Best Practices for the Security of Traffic Control Systems

By

Huipu Fan and Ming Yu

Department of Electrical and Computer Engineering
Florida State University

EXECUTIVE SUMMARY

Due to coordinated effort among the FSU electrical engineering research team and key FDOT personnel, an investigation of the traffic control network security issues have been reported.

The report consists of the following:

Current security issues in the existing ASCs
Possible attacks against traffic control networks
Configuration of the attacks against the traffic control networks
Defense techniques for the traffic control networks

This report mainly addresses the possible security issues in the traffic control networks. All the tests are conducted at FLDOT Traffic Engineering Research Lab (TERL).

Table of Contents

List of Figures

I. Introduction

I.1. Background

In the Traffic Engineering Research Lab (TERL) of the FLDOT, we define a traffic control network as a LAN or wireless LAN that connects a collection of traffic devices. The basic components in the network are the control console that is used to set traffic devices' parameters, Actuated Signal Controller (ASC) or Actuated Traffic Controller (ATC) that is used to send and receive the commands between the ASC and other traffic devices, BIU (bus interface unit), MMU (malfunction unit) and other devices, etc. The ASC plays the key role in the traffic control network. It has been widely deployed at the traffic intersections across the states.

Recently security issues have gained great interests among the researchers in the traffic engineering industry. Particularly, there is insufficient research on the security issues of the communication link that goes between the control console and the ASC. In our research, we mainly concern the security issues against the traffic control network, especially in the viewpoint of network security. Usually, the hardware and software of the ASC are blocked to the normal users of the ASC, even if just using a simple login and password. In this situation, we can investigate the possible attacks, i.e., those against the traffic control network. In this investigation, we demonstrate that the traffic control network is vulnerable to the network attacks. Disaster may happen if the network has being attacked. We also discuss the defense techniques to protect the network.

The simple network management protocol (SNMP) is widely deployed in traffic control network. It manages the communication between a management station (e.g., the control console) and a managed device (e.g., ASC). The database of a managed device is called management information database (MIB). All the traffic object identifier (OID) and status are stored in the MIB. For instance, OID 1.3.1.1.2.1.1.1.0 points to the system information of the ASC. The communication is realized by SNMP GET/SET commands:

the control console can manage all the traffic parameters/values of the device (e.g., ASC) through the commands sent to the ASC via a LAN or wireless LAN.

The SNMP can be easily implemented and is compatible with most traffic control devices. It complies with the National Transportation Communications for ITS Protocol (NTCIP). However, the SNMP version 1 (or simply SNMPv1) does not have any security feature: the SNMP commands within a traffic control network are exposed to other traffic. The SNMPv1 does not have authentication function. If a malicious node breaks into the communication between the control console and ASC, the device MIB can be manipulated and thus can cause serious damages to the traffic systems controlled by the ASC. To implement a security solution in the ASC, we must get the permissions from the vendors of the ASC. For example, to implement SNMP version 3 (or simply SNMPv3), we must work with the vendors that build the ASC.

In this report, we identify the major attacks against the traffic control networks and investigate the possible solutions to defend the attacks. In Section II, related work will be summarized. In Section III, major attack scenarios are discussed. In Section IV, we investigate the configuration of the attack scenarios, or the possible scenarios in which the attacks can be launched to the traffic control network. We also study the possible defense technique. In Section V, we present our best practices to avoid the attacks and conclude our report.

I.2. Research Objectives and Supporting Tasks

The main objective of this project is to investigate the possible security issues against the traffic control network and defense techniques.

To achieve this objective, the following tasks are anticipated:

- Research and review of past efforts applicable to this project

- Research, review, and selection of existing commercial-off-the-shelf (COTS) products required for this project
- System requirements development
- System design and design reviews
- System implementation
- System testing and validation
- Implementation of production test environment
- Documentation

II. Literature Review

Typically, in a local traffic control network, the ASC firstly receives commands from the control console via SNMP protocol, and then broadcasts these commands to two types of traffic devices via SDLC (Synchronous Data Link Control) protocol. These devices include MMU and BIUs. The ASC plays a critical role in the traffic control network. However, since the existing ASC does not have sufficient security features, serious damages may occur if the network has being attacked.

For example, an attacker may break into the communication between the ASC and the control console. On one hand, he (or she) may launch a denial-of-service (DoS) attack to the ASC. On the other hand, an attacker may pretend he is the ASC, and thus sends fake SDLC commands to the MMU and BIUs. Accordingly, the MMU and BIUs will follow these fake commands to disrupt the traffic service since there is no authentication implemented in the network.

In this report we investigate what are the possible attacks to the existing ASCs.

We investigate the major ASC models, including: Econolite ASC/3, Siemens M-50 series, MaCain eX NEMA, Peek ATC 1000, Intelight 2070 LDX, and Trafficware ATC 2070 [1]-[6]. Currently, none of these models are provided with sufficient security solutions to the attacks against the ASCs (Appendix A).

- For the ASCs of Siemens M-50 series and Intelight 2070 LDX, the length of the SNMP command packet sent from these ASCs is 2 bytes. However, the NTCIP requires that the command packet length must be 4 bytes. First, if the packet length is shorter than 4 bytes, the ASC is not NTCIP compatible. Second, it is easier for an attacker to understand the meaning of the packets and thus may be able to attack the ASC.

- As to the Econolite ASC/3 series, the ASC has log in/off function on its control panel. However, the setup process is not clear for an operator to implement this function. Furthermore, even with the protection of a log in/off function, the ASCs can still be easily attacked by a network attacker.
- For Trafficware ATC 2070 and MaCain eX NEMA, the ASC has a USB 2.0 port. Since there is no authentication function, anyone with a flash drive can download and upload data from this ASC by using the USB port. Thereby, he or she may launch an eavesdrop attack easily.
- For the above six major ASC models, the most important security implementation is a cabinet lock. Even with a lock, the attacker can easily break into the cabinet and then modify the ASC's parameter values.

In summary, all of these major vendors of ASC have not implemented sufficient security features in their ASCs. They choose SNMPv1 to manage the traffic devices. The SNMPv1 does not have data encryption/decryption and authentication functions. Without these two critical security functions, the ASCs can be easily attacked by many network attacks, such as Deny-of-Service (DoS) attack, Men-in-the-Middle (MitM) attack, VLAN hopping attack, and other wireless network attacks.

- The DoS attack can block an ASC to its controlled traffic devices. Since the ASC does not provide authentication function, the ASC will response to all the requests it receives. Once the attack has been launched successfully, the ASC will become unreachable from other devices in the traffic control network.

- In the MitM attack, the packets going between the ASC and the control console are not encrypted. Once the attacker obtains the packets, he or she can understand the meaning of the packets directly. Then, he can modify the packets, and finally sends the bogus packets to the ASC. In this way, the communications between the

ASC and its controlled devices become completely unsecure. The devices can be manipulated to disrupt the traffic.

- In the VLAN hoping attack, there is not enough security feature implemented on the switch in the traffic control network. The attacker can easily change the switch mode; obtain the authority to access the communication that is denied to him. Once the attacker breaks into the ASC's VLAN, he may launch a DoS attack or MitM attack to the ASC.

- In the wireless attacks, the wireless communications are susceptible to all types of security attacks. Although the wireless communication capability has not been provided by many ASCs and the traffic devices, it is becoming popular in the near future. For example, as one of the largest ASC vendors, Econolite has implemented a few wireless devices in their latest model Econolite Cobalt. In a wireless attack against the traffic control network, the attacker can launch an attack based on the vulnerability of the IEEE 802.11 WAP2 protocol. The attacker can crack the password of the traffic control network by using special attacking software, such as Aircrack-NG. Once the attacker obtains the password of the wireless network, he may launch some LAN attacks to the ASC more effectively.

Due to the lack of security in their implementations, the ASCs have been attacked many times across the states. Some serious damages to the city traffic devices have been reported.

- In 2009, a fired engineer hacked into the traffic control center in Los Angeles. He reprogrammed the red light time and made it longer. Although the local police caught him shortly, the longer red light still caused a lot troubles for the city's traffic. If the authentication is implemented, such problems cannot happen.

Recently, wireless technique becomes more and more popular in traffic device industry [15-17]. Many wireless devices have been deployed in traffic engineering.

- In 2008, an Ebay seller sold universal remotes for traffic control [22]. Although he was caught by the police shortly, the wireless devices are still in risk of damage if not sufficient security features have been implemented in the traffic control systems.
- A website called 'Hack a day' sells traffic Wi-Fi devices to the public. The Wi-Fi devices can change the traffic light remotely from a traffic intersection (around 10m distance). If the data encryption/decryption functions are implemented, such devices will not be able to attack the traffic light controllers.

Meanwhile, the NTCIP standards 1105 [7], 1202 [8], and 1210 [9] for the ASCs become widely accepted. Among the stands, the NTCIP 1202 and 1210 are the standards for the technique requirements on the ASCs. The NTCIP 1105 was designed for the security implementation. But it has been terminated in 2005 and no further action has been announced yet. However, few security concerns have been addressed in the other two standards (Appendix B). Currently, there are no topics in security have been mentioned in the NTCIP standards.

Furthermore, according to the *ITS Standards Program Strategic Plan for 2011-2014* [15], the *Action Plan and Legal Framework for the Deployment of Intelligent Transport System* in Europe [16], and *Best Practices in ITS Equipment Procurement Report* [17], the Ethernet and wireless networking technologies will be widely used in traffic control devices. The networking protocols will replace many old protocols such as SDLC, etc. in the near future. The vulnerability of the wireless communication requires us to search for possible security solutions in traffic engineering. Otherwise, serious damages may be caused to the traffic control networks by various attackers.

Therefore, it is extremely important for us to investigate the possible attacks against the ASCs. We must find the possible defense techniques in both device level and network level, which deal with the attackers by an individual device and by the traffic control network, respectively.

In the device level, one effective way to protect the traffic control devices is to adopt the new SNMP protocols for the communication between the ASCs and their controlled traffic devices. It is well-known that the SNMP v3 provides data encryption/decryption and authentication functions in device management. Therefore, the SNMMP v3 can be a good choice to secure the ASCs from the above attacks. For instance, the data encryption/decryption functions can be used to defense many attacks, such as MitM, VLAN hopping, and wireless attacks. The authentication function in SNMPv3 can be used to protect the ASCs from the DoS attacks. Once the device management protocol has been updated from SNMP v1 to SNMP v3, the attacks against the ASCs will be largely defended effectively.

This report mostly will investigate the security issues and solutions in the network level. More specifically, we will identify what are the typical scenarios in which possible attacks can be launched against the traffic control networks. Furthermore, we will configure the hardware and software to conduct experiments and demonstrate the possible attacks can be effectively launched in our testing environment. First, we will report the experiment configurations to test various possible attacks. If an attack scenario can be configured in our lab environment, then the attack will be a possible one in the traffic control networks deployed in the field. Then, we will report the testing results and validate that the possible attacks can be launched against the traffic control network. After that, we will summarize our recommendations to prevent the attacks in network level.

III. Areas of Work

In this section, we will report the seven typical scenarios, each corresponding to an attack to the traffic control network. They are:

- UDP flooding attack,
- Man-in-the-Middle attack,
- SYN flooding attack,
- VLAN hopping attack,
- Wireless MIB attack,
- WAP2-PSK attack, and
- WAP Jack-DNS attack

The experimental results will be reported in the next section.

III. 1: The UDP Flooding Attack

A UDP flooding attack can be easily deployed to attack the ASC (normally the ASC) without knowing the configuration of the traffic control network. It is a type of the DoS attacks that are usually hard to be defended and detected. We assume that initially an attacker installs a UDP flooding attack program in a malicious node (e.g., a network device) that is connected to the traffic control network, that is, the network can be accessed by the attacker. In our test-bed for the traffic control network, we assume that the attacker launches the attack from a malicious node. This node sends a large number of UDP packets to the ASC in order to disrupt the services of the ASC provided to its controlled devices. The ASC will become too busy to respond these meaningless UDP packets. It finally does not respond to the others legal devices on the traffic control network.

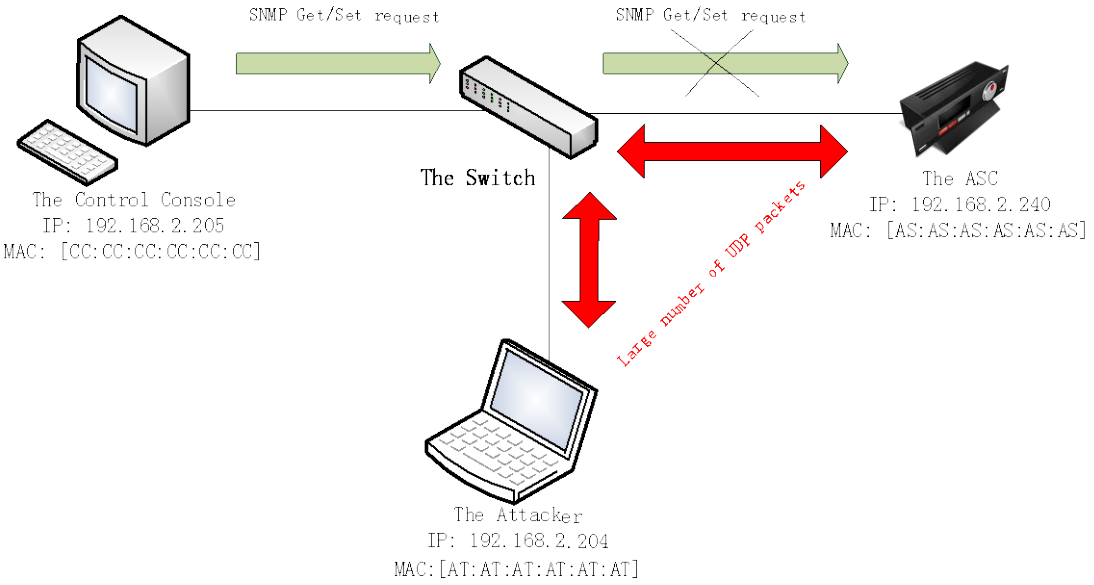


Figure 1: Illustration of the UDP flooding attack scenario.

Figure 1 illustrates an example of a UDP flooding attack against the ASC that is connected to the same network. We assume that the control console sends an SNMP

GET/SET command in the form of UDP packet. This packet goes to the ASC through the traffic control network. Meanwhile, the attacker controls a malicious node that is also located at the network. The malicious node keeps sending a large amount of meaningless UDP packets to the ASC. The ASC has to response to these UDP packets. It is thereby kept busy. During this time period, if there is another device sending a legal request to the ASC, the request will not be responded, i.e., the ASC becomes unreachable for the device on the traffic control network.

We define the following procedures to launch the UDP flooding attack:

1) The malicious node scans the entire traffic control network. It gathers the necessary system information (e.g., type of operating systems) of all the traffic control devices on the network.
2) The malicious node captures the packets coming from the ASC. It analyzes the packets in order to find the port number and IP address of the ASC.
3) The malicious node sends a large number of UDP packets to the ASC, after it finds the port number and IP address of the ASC.
4) The ASC keeps sending response packets to the malicious node, which keeps the ASC busy from responding to the legal requests. Therefore, it seems to the other devices on the network that the ASC is unreachable to the control console.

III. 2: The Man-in-the-Middle Attack

Recently, the Man-in-the-Middle (MitM) attack has gained more and more attention among the researchers. In a scenario of this type of attacks, a malicious node eavesdrops on the traffic control network. It modifies the SNMP packets between the control console and a victim ASC. The MitM attack can cause serious damage to a city's traffic control systems. For example, if an attacker that has hacked into a node locating on the traffic control network, he can implement the MitM attack on the malicious node. Then the SNMP packets are exposed to the attacker. Thus, he may be able to modify the traffic device’s parameter values. Usually, the attacker launches the MitM attack in a malicious node on the same traffic control network. In our test-bed in TERL, we assume that the attack can be implemented in certain node. Then, the node can capture the packets coming from other traffic devices. After analyzing the packets, the attacker is able to modify the packets and send it to the ASC.

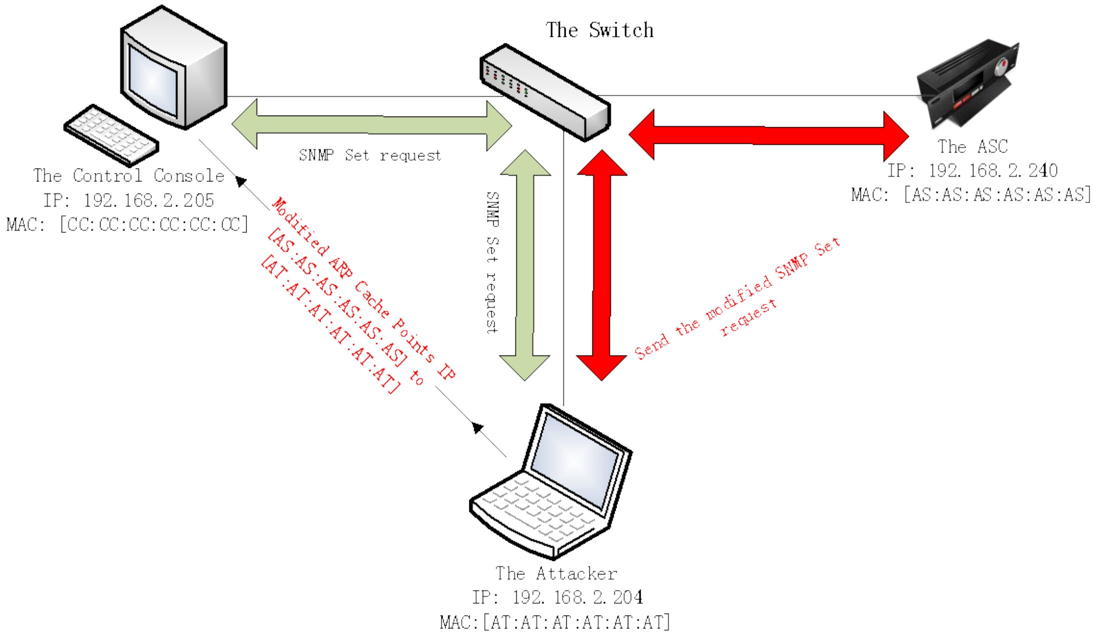


Figure 2: Illustration of the MitM attack: an attacker eavesdrops the packets in the traffic control network.

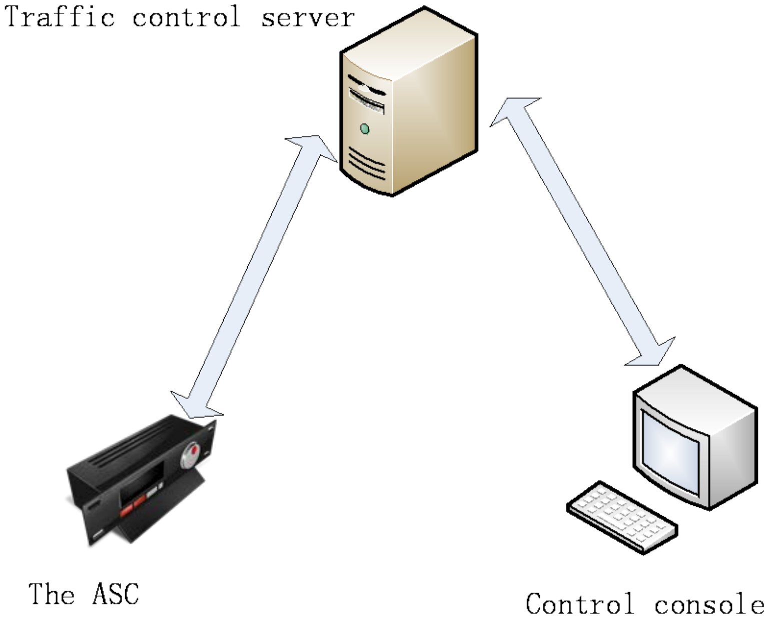
Figure 2 illustrates a MitM attack against the ASC. We assume that the control console sends an SNMP GET packet to the ASC through the traffic control network. The malicious node invades the communication between the control console and the ASC. It captures and modifies the packets coming from the control console to the other traffic devices (e.g., BIUs, ASC, etc.). The malicious node pretends to be the legal control console. It then sends the bogus packets to the ASC.

In order to launch a MitM attack, we define the following procedures:

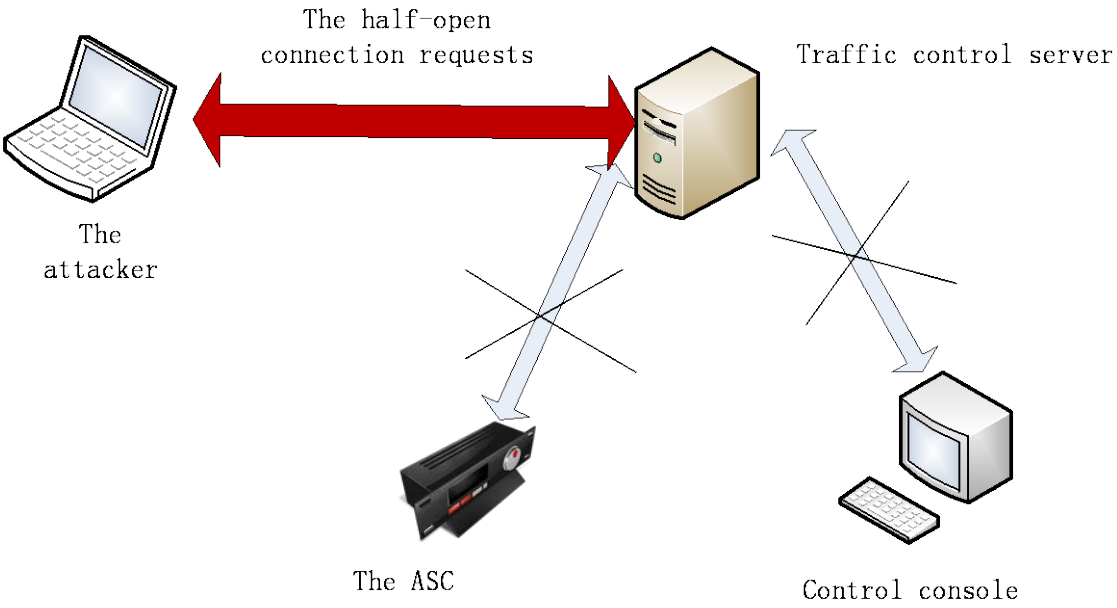
1) The malicious node scans the LAN. It then gathers the information of the control console and the ASC.
2) The malicious node sends ARP poisoning packets to the control console and the switch. By receiving these packets, the control console and the switch may think that the attacker is the ASC.
3) The malicious node captures and analyzes the packets that are sent from the control console to the ASC.
4) The malicious node modifies the captured packets. Then it sends the packets to the ASC.
5) The ASC receives the bogus packets and follows the false commands accordingly.

III. 3: The SYN Flooding Attack

A SYN flooding attack can be deployed outside the traffic control network. It is a type of DoS attacks that are hard to be defended and detected. Usually, the attacker installs a SYN flooding attack program in a malicious node outside the traffic control network. In our test-bed of the traffic control network, the attacker launches the attack from a malicious node that is outside the traffic control network. This node sends a large number of SYN packets to attack the server of the traffic control network. The server will become too busy to respond the meaningless half-connection SYN packets and finally not be able to respond to the others legal traffic devices in the traffic control network.



(a)



(b)

Figure 3: Illustration of a SYN flood attack.

Figure 3 illustrates an example of a SYN flooding attack against the server in the traffic control network. We assume that the control console sends an SNMP GET/SET command in a UDP packet. This packet goes to the ASC through the traffic control network. Meanwhile, the attacker controls a malicious node that is also located outside the network. The malicious node keeps sending a large amount of half-connection SYN packets to the server in the traffic control network. The server is forced to response to the packets and is thereby kept busy. During this time period, if other devices send legal requests to the server, these request will not be responded, i.e., the traffic control network becomes unreachable for the other devices.

We define the following procedures to launch a SYN flooding attack:

1) The malicious node scans the entire traffic control network and gathers the necessary system information (e.g., the type of server) of all the traffic control devices.

2) The malicious node captures the packets that come from the traffic control network. It then analyzes the packets in order to find the IP address of the server.

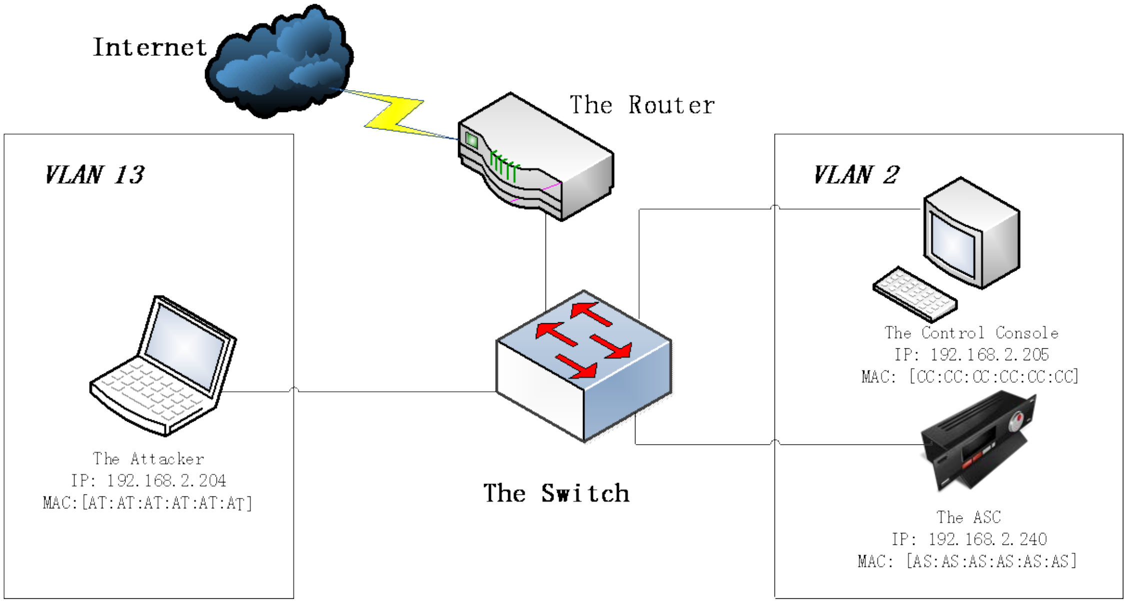
3) The malicious node sends a large number of half-connection SYN packets to the server.

4) The server keeps sending response packets to the malicious node, which keeps the server busy. This makes the network unreachable to the other traffic devices and control centers.

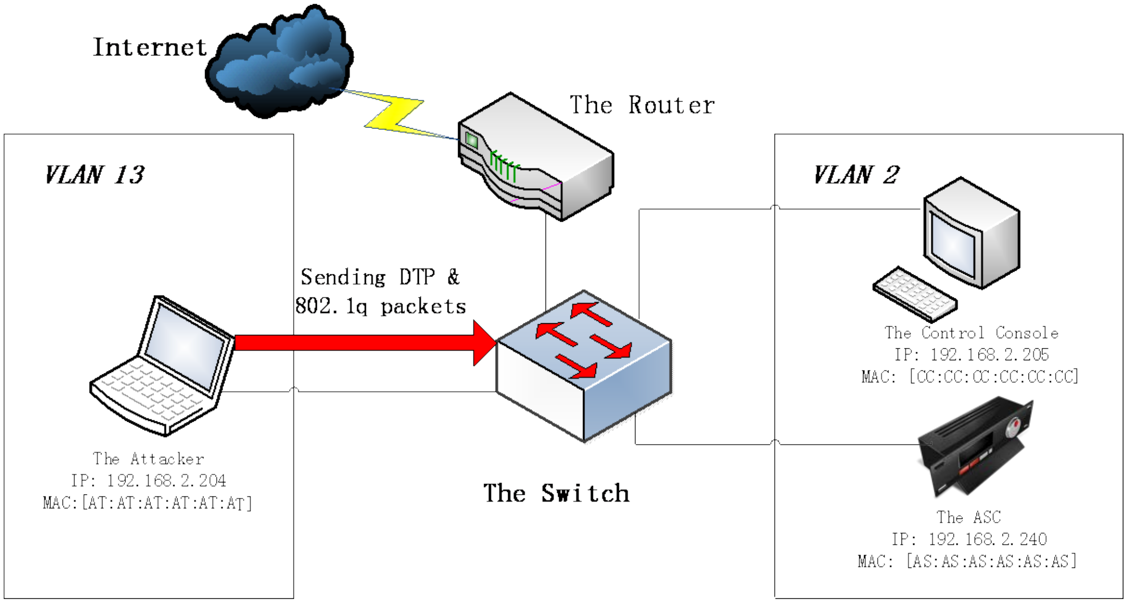
III. 4: The VLAN Hopping Attack

Virtual LAN (VLAN) has been widely deployed in traffic control networks to switch packets among several LANs. The VLANs can be configured in a VLAN switch by a traffic network administrator. All the communications among the VLANs go through the switch, which makes the communications not like the regular LANs. In addition, the major difference between a regular LAN and VLAN is that the regular LAN is a physical concept while the VLAN is a logical concept. From the network management point of view, the main advantage of VLAN is to classify traffic devices into different categories. For the VLAN test-bed in our traffic control network, the control devices are placed on VLAN 1. The ASC is placed on VLAN 2. The malicious node is placed on VLAN 3 and so on. The communication protocol of VLAN is on the data link layer (in the OSI model of seven layers). We implement the VLAN hopping attack against the ASC in our VLAN test-bed.

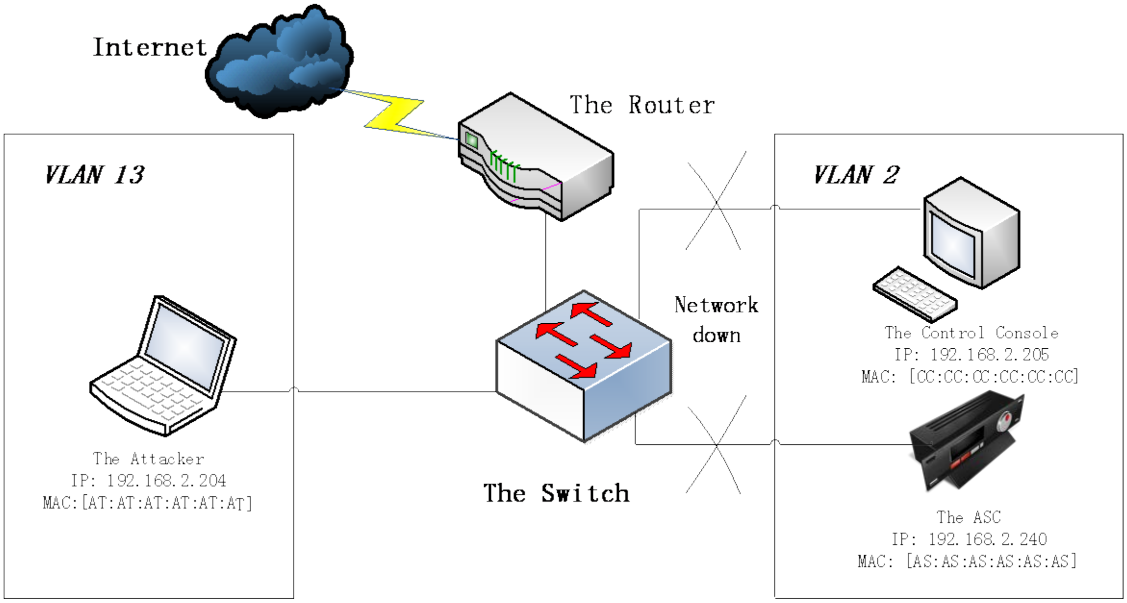
Usually, in a traffic control network, VLANs have different authority levels. For example, a control console has the authority to access and monitor the communications of all the other VLANs, while the ASC's VLAN can only communicate with the control console's VLAN, not others. However, if a VLAN hopping attack has been implemented in a malicious node, the attacker may obtain the authority to access and monitor other VLANs illegally. For a VLAN switch, according to the dynamic trunk protocol (DTP), there are five different modes: auto, trunk on, trunk off, desirable, and no negotiate. To implement a VLAN hopping attack, the attacker installs the attack software in a malicious node. The malicious node pretends to be a VLAN switch (highest authority) by sending false DTP packets to the victim VLANs. Once the attack is successful, the malicious node can obtain the highest authority. But the victim VLAN switch mode will be changed from "auto" to "trunk on". The "trunk on" mode means that this VLAN is totally open to others. Thus, the malicious node can launch a UDP flooding attack or a MitM attack to the ASC.



(a): Illustration of VLAN in TERL



(b) Step 1: Attacker sends DTP packets to the switch



(c) Step 2: VLAN 2 has been overloaded

Figure 4: Illustration of the attack.

Figure 4 illustrates the scenario of a VLAN hopping attack against the ASC. We deploy the control console and ASC on VLAN 2 while the malicious node on VLAN 13, respectively. The malicious node keeps sending false DTP packets to the switch and VLAN 2, which changes the switch mode to "trunk on". Then the malicious node obtains the authority to access VLAN 2. After that, the malicious node launches a UDP flooding or a MitM attack to the ASC.

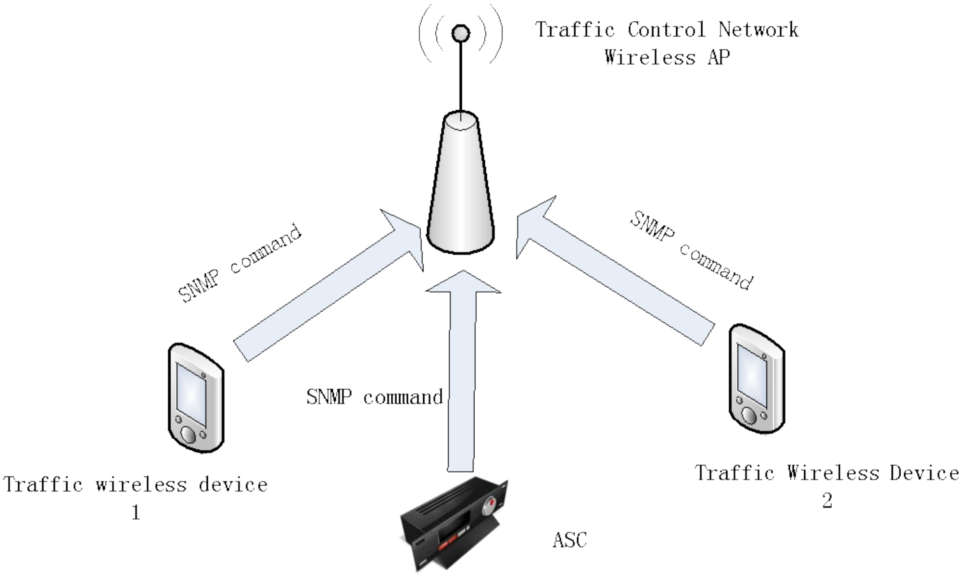
We define the following procedures to implement a VLAN hopping attack:

1) The malicious node scans all the VLANs and locates the VLAN of the ASC
2) The malicious node sends false DTP packets to the ASC VLAN and the switch
3) The switch of the ASC VLAN is forced to change its mode from "auto" to "trunk on"
4) The malicious node now obtains the authority to access and monitor the traffic inside the victim's VLAN

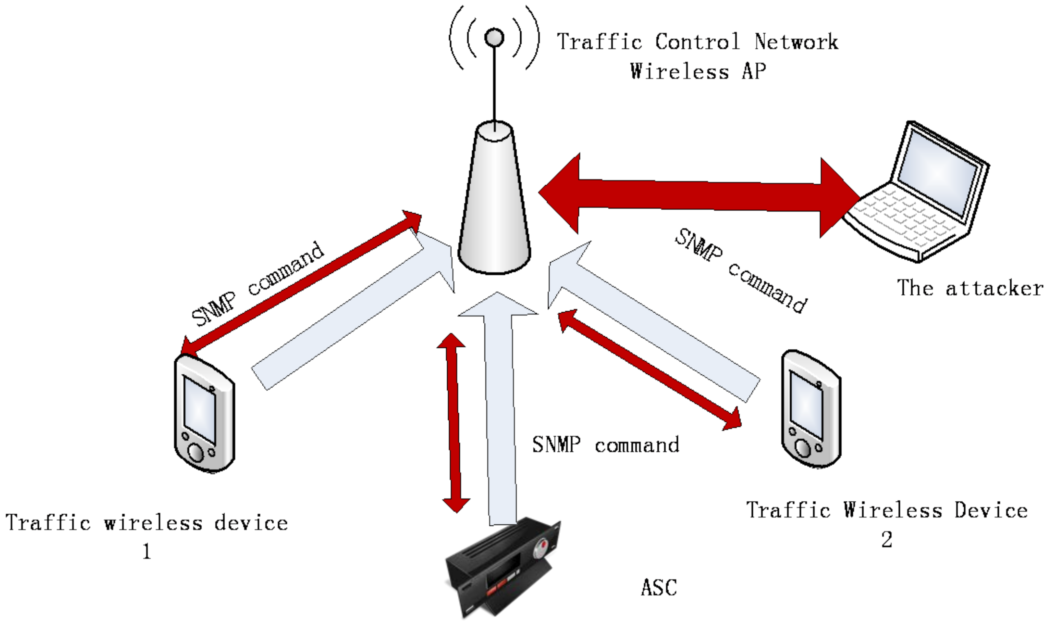
5) The malicious host launches a UDP flooding or a MITM attacks to the ASC

III. 5: The Wireless MIB Attack

As wireless devices start to be deployed in traffic control network, the attack against the SNMP MIB of the wireless devices, or simply the wireless MIB attack, becomes a popular attack among the ones against the traffic devices. In the scenario of this type of attacks, a malicious node eavesdrops on the wireless traffic control network. It modifies the SNMP packets sent from and to the victims ASCs. It can cause serious damage to the ASCs if the attack is launched successfully. Usually, the attacker launches the attack in a malicious node outside the wireless traffic control network. In our test-bed in TERL, we assume that the attack can be implemented in an external node. Then the node can capture the packets that come from the other traffic devices. After analyzing the packets, the attacker is able to manipulate the packets and sent it back to the ASC.



(a)



(b)

Figure 5: Illustration of SNMP attack.

Figure 5 illustrates an example of the wireless SNMP MIB attack against the ASC in the traffic control network. We assume that the control console sends an SNMP GET packet to the ASC through the traffic control network. The malicious node invades the communication between the control console and the ASC. It captures and manipulates the packets that come from the control console to other traffic devices, such as BIUs, ASC, etc. The malicious node pretends to be the legal control console, if the attack is successful. It then sends the bogus packets to the ASC and thus disrupts the service.

In order to launch this attack, we define the following procedures:

1) The malicious node scans the wireless network and gathers the information of the control console and the ASC.

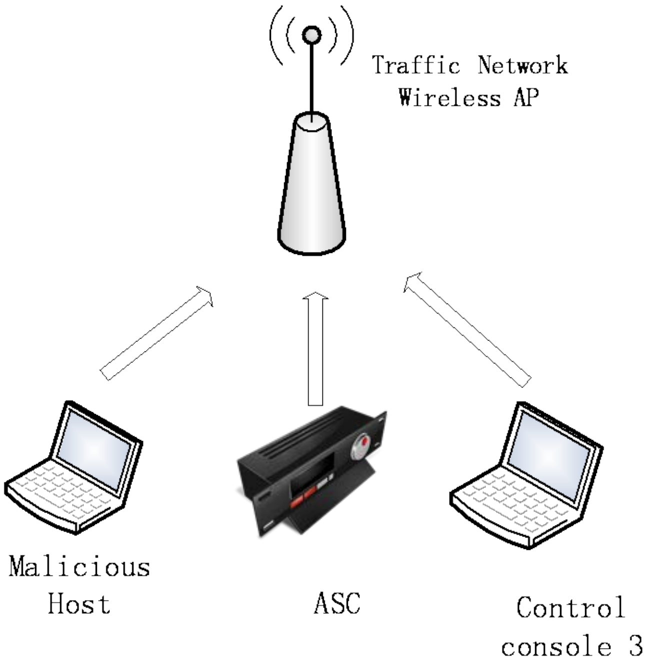
2) The malicious node uses the MIB attack software, such as Solar, to obtain the ASC MIB information.

3) The malicious node modifies the captured packets and then sends the modified packets to the ASC.

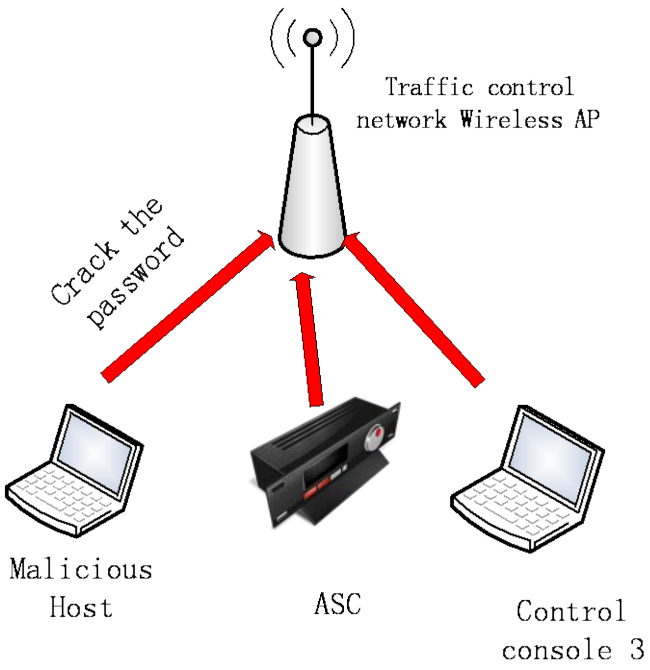
4) The ASC receives the bogus packets and follows the false commands accordingly.

III. 6: The WAP2-PSK Attack

A WAP2-PSK attack is a type of wireless network attacks that are usually hard to defend. Initially, the attacker installs a WAP2-PSK attack program in a malicious node that is connected to a wireless traffic control network. The attacker captures the communication between the control console and the ASC. It then analyzes the packets to crack the password of the wireless traffic control network. In our test-bed, the attacker launches the attack from a malicious node, which will crack the password of the wireless network. The communications among the traffic devices (e.g., ASCs, control consoles, and traffic sensors) will be exposed to the malicious node.



(a)



(b)

Figure 6: Illustration of a WAP2-PSK attack: (a) network configuration (b) the attack scenario in the traffic control network

Figure 6 illustrates an example of a WAP2-PSK attack against the wireless traffic control network. We assume that the control console sends an SNMP GET/SET command in a UDP packet. This packet goes to the ASC through the wireless traffic control network. Meanwhile, the attacker controls a malicious node that is located outside the wireless network. The malicious node scans the wireless network. It then cracks the password to access the network. After that it breaks into the wireless network. Finally it implements a DoS attack to the ASC. The procedures are summarized as follows.

1) The malicious node scans all the nearby wireless networks
2) The malicious node locates the target traffic control network
3) The malicious node breaks into the target wireless network and takes control of the wireless switch
4) The malicious node launches a DoS attack to the ASC in the network

III. 7: The WAP Jack-DNS Attack

A WAP Jack-DNS attack is a type of wireless network attacks combined with the WAP2-PSK attack. After successfully launching a WAP2-PSK attack, the malicious node creates a fake server in the network. The ASC will visit the fake server, instead of legal one. By visiting the fake serve, the malicious node can record all the important information about the ASC. It then may modify the parameter values of the ASC or even launch a DoS attack to the ASC.

Figure 7 illustrates an example of the WAP Jack-DNS attack against the devices in a traffic control network. We assume that the control console sends an SNMP GET/SET command in a UDP packet. The packet goes to the ASC through the traffic control network. Meanwhile, the attacker controls a malicious node that is located outside the wireless network. The malicious node cracks the password of the wireless traffic control network. It then breaks into the wireless network. After that, it reconfigures the wireless access point (AP), i.e., enters fake DNS information to the router. Finally, the traffic devices in the network will be guided to visit the fake web server pointed by the DNS information.

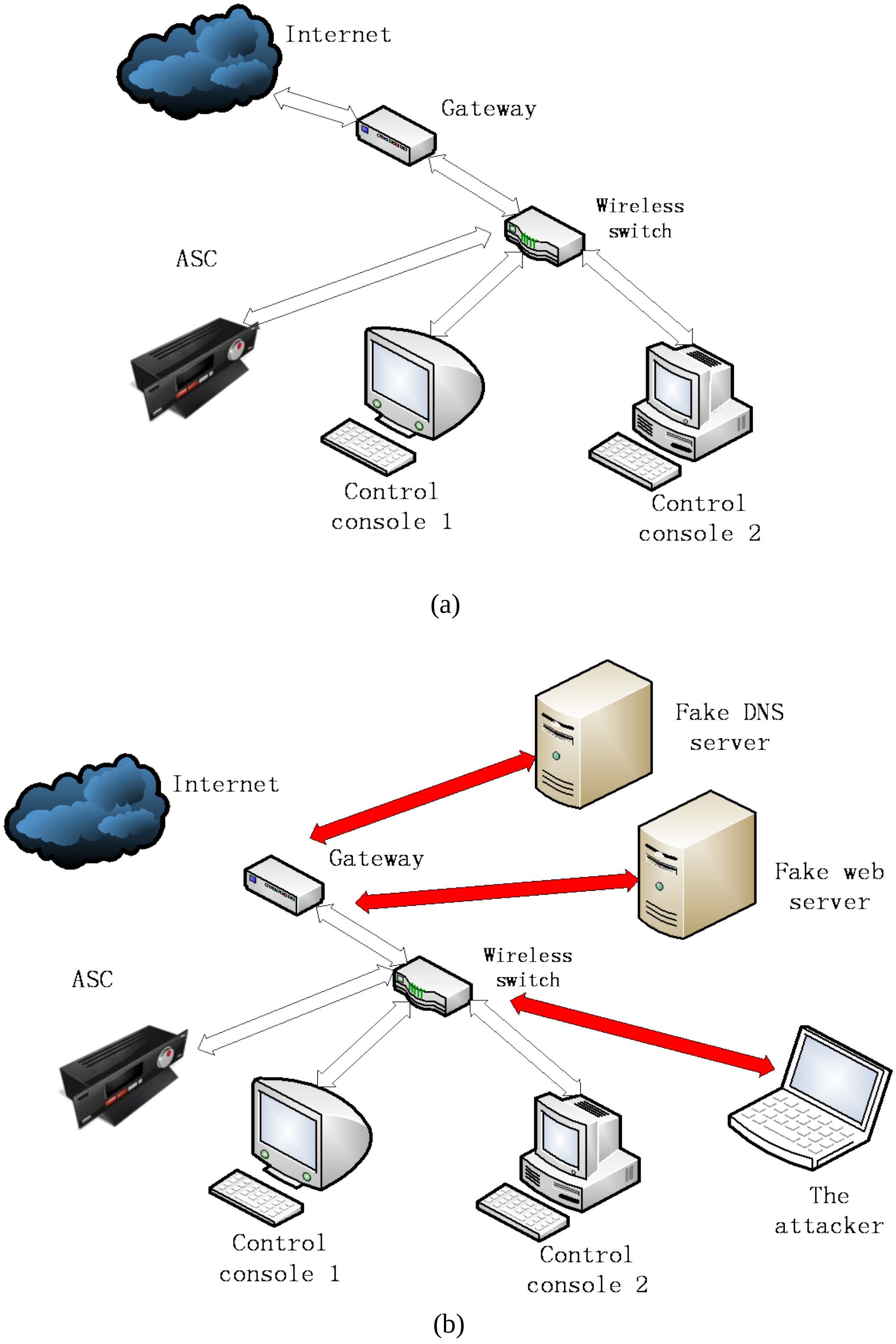
We define the following procedures to launch the attack:

1) The malicious node builds the fake DNS and a web server

2) The malicious node cracks the password of the target wireless traffic control network

3) The malicious node breaks into the target wireless network and takes control of the wireless router or access point

4) The malicious node sets up the fake DNS server in the wireless network



(a)

(b)

Figure 7: Illustration of the WAP Jack-DNS attack: (a) network configuration (b) the attack scenario in such a network.

IV. Experimental Results and Products

In this section, we conduct a series of experiments to validate the above attacks that can be launched successfully in a traffic control network with right configurations. In terms of the configurations in the previous section, we demonstrate that scenarios are possible attacks in real-work traffic control systems. We report the experimental results for each of the possible attacks.

IV.1: The UDP Flooding Attack

We configure a simulation of the UDP flooding attack in the test-bed. As shown in the figure, one laptop plays the role of control console. Meanwhile, another laptop simulates a malicious node. The operating system in the control console laptop is Windows 7. The laptop is loaded with the NTCIP compatible SNMP GET/SET program. The malicious node is loaded with Ubuntu operating system. The attack software has been also installed in the node, including *Nmap*, *UDP flooding program*, and *Wireshark*, which are publically available for free downloading. For the ASC, we choose the Econolite model 3/2100 since it has been widely deployed in the traffic intersections across the states. The test-bed is NTCIP compatible.

In the traffic control network, both the control console and ASC use the SNMP protocol to communicate with each other. We configure the control console with port number 161/501 and IP address 192.168.2.202, respectively. The malicious node that simulates the attacker is given the IP address of 192.168.2.203. For the Econolite ASC 3/2100, we assign the IP address of 192.168.2.204 and port number 501, respectively.

Initially, we assume that the malicious node does not have the basic information (i.e., operating system) of the traffic control system. To launch a UDP flooding attack, the malicious node uses Wireshark (e.g., network sniffer software) to sniff the packets within the traffic control network. Then, with the assistance of the sniffer software, the malicious node captures some of the SNMP packets sent between the control console and ASC. Finally, the malicious node uses Wireshark to analyze these packets. It finds out the IP address and port number of the control console and ASC, respectively.

Meanwhile, the malicious node scans the entire traffic control network by using Nmap, i.e., network scanner software. With the assistance of the Nmap, the malicious node now can obtain the system information of all the nodes in the network. From the information, the malicious node now can locate the ASC. This is feasible because the ASC normally is loaded with Linux operating system, which supports the network sniffing and scanning software.

In order to configure the UDP flooding attack, the attacker needs to configure the UDP packets. The destination IP address and port number are put into the header of the UDP packet, along with the ACK, sequence number, checksum, and reserved bits, etc. The size of the UDP packet is 256 bytes.

Scenario 1 has been set up to test the effectiveness of the UDP flooding attack. In this scenario, the malicious node sends 200, 300, 400 and 450 UDP packets per second to the ASC, respectively. The scenario has been repeated 10 times. We choose the average of the packet loss ratio over the 10 times to analyze the attack.

As shown in Figure 8, it can be seen that the average packet loss ratio increases as the UDP flooding speed increases. When the UDP attack speed passes 300 packets/s, no SNMP packet can reach the ASC. It shows that the ASC finally becomes isolated from the control console, i.e., the UDP flooding attack is successful.

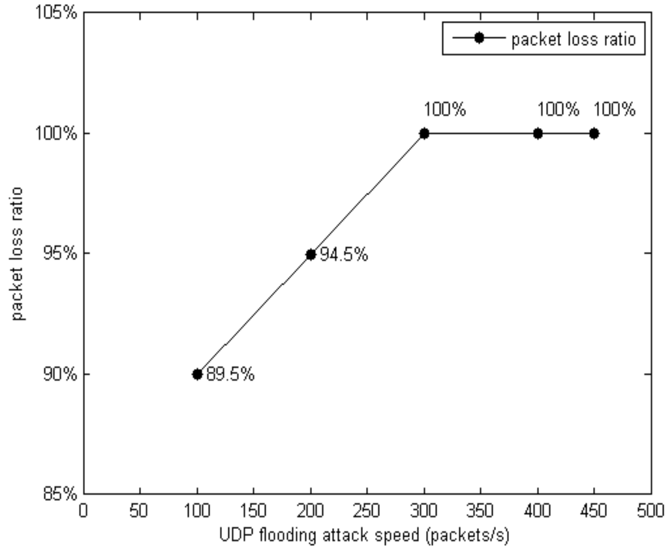


Figure 8: The SNMP packet loss ratio caused by the UDP flooding attack.

To protect the traffic control network from the UDP flooding attack, we suggest that there should be a firewall to be added to the traffic control network, for the following reasons:

1) The firewall can stop all the packets from an unauthorized node. For instance, we can set up a white list in the control center. This list maintains the IP addresses of all the trusted nodes. The packets other than from these trusted nodes will be ignored automatically. In this way, the malicious node cannot reach the control console.

2) The firewall can be easily implemented. Considering the restriction on the blocked ASC, we can implement the firewall in the control console. The firewall can be configured with a few steps.

3) The firewall can be easily maintained. It is a mature defense technique widely used in security industry. Most operating systems are installed with the firewall software.

IV.2: The MitM Attack

In our test-bed, we use two laptop computers and an ASC to simulate the MitM attack. One laptop works as the control console. The other represents a malicious node in the traffic control network. The operating system of the control console is Windows 7, which is popular choice for the traffic control consoles. The malicious node uses Ubuntu as the operating system. It has been installed with the attack software, including *Ettercap*, *Nmap*, *Wireshark*, and *MitM program*. For the ASC, again, we choose the Econolite ASC of model 3/2100.

In the traffic control network, both the control console and ASC use the SNMP v1 protocol to communicate with each other. The port number and IP address of the control console are configured as 501 and 192.168.2.205, respectively. We assign the IP address of 192.168.2.206 to the malicious node that simulates the attacker. For the Econolite ASC of model 3/2100, we assign it with the IP address of 192.168.2.207 and port number 501, respectively.

We assume that the malicious node has no knowledge about the traffic control network. After the communication starts, the malicious node sniffs the network with Ettercap (e.g., network sniff/attack software). The Ettercap will return a list of hosts in the traffic control network. On this list, the IP addresses will be shown. Then, the malicious node scans these hosts by using Nmap to obtain the system information (e.g., OS) of the corresponding devices. Once obtaining the OS of the devices, the malicious node can figure out the IP address of the ASC. This is usually the case in practice. The ASC usually uses Linux OS while the control console uses Windows OS.

In our first scenario, the malicious node launches the MitM attack after gathering all the necessary information. First, it sends ARP poisoning packets to the control console. Usually, each node in the traffic control network maintains an ARP table. The main function of the table is to resolve the mapping from destination IP address to the MAC address of a node in the network. Once the ARP poisoning packets are received, the control console is forced to update the ARP table. Then, the ASC's IP address and MAC address are replaced by those of the malicious node. Finally, the malicious node successfully fools the control console. In this way, all the packets that come from the control console will go to the malicious node, instead of the ASC.

Once the SNMP packets are received by the malicious node, the attacker starts to analyze the packets. Note that the SNMP v1 does not provide packet encryption/decryption function. Thus, the attacker can get the packet information directly. For instance, the console sends an SNMP set command "set OID 1.3.6.1.4.1.1206.1.2.1 to 20". If this packet is captured by the malicious node, the attacker can find the meaning of the packet directly without decryption.

After finding the meaning of the packet, the attacker can manipulate the packet field and resend the modified packet to the ASC. For the above instance, the attacker can first modify the SNMP set command from "set OID 1.3.6.1.4.1.1206.1.2.1 to 20" to "set OID 1.3.6.1.4.1.1206.1.2.1 to 200" and then resends the modified packet to the ASC.

Note that there is no authentication function implemented in the ASC. Therefore, the ASC will follow the commands it has received. At this point, the ASC has been taken over by the attacker and thus the attack is successful.

In our second scenario, we configure the test-bed to validate the effectiveness of the MITM attack performance. In this scenario, the control console sends 10, 20, 40, 60, and 80 SNMP commands per minute to the ASC, respectively. Meanwhile, the malicious node continuously sends ARP poisoning packets to the control console and the switch. We repeat the test for 10 times. We use the average of the packet loss ratio over the 10 times to analyze the effectiveness of the attack.

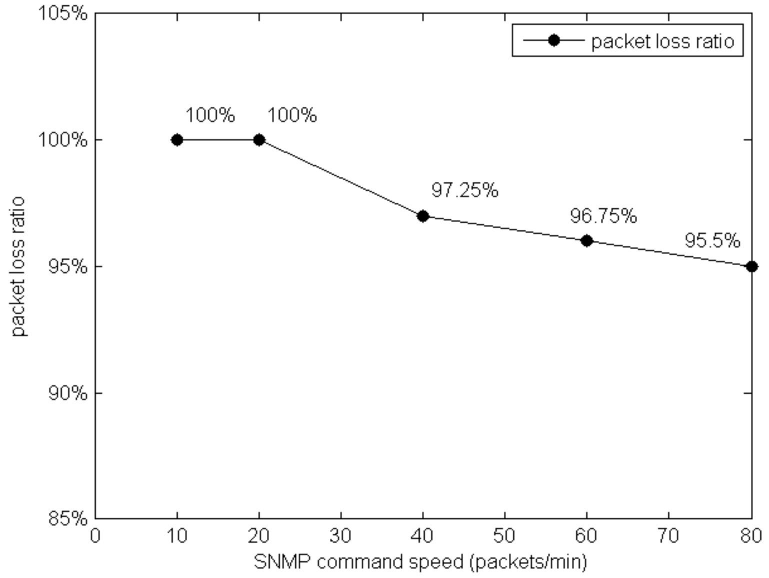


Figure 9: The packet loss ratio of the SNMP commands in the MitM attack scenarios.

Figure 9 shows that the SNMP commands can be completely lost due to the attack, i.e., the packets do not reach the intended ASC, if the sending speed is lower than some value. It also indicates that the packet loss ratio decreases while the sending speed of the control console increases. Once the control console’s sending speed exceeds 40 packets/min, the ASC receives some of the SNMP commands, which are still a small percentage, as compared to the total number of packets sent per minute. Clearly, the packet loss ratio is still too high: even at the speed of 80 packets per minute, only less than 4 packets per minute can be accepted by the ASC. Therefore, the control console can hardly reach the ASC in the traffic control network, or the MitM attack has been launched successfully.

To protect the traffic control network from the MitM attack, we suggest that the data encryption/decryption technique can be applied the packets exchanged in the traffic control network. First, all the packets that are received by the control console must be encrypted. Then, the console decrypts the packets with right key and security algorithms. Once correctly decrypting the packets, it sends the packets to the ASC. Since we cannot add the encryption/decryption function to the ASC, we suggest that the ASC should be configured only to communicate to the control console only. The added functions of data encryption and decryption can stop the attacker to obtain the meaning of the packets. In this way, the malicious node will not be able to send bogus packets to the ASC.

IV.3: The SYN Flooding Attack

We set up a SYN flooding attack in our test-bed to simulate the attack in real-world. One laptop plays the role of the control console. Meanwhile, another laptop simulates the malicious node. The operating system on the control console is Windows 7. The laptop is also loaded with the NTCIP compatible SNMP GET/SET program. The malicious node is loaded with Ubuntu operating system. The attack software installed in the malicious node includes Nmap and the SYN flooding program. For the ASC, we choose Econolite ASC 3/2100 since it has been widely deployed in the traffic intersections across the states. The test-bed is NTCIP compatible.

We configure a scenario to validate the SYN flooding attack. In the traffic control network, we set the control console's port number and IP address as 501 and 192.168.56.202, respectively. We give the IP address of 192.168.56.101 to the malicious node that simulates the attacker. For the Econolite ASC 3/2100, the IP address of 192.168.56.204 and port number 501 are assigned to it, respectively.

Initially, the malicious node scans the entire traffic control network by using the network scanner software (Nmap). With the assistance of Nmap, the malicious node now can obtain the system information of the nodes in the network. From the obtained information, the malicious node can locate the ASC server. This is feasible because the server in the traffic control network is normally loaded with the operating system of windows server, which supports the attack software such as Nmap.

In order to launch the SYN flooding attack, the attacker needs to configure the SYN packets. The destination IP address is put into the header of the half-connection SYN packet, along with the ACK, sequence number, checksum, and reserved bits, etc. The size of the packet is 256 bytes.

The scenario has been configured to test the effectiveness of the SYN flooding attack. In this scenario, the malicious node sends 20000, 30000, 40000 and 50000 SYN packets per second to the traffic control server, respectively. This test has been repeated 10 times. We choose the average of the packet loss ratio over the 10 times to analyze the effectiveness of the attack.

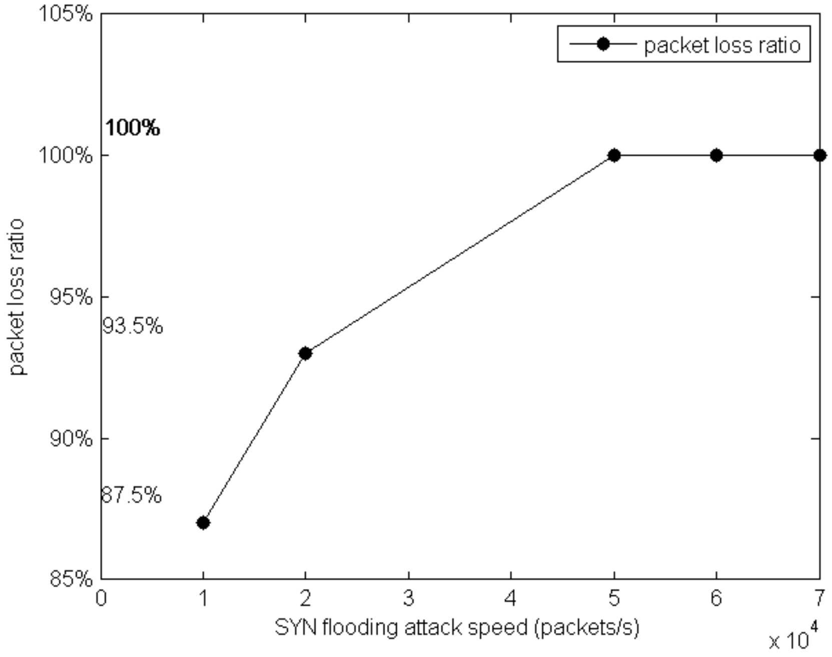


Figure 10: The packets loss ratio in the presence of the SYN flooding attack in the traffic control network.

As we can see from Figure 10, the packet loss ratio increases as the SYN flooding attack increases its sending speed. After the sending speed passes 50000 packets/s, all the SNMP packets are dropped and the packet loss ratio reaches 100%. It indicates that the ASC server finally become unreachable from the other devices in the traffic control network. The malicious node blocks the ASC server completely and thus the attack is launched successfully.

To protect the traffic control network from the SYN flooding attack, we suggest adding a firewall to the traffic control network. The firewall simply stops all the unknown packets from untrusted nodes. Therefore, the malicious node will not be able to block the ASC. In addition, the traffic control network should be blocked to other users except the designated control center. By doing so, we can reduce the risk that the traffic control network will be found by the attackers.

IV.4: The VLAN Hopping Attack

To implement a VLAN hopping attack in our test-bed, a laptop works as the control console is loaded with Windows 7 OS. The laptop and an Econolite 3/2100 ASC are deployed on VLAN 2. Another laptop that simulates a malicious node or attacker is loaded with the attack software, including *Yersinia*, *Nmap* and *Wireshark*. The node is placed on VLAN 13. All the VLANs in the traffic control network are set to mode "auto" that means they are not open to each other. The IP address 192.168.2.209 is assigned to the control console. The IP addresses 192.168.2.210 and 192.168.13.30 are assigned to the ASC and the attacker, respectively. Note that the attack software programs are publically available for free downloading over the Internet.

Initially, the malicious node has no knowledge about the VLAN configuration. So the malicious node scans the entire VLANs with IP address 192.168.xx.xx. Then, the sniffer software returns all the system information to the malicious node. With the assistance of the attack software, the malicious node can locate the VLAN of the ASC. After that, the malicious node sends false DTP packets to the target VLAN, which will force the VLAN switch to change the mode, i.e., from “auto” to “trunk on”. Finally the traffic in VLAN 2 is exposed to the malicious node. By accessing and monitoring the communications in the victim's VLAN, the malicious node can launch a UDP attack or a MitM attack to the ASC. For instance, once the malicious node can access the VLAN 2, it launches a MitM attack, in which it can change the minimum green time from 3s to 10s.

Also, the malicious node can launch a UDP flooding attack to the ASC to block the ASC’s communications with other traffic devices. There are two scenarios that have been tested in our test-bed. The first one is a VLAN hopping attack followed by a UDP flooding attack. The second one is a VLAN hopping attack followed by an MitM attack. Both scenarios can reuse the configurations in the previous attack scenarios.

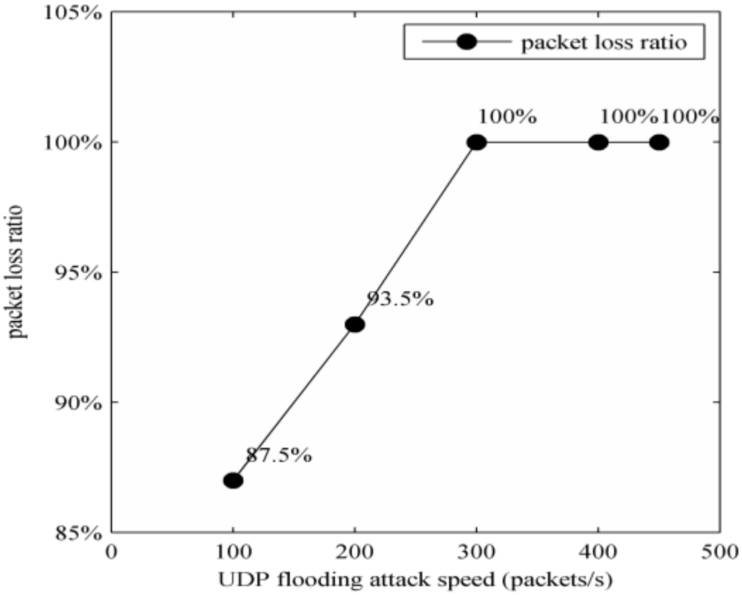


Figure 11: The packet loss ratio of the SNMP commands in our first scenario.

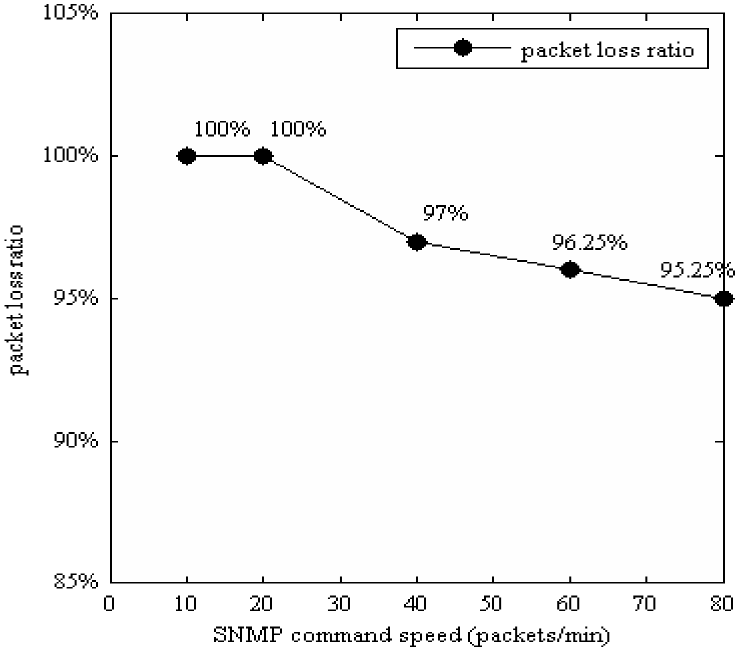


Figure 12: The packet loss ratio of the SNMP commands in our second scenario.

After successfully launching the VLAN hopping attack in our test-bed, we repeat the UDP flooding and MITM attack, respectively, as we did in launching the two single attacks in the previous scenarios. Figures 11 and 12 illustrate the effectiveness of the combined attacks. In the scenario corresponding to Figure 11, the ASC finally becomes blocked to other traffic devices due to the 100% packet loss ratio. In the scenario corresponding to Figure 12, the attacker fools the control console and sends bogus packets to the ASC. Only a very small percentage of packets can finally reach the ASC.

In order to defend the VLAN hopping attack in the traffic control network, we must implement effective defense techniques in the VLAN switch. We suggest using a guideline as a security solution before we can implement more sophisticated security solutions, including encryption/decryption and authentication.

To protect the traffic control network that is implemented in VLANs, we develop a guideline that can be used a best practice:

1) For the VLAN switch, login name and password should be changed regularly with complex password combinations of numbers, letters, and symbols.
2) For the switch, the port mode should never be set to "trunk on" mode.
3) For the switch, the switch port should not be configured as an access port.

IV.5: The SNMP MIB Attack

In our test-bed, we use two laptops and one ASC to simulate the wireless SNMP MIB attack. One laptop works as the control console and another one the malicious node or attacker. The operating system of the control console is Windows 7, which is a popular choice for the traffic control consoles. The malicious node chooses Ubuntu as the operating system. It has been installed with the attack software, including *Ettercap*, *Nmap*, *Wireshark*, and *Solar*. For the ASC, again, we choose the Econolite ASC 3/2100.

In the wireless traffic control network, both the control console and ASC use the SNMP v1 protocol to communicate with each other. We configure the control console's port number and IP address as 501 and 192.168.24.205, respectively. We assign the IP address of 192.168.24.206 to the malicious node that simulates the attacker. For the Econolite ASC 3/2100, we assign it with the IP address of 192.168.24.207 and port number 501, respectively.

We assume that the malicious node has no knowledge about the wireless traffic control network. After the communications start, the malicious node sniffs the wireless network with Ettercap (e.g., network sniff/attack software). The Ettercap software will return a list of hosts in the traffic control network. On this list, the IP addresses of the hosts will be shown. Then, the malicious node scans the hosts by using Nmap to obtain the system information of the devices. By obtaining the OS information of the devices, the malicious node can figure out the IP address of the ASC. This is usually the case in practice. The ASC usually chooses Linux while the control console chooses Windows operating system.

The malicious node launches the SNMP MIB attack after gathering all the necessary information from the network. First, it repeats the MitM attack procedures to attack the traffic device. Then, it uses the Solar MIB attack software to modify all the MIBs of the ASC. After that, the attacker can manipulate all the packets and resend the modified packets to the ASC. For instance, the attacker can modify the SNMP set command from "set OID 1.3.6.1.4.1.1206.1.2.1 to 20" to "set OID 1.3.6.1.4.1.1206.1.2.1 to 200" and the resend the modified command to the ASC.

Note that there is no authentication function that has been implemented in the ASC. Therefore, the ASC will follow all of the commands that it has received, i.e., the ASC has been taken over by the attacker. At this point, the attack to the ASC is successful.

We configure a scenario to test the effectiveness of the attack. In this scenario, the control console sends 10, 20, 40, 60, and 80 SNMP commands per minute to the ASC, respectively. Meanwhile, the malicious node continuously sends ARP poisoning packets to the control console and the VLAN switch. We repeat the test 10 times and use the average of the packet loss ratio over the 10 times to analyze the effectiveness of the attack.

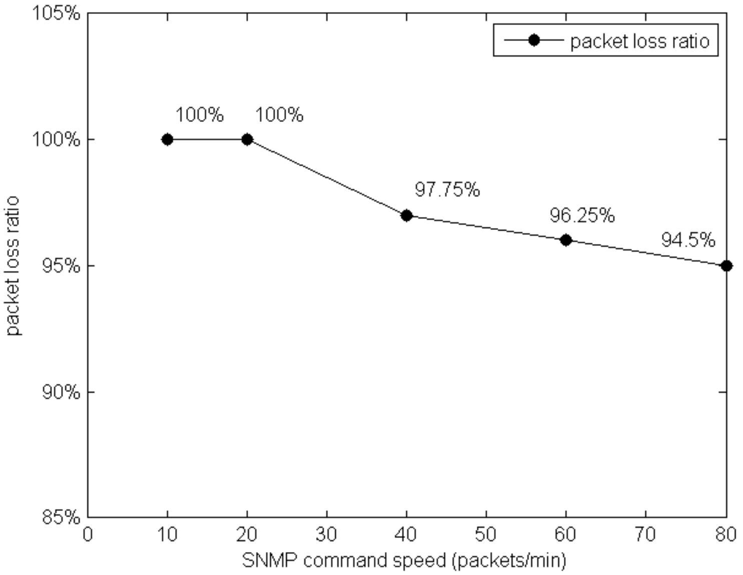


Figure 13: The packet loss ratio of the SNMP commands in the scenario of the SNMP MIB attack.

Figure 13 indicates that the packet loss ratio decreases while the control console increases its sending speed. Once the control console’s sending speed exceeds 60 packets/min, the ASC can receive a small number of the SNMP commands. However, the packet lost ratio is still too high for the SNMP commands to reach the ASC: even at the speed of 80 packets per minute, only 4 packets can reach the ASC. Therefore, the control console can hardly reach the ASC in the traffic control network. The SNMP MIB attack is launched successfully.

To defend the SNMP MIB attack against the traffic control network, we suggest introducing the data encryption techniques to the network, including encryption/decryption and authentication. Once equipped with the data encryption techniques, the malicious node will not be able to analyze the packets that go through the wireless traffic control network.

IV.6: The WAP2-PSK Attack

We simulate a WAP2-PSK attack in our test-bed in the lab. One laptop plays the role of control console. Meanwhile, another laptop simulates the malicious node or attacker. The operating system in the control console is Windows 7. The console is also loaded with the SNMP GET/SET program, which is NTCIP compatible. The malicious node is loaded with Ubuntu operating system. It has been installed with the attack software, including *Nmap*, *Aircrack-NG program*, and *Wireshark*. For the ASC, we choose Econolite ASC 3/2100 since it has been widely deployed in the traffic intersections across the states. The test-bed is NTCIP compatible.

In this scenario, we will launch a WAP2-PSK attack to the wireless traffic control network. The BSSID of our wireless network is 08:5D:4C:4C:A0:2A. We assign the IP address of 192.168.23.63 to the malicious node that simulates the attacker. For the Econolite ASC 3/2100, we assign it with the IP address of 192.168.23.204 and port number 501, respectively.

Initially, we assume that the malicious node does not have the basic information (i.e., operating system) about the traffic control system. To launch a WAP2-PSK attack, the malicious node uses the Wireshark (e.g., network sniffer software) to sniff the packets within the wireless traffic control network. Then, with the assistance of the sniffer software, the malicious node captures some of the SNMP packets between the control console and ASC. Finally, the malicious node uses the Wireshark to analyze the packets and get the IP address of the wireless network.

Meanwhile, the malicious node scans the entire wireless network by using wireless network attack software (e.g., Aircrack-NG). With the assistance of the software, the malicious node now can use the attack software to crack the password of the wireless network and thus gain the access to the network.

This scenario has been configured to test the effectiveness of the attack. In this scenario, the malicious node cracks the password of the wireless traffic control network. This scenario has been repeated 10 times. We choose different passwords with different secure levels to test the effectiveness of the attack.

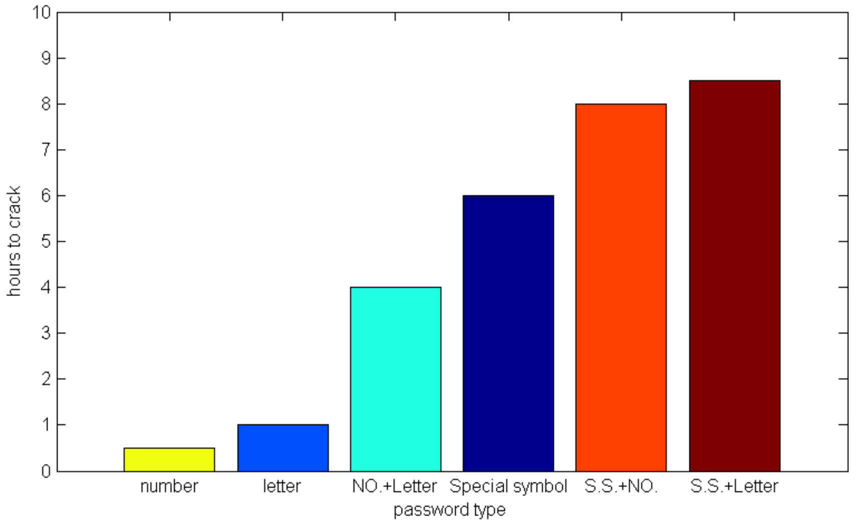


Figure 14: The average time to crack the password (in hours).

As shown in Figure 14, the average time to crack the password increases as the password increases its complexity. When the password has a special symbol, it takes the attacker 12 hours more to crack a password of 8 digits. It can be seen that the wireless traffic control network is finally cracked down after hours of computations. Therefore the WAP2-PSK attack is successful.

To protect the traffic control network from the WAP2-PSK attack, we suggest implementing the following practices.

1) We have to update the password frequently and periodically. By doing so, even if the attacker can finally obtains the password after hours of computations, it may become useless because the password has been updated already.

2) The wireless traffic control network must install a firewall and anti-virus software. The firewall and anti-virus software can stop most of malicious sniffers, so that the attacker will not be able to obtain the system information from the wireless traffic control network.

3) We must install monitoring software to monitor the wireless network behavior continuously. Once an unknown host appears in the network, it should be removed from the wireless network and prevented from further access immediately.

4) The configuration information of the wireless router must be kept safely. The router can be only configured by an authorized person. By doing so, we can stop the malicious nodes that try to modify the wireless router, in order to block their access to the communications between the control console and ASC.

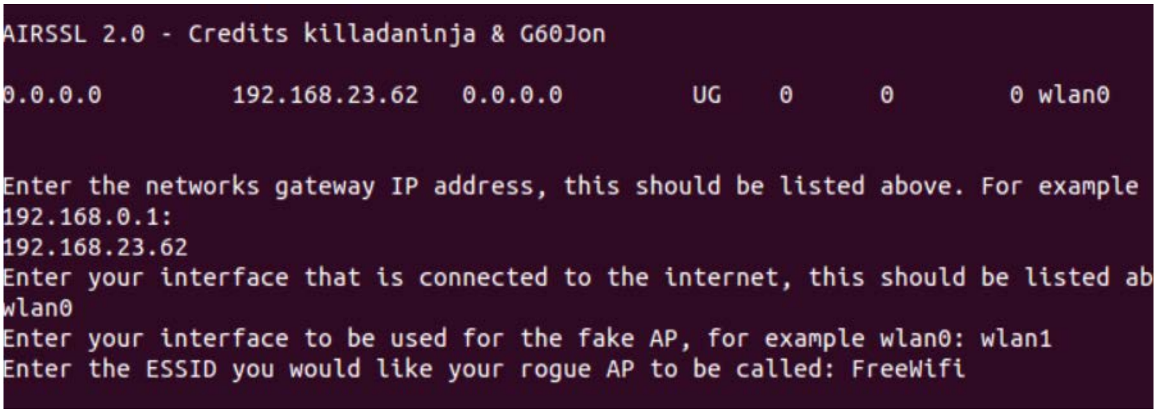
IV.7: The WAP Jack-DNS Attack

We simulate a WAP Jack-DNS attack in our test-bed in the lab environment. One laptop plays the role of control console. Meanwhile, another laptop simulates the malicious node or attacker. The operating system in the control console is Windows 7. The laptop is also loaded with the SNMP GET/SET program that is NTCIP compatible. The malicious node is loaded with Ubuntu operating system. It has been installed with the attack software, including *Nmap*, *Aircrack-NG program*, and *Wireshark*. For the ASC, we choose Econolite ASC 3/2100 since it has been widely deployed in traffic intersections across the states. The test-bed is NTCIP compatible.

In the wireless traffic control network, both the control console and ASC use the SNMP v1 protocol to communicate with each other. We configure the control console's port number and IP address to 161/501 and 192.168.23.202, respectively. We assign the IP address of 192.168.23.63 to the malicious node that simulates the attacker. For the Econolite ASC 3/2100, we assign it with the IP address of 192.168.23.204 and port number 501, respectively.

Initially, we assume that the malicious node does not have the basic information (i.e., operating system) of the traffic control system. To launch a WAP Jack-DNS attack, the malicious node uses the Wireshark (e.g., network sniffer software) to sniff the packets within the wireless traffic control network. Then, with the assistance of the sniffer software, the malicious node captures some of the SNMP packets between the control console and ASC. Finally, the malicious node uses the Wireshark to analyze the packets and find the IP address of the wireless network.

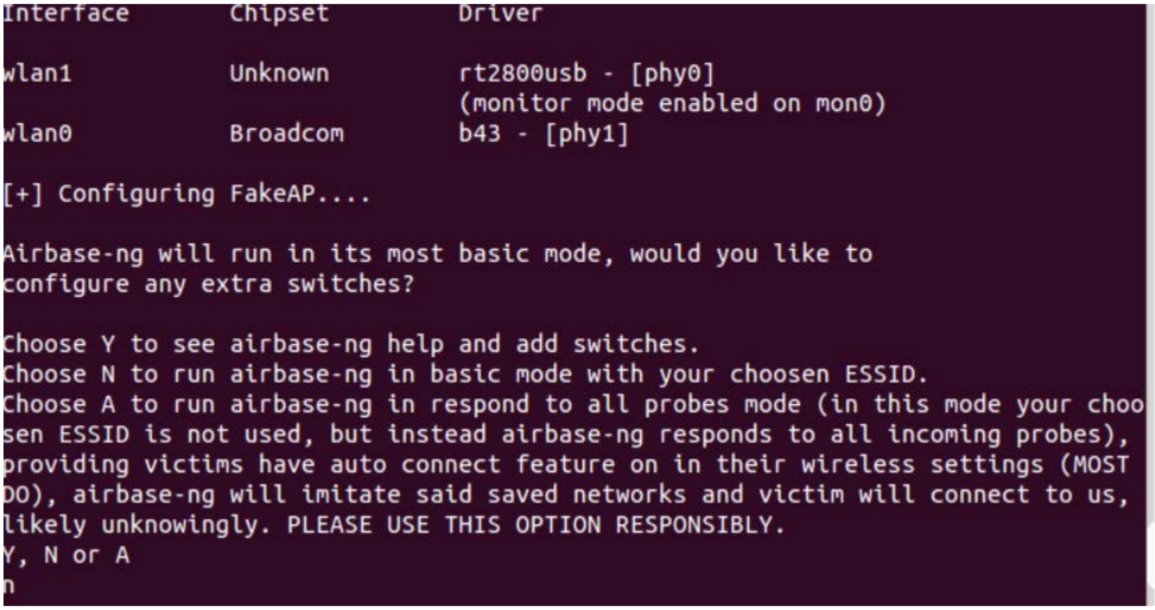
Meanwhile, the malicious node scans the entire wireless network by using the wireless network attack software (e.g., Aircrack-NG). With the assistance of the software, the malicious node now can obtain the system information of the nodes in the network. From the obtained information, the malicious node now can obtain the password of the wireless traffic control network.



```
AIRSSL 2.0 - Credits killadaninja & G60Jon

0.0.0.0         192.168.23.62   0.0.0.0         UG    0      0        0 wlan0


Enter the networks gateway IP address, this should be listed above. For example
192.168.0.1:
192.168.23.62
Enter your interface that is connected to the internet, this should be listed ab
wlan0
Enter your interface to be used for the fake AP, for example wlan0: wlan1
Enter the ESSID you would like your rogue AP to be called: FreeWifi
```



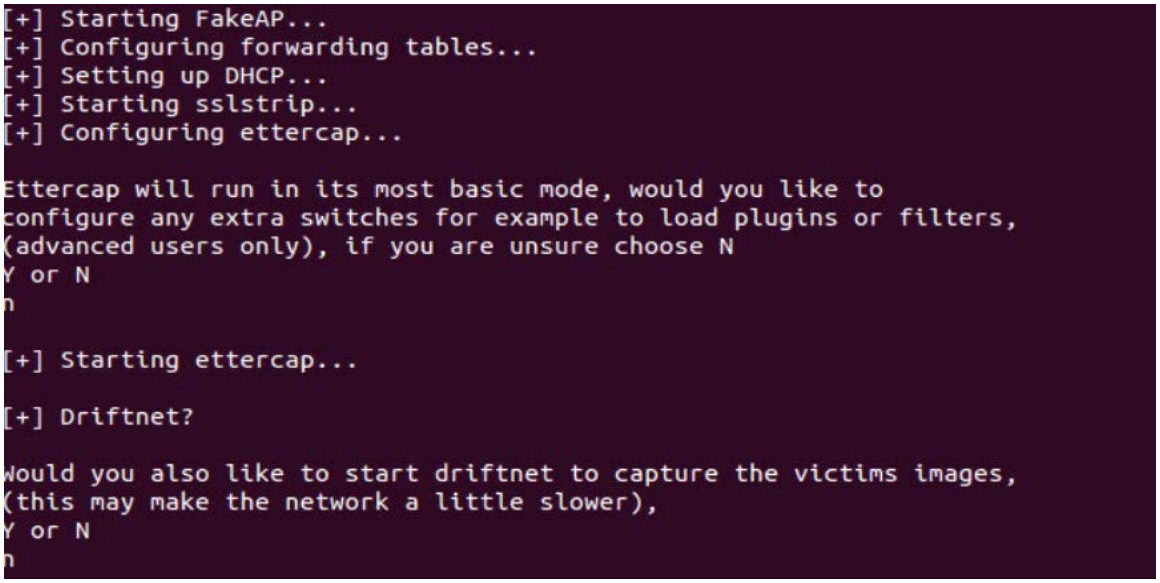
```
Interface       Chipset         Driver

wlan1           Unknown         rt2800usb - [phy0]
                                (monitor mode enabled on mon0)
wlan0           Broadcom        b43 - [phy1]

[+] Configuring FakeAP....

Airbase-ng will run in its most basic mode, would you like to
configure any extra switches?

Choose Y to see airbase-ng help and add switches.
Choose N to run airbase-ng in basic mode with your choosen ESSID.
Choose A to run airbase-ng in respond to all probes mode (in this mode your choo
sen ESSID is not used, but instead airbase-ng responds to all incoming probes),
providing victims have auto connect feature on in their wireless settings (MOST
DO), airbase-ng will imitate said saved networks and victim will connect to us,
likely unknowingly. PLEASE USE THIS OPTION RESPONSIBLY.
Y, N or A
n
```



```
[+] Starting FakeAP...
[+] Configuring forwarding tables...
[+] Setting up DHCP...
[+] Starting sslstrip...
[+] Configuring ettercap...

Ettercap will run in its most basic mode, would you like to
configure any extra switches for example to load plugins or filters,
(advanced users only), if you are unsure choose N
Y or N
n

[+] Starting ettercap...

[+] Driftnet?

Would you also like to start driftnet to capture the victims images,
(this may make the network a little slower),
Y or N
n
```

Figure 15: Screenshots of the WAP Jack-DNS attack.

In order to launch the WAPJack-DNS attack, the attacker needs to configure the Aircrack-NG parameter values. Figure 15 demonstrates how to set up the software. It also shows the attack results.

To protect the traffic control network from the WAPJack-DNS attacks, we can use the defense techniques that have been presented to defend the WAP2-PSK attack in the previous section. In addition, the network administrator should scan the traffic control network frequently and periodically to make sure that there is no fake server inside the traffic control network.

V. Conclusion

This report addresses the major attacks against the traffic control network within the framework of the NTCIP standards. After literature review and extensive experiments, we find that the major attacks against the control console and the ASC are the UDP flooding attack, MitM attack, VLAN hopping attack, SYN flooding attack, SNMP MIB attack, WAP2-PSK attack, and WAP Jack-DNS attack. Each of the attacks is experimented in our test-bed in a traffic control network. We have demonstrated that these attacks can cause serious damages to the traffic control system in the traffic control network.

There are several possible defense techniques that are proposed to protect the network, including encryption/decryption, authentication, and firewall, in addition to the SNMP v3 for device management.

As we pointed out, in the device level, one effective way to protect the traffic control devices is to adopt the new SNMP protocols for the communication between the ASCs and their controlled traffic devices. It is well-known that the SNMP v3 provides data encryption/decryption and authentication functions in device management. Therefore, the SNMMP v3 can be an effective choice to secure the ASCs from the above attacks, such as MitM, VLAN hopping, and wireless attacks. The authentication function in SNMPv3 can be used to protect the ASCs from the DoS attacks.

To protect the ASCs, we suggest the following guidelines to be implemented in practice.

1. The cabinet should be always locked; the key of the cabinet should be kept safely.
2. The login/off password of the ASC (e.g., Econolite ASC 3/2100) should be updated frequently. The password should contain symbols, number, and letters, instead of the default ones used by the device vendors.

3. Only authorized persons can configure the traffic control network. The network configuration should be kept in safe place that cannot be accessed by other persons without the authority level.
4. The switch/router should be maintained carefully. The network administrator should check the log periodically. Once any unusual log has been found, the network administrator should report it immediately.
5. The traffic control network should install firewall/anti-virus software. The software should be undated frequently.
6. The major vendors may consider undated the device management protocol from SNMP v1 to SNMP v3. Alternatively, the vendors should implement data encryption/decryption, authentication functions to their ASC.

In our future work, we will investigate more defense techniques for the traffic control network.

Reference:

[1] Econolite ASC/3 user manual. (n.d.). Retrived March 15th, 2014 from http://www.econolite.com/Products/controllers/asc-3.aspx

[2] Siemens M-50 series user manual. (n.d.). Retrived March 15th, 2014 from http://www.rgatraffic.com/pdf/siemens_controller_line_for_use_in_nema_style_cabinets_m50_series_traffic_controller.pdf

[3] MaCain eX NEMA user manual. (n.d.). Retrived March 15th, 2014 from http://controlspecialists.com/images/epacm50.pdf

[4] Peek ATC 1000 user manual. (n.d.). Retrived March 15th, 2014 from http://www.ustraffic.net/atc_1000.php

[5] Intelight 2070 LDX user manual. (n.d.). Retrived March 15th, 2014 from http://www.intelight-its.com/product/controllers/item/3-intelight-controller-model-2070l.html

[6] Trafficware ATC 2070 user manual. (n.d.). Retrived March 15th, 2014 from http://www.trafficware.com/wp-content/uploads/2013/08/ATC-Traffic-Controller.pdf

[7] Insignares, M. (2005). NTCIP CORBA Security Service Specification 1105.

[8] Ragsdale, P. (2007). NTCIP Object Definitions for ASC 1202 v02.

[9] Denney, R. (2010). NTCIP Object for Signal System Masters 1210.

[10] http://www.wired.com/science/discoveries/news/2005/08/68507

[11] http://latimesblogs.latimes.com/lanow/2009/12/engineers-who-hacked-in-la-traffic-signal-computers-jamming-traffic-sentenced.html

[12] http://articles.latimes.com/2007/jan/09/local/me-trafficlights9

[13] http://hackaday.com/2012/06/13/traffic-signal-controller-pulls-data-over-wifi/

[14] http://www.cyberwarzone.com/hack-traffic-lights-cisco-equipment-future

[15] U.S. Department of Transportation ITS Joint Program Office-HOIT. Intelligent Transportation Systems (ITS) Standards Program Strategic Plan for 2011 -- 2014.

[16] Directorate-General for Mobility and Transport. Intelligent transport systems in action : action plan and legal framework for the deployment of Intelligent Transport Systems (ITS) in Europe. 2013.

[17] U. of Missouri/MoDOT. Best Practices in ITS Equipment Procurement. 2013.

[18] SNMP Research International, Inc. SNMP research white paper. http://www.snmp.com/snmpv3/v3white.shtml

[19] Herrick, G. C. (1999). THE NTCIP GUIDE: NATIONAL TRANSPORTATION COMMUNICATIONS FOR ITS PROTOCOL (VERSION 2 DRAFT) (No. NTCIP 9001 v02. 05).

[20] ESET. Internet Security White Paper. http://www.eset.com/us/resource/papers/white-papers. 2013

[21] SNMP v3 website. https://www.ibr.cs.tu-bs.de/projects/snmpv3/

[22] http://www.drivers.com/article/651/

Appendix A

Major ASC Models and Security Features

Model	security related features
Econolite ASC/3	Enhanced transient and environment protection; protocol support for NTCIP; software can be easily downloaded via laptop; user programmable default database; log in/off; wireless maintain service; and Linux development environment.
Siemens M-50 series	Ethernet port; 8 MB flash memory; system can be updated; and following the NEMA standard.
MaCain eX NEMA	Compliant with NEMA and ATC standard; powerful CPU; multi-task ability; Linux platform; Ethernet port.
Peek ATC 1000	Meet the NEMA ATC standard; Linux operating system; and compliant NTCIP 1201, 1202
Intelight 2070 LDX	Configurable for NEMA TS-2; ITS serially interfaced cabinet applications in OS-9 operating system.
Trafficware ATC 2070	Meet the NEMA TS2 type 1 and type 2; USB 2.0 full speed port; shelf-mount configurations.

Appendix B

NTCIP Standards

NTCIP 1105 CORBA Security Service Specification [7].

Note: May 2005 -- the NTCIP C2C/C2F working group agreed to SUSPEND the work on this standard. There is no known plan for future use.

NTCIP 1202 Object Definitions for Actuated Traffic Signal Controller units [8].

Note: No security solution has been presented in this standard.

NTCIP 1210 Field Management Stations Object Definitions for Signal System Masters [9].

Note 2.6 This standard does not address any security issues. Any security pertaining to protecting the communications with a SSM should be implemented either physically by protecting the communications access points, or logically by enabling security features associated with the underlying communications protocols.

Appendix C

Traffic Attack Report

1. A hacker changed the red light time, caused traffic jam [10].

2. An engineer who hacked into L.A. traffic signal computer has been sentenced [11].

3 Two hacker hacked into traffic control system and caused traffic jam [12].

4 Tutorial for using wireless device to hack into a traffic control system[13].

5 Tutorial for hacking traffic lights with CISCO equipment in the future [14].