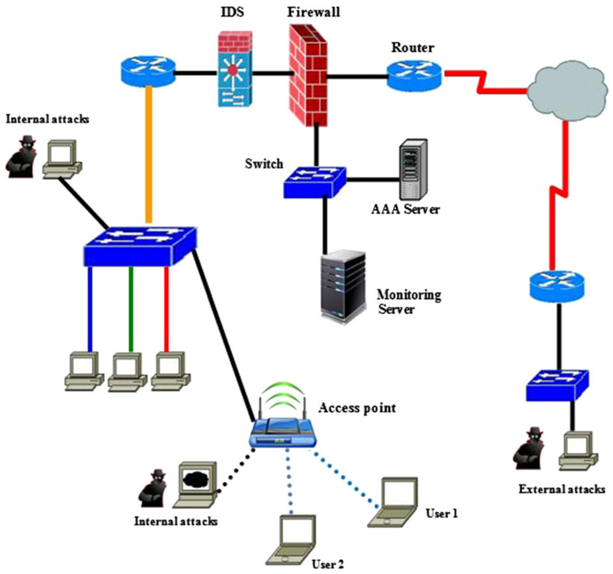

Fig. 2 Testbed network layout experimental

In this work, the following actions were taken to examine and investigate the network security policy opposite to dissimilar types of attacks.

1. Snort program is used as a network intrusion detection system (NIDS) to monitor network nodes opportune, and find the doubtful conduct of nodes. Snort can detect a wide assortment of distrustful traffic and attack attempts.
2. To monitor traffic, Ethereal program was used. Observing network provide cautionary of a number of network security breaches.
3. To simulate sniffer and inspection network attacks the Ethereal program is used. Attempt to find the password. This act was blocked because all passwords was encryption and using SSH, SSL encryption for all remote connections.
4. To imitate an admission attacks, a super scanner program was used. This tool used to discover which the IP and port address that active and open in the network. This action was blocked by the ACLs that applied in network devices.
5. TELNET service, ping, netsata, arp, tracert, and pathping commands were stopped by router, firewall and AAA server access lists.
6. TELNET service was used to access the network devices. This act was blocked because the routers use TACACS + protocols for all user authentications. In addition, we deactivate unnecessary all non-IP-based remote access protocols. We proposed use IPSec encryption, SSL, and SSH for all remote connections.
7. To imitate DHCP starvation attacks, ARP spoof tools and DHCP gobbler programs was used. This activity was blocked by the ACLs in AAA server, Firewall, and routers.
8. To imitate a DoS attacks a Dsniff program was used. This action was blocked by applying ACLs on routers and firewalls. The ACLs prevent the malicious packets, and discard all traffic from the internal side.

Table 1 Samples of network test

Attack type	Tool	Target	Security protection
Network Sniffers	Ethereal, Sniffit and WinDump	Firewall,Routers, Switches, and AAA server	Encrypting all passwords Disable the CDP SSH, SSL, IP Security (IPsec) AAA server
Password Crackers	IMP 2.0, John the Ripper	Firewall, Routers, Switches, AAA server, and PCs	Encrypting all passwords AAA server ACL in router and firewall Apply port security on the switch TACACS + protocols
Scanning and Listing	Fscan (TCP and UDP ports), LANguard Network Scanner, Nmap	Routers, Switches, and PCs	AAA server
Listen to routers, firewalls, and computers	Kiwi Syslog	Firewall, Routers, Switches, and PCs	Disabling protocols such as: Network Time Protocol, CDP, ICMP, multicast route caching protocol and proxy ARP Protocol ALC in router and firewall Perform the port security on the switch
Vulnerability scanner	Nessus	All network devices, including the PCs	Close the unused interfaces on all routers and firewall. Disable CDP, IP directed broadcasts, http server, bootp server, TCP small services, UDP small services and IP source routing ALC in router and firewall Perform the port security on the switch

9. To imitate a MAC spoofing and CAM table overflow attacks, Macof tools was used. This activity was blocked through apply port security policy in the switch using three ways: sticky secure MAC addresses, dynamic and static secure MAC addresses.
10. Nmap program was used to look over of TCP and UDP open ports in the network devices. The attack used port scanner tools to appraisal the network map and estimated the network structure. This activity was blocked by deactivate needless services such as: TCP and UDP small services, and IP directed broadcasts.
11. To examination the vulnerabilities in the network a Nessus program is used. This action was blocked through shut down unused interfaces on network devices, and deactivate unnecessary features and services on route such as: TCP and UDP small services, DP, bootp server, IP directed broadcasts, http server and IP source routing. Furthermore, the NAT is concealing information about the network.
12. To capture and reservation log messages for network devices, a Kiwi Syslog program was used. Because disablement some protocols (finger protocol requests,

proxy ARP Protocol, NTP, CDP, and ICMP) on the network devices, this action was stopped, and that avoid attacks used it.

To investigate the performance of the suggested network security model, several tests is applied on the proposed model. The test results demonstrated that the security policy that applied on the proposed model achieved an actual efficient security performance with an acceptable network performance.

7 Conclusion

Recently, as the number of devices is increasing, privacy and security threats are, also increasing. The improvement of IoT security is an imperative part of IoT. In this paper, an applied network security model for small network topology is exhibited. This model depends on utilizing firewall, routes and AAA server with VLAN technology. The paper clarifies the benefits of utilizing firewall where provides an extra level of protection on network. Utilizing firewall with AAA server together can offer preferred security over it is possible that only one. A poor VLAN arrangement and router filtering configuration cause to decrease the overall network security and expose the network to scans and attacks. Besides, the paper introduced a few suggestions to protect and shield the network from threats, and get a best security and by applying the security setups on network devices. Testbed results on the network security model, demonstrated an extremely effective security execution keeping a best of the network speed and services, which is very desirable in the IoT era.

References

1. Al-Turjman, F., Kirsal Ever, Y., Enver, E., Nguyen, H.X., David, D.B.: Seamless key agreement framework for mobile-sink in IoT based cloud-centric secure public safety networks. IEEE Access (2017). https://doi.org/10.1109/access.2017.2766090
2. Maple, C.: Security and privacy in the Internet of Things. J. Cyber Policy **2**(2), 155–184 (2017)
3. Ulusar, U.D., Celik, G., Al-Turjman, F.: Wireless communication aspects in the Internet of Things: an overview. In: IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), pp. 165–169 (2017)
4. Al-Turjman, F.: 5G-enabled devices and smart-spaces in social-IoT: an overview. Future Gener. Comput. Syst. (2017). https://doi.org/10.1016/j.future.2017.11.035
5. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
6. Faezipour, M., Mehrdad, N., Adnan, S., Sateesh, A.: Progress and challenges in intelligent vehicle area networks. Commun. ACM **2**(90–100), 55 (2012)
7. Luigi, A., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
8. Debasis, B., Jaydip, S.: Internet of Things: applications and challenges in technology and standardization. Wirel. Pers. Commun. **58**(1), 49–69 (2011)
9. Al-Turjman, F.: Cognitive caching for the future fog networking. Elsevier Pervasive Mob. Comput. (2017). https://doi.org/10.1016/j.pmcj.2017.06.004
10. Chu, Z., Nguyen, H.X., Le, T.A., Karamanoglu, M., To, D., Ever, E., Al-Turjman, F., Yazici, A.: Game theory based secure wireless powered D2D communications with cooperative jamming. In: IEEE Wireless Days Conference, Porto, Portugal (2017)

11. Zhou, H., Wu, C., Jiang, M., Zhou, B., Gao, W., Pan, T., Huang, M.: Evolving defense mechanism for future network security. IEEE Commun. Mag. **53**, 45–51 (2000)
12. Ahmad, I., Namal, S., Ylianttila, M., Gurtov, A.: Security in software defined networks: a survey. IEEE Commun. Surv. Tutor. **17**(4), 2317–2346 (2015)
13. Salah, K., Chaudary, A.: Modelling and analysis of rule-based network security middleboxes. IET Inf. Secur. **9**(6), 305–312 (2015)
14. Bechtsoudis, A., Sklavos, N.: Aiming at higher network security through extensive penetration tests. IEEE Lat. Am. Trans. **10**(3), 1752–1756 (2012)
15. Carter, K.M., Idika, N., Streilein, W.W.: Probabilistic threat propagation for network security. IEEE Trans. Inf. Forensics Secur. **9**(9), 1394–1405 (2014)
16. Mukhtar, H., Salah, K., Iraqi, Y.: Mitigation of DHCP starvation attack. Comput. Electr. Eng. **38**, 1115–1128 (2012)
17. Liu, A.X., Gouda, M.G.: Firewall policy queries. IEEE Trans. Parallel Distrib. Syst. **20**(6), 766–777 (2009)
18. Shin, S., Wang, H., Gu, G.: A first step toward network security virtualization: from concept to prototype. IEEE Trans. Inf. Forensics Secur. **10**(10), 2236–2249 (2015)
19. Qiu, X., Paterson, R.: An innovative network security vulnerability modeling method and tool. IEEE Commun. Mag. **48**, 104–108 (2010)
20. Liang, X., Xiao, Y.: Game theory for network security. IEEE Commun. Surv. Tutor. **15**(1), 472–486 (2013)
21. Zhu, M., Molle, M., Brahmam, B.: Design and implementation of application-based Secure VLAN. In: 29th Annual IEEE International Conference on Local Computer Networks (LCN'04) (2004)
22. Otsuka, T.: A switch-tagged VLAN routing methodology for PC clusters with ethernet. In: International Conference on Parallel Processing (ICPP'06) (2006)
23. Alabady, S.A.: Design and implementation of a network security model using static VLAN and AAA server. In: The 3rd IEEE International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA 2008) (2008)
24. Alabady, S.A.: Design and implementation of a network security model for cooperative network. Int. Arab J. e-Technol. (IAJe-T) **1**(2), 26–36 (2009)
25. Giotis, K.: Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Comput. Netw. **62**, 122–136 (2014)
26. Nayak, G.N., Samaddar, S.G.: Different avours of man-in-the-middle attack, consequences and feasible solutions. In: ICCSIT (2010)
27. Lee, C.P., Uluagac, A.S., Fairbanks, K.D., Copeland, J.A.: The design of NetSecLab: a small competition-based network security lab. IEEE Trans. Educ. **54**(1), 149–155 (2011)
28. Shirali-Shahreza, S., Ganjali, Y.: FleXam: flexible sampling extension for monitoring and security applications in openow. In: ACM SIGCOMM HotSDN'13 Workshop (2013)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.