Journal of KIIT. Vol. 19, No. 6, pp. 99-107, Jun. 30, 2021. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.6.99

SDN기반 군용무인차량 내부네트워크 보안

김남곤*[1], 성기열*[2], 김도종*[3]

A Secure In-Vehicle Network of Military Unmanned Ground Vehicle based on SDN

Namgon Kim*[1], GiYeul Sung*[2], and DoJong Kim*[3]

요 약

최근의 군용무인차량들은 기존의 차량용 네트워크 기술의 한계를 극복하기 위해 내부네트워크를 이더넷 기반으로 구축하고 있다. 하지만, 이더넷은 쉽게 접근 가능하면서도 잘 알려진 기술이기 때문에, 차량이 다양한 보안위협에 노출될 수 있는 가능성이 높다. 이러한 보안위협을 차단하기 위해서는 권한이 없는 단말의 접근을 차단하고, 적절한 권한을 부여받은 단말간의 통신만을 허가하는 등의 대응방안이 필요하다. 이를 위해 본 논문에서는 중앙제어기의 응용소프트웨어에서 네트워크의 동작을 정의하는 SDN(Software-Defined Networking)기술을 활용하여 군용무인차량 내부네트워크 보안솔루션을 제안한다. 군용무인차량 운용에 필요한 단말들의 정보를 관리하고, 인가된 통신만을 허용하도록 함으로써 이더넷 환경에서 발생가능한 공격들을 별도의 방화벽을 도입하지 않고도 차단할 수 있음을 보인다.

Abstract

Modern in-vehicle networks of military UGVs(unmanned ground vehicles) are moving toward ethernet to overcome the limitations of legacy in-vehicle networking technologies. However, as the ethernet is well-known and widely-used, it is very likely to be exposed to security threats. To protect UGVs from the threats, a strong counterplan is required that could block access from unpreviledged endpoints and allow communications only between endpoints with proper access rights. In this paper, we propose an in-vehicle network security solution based on SDN(Software-Defined Networking) which defines networking based on software applications of a centralized network controller. We will show that it can block security attacks of in-vehicle ethernet networks without introducing additional firewalls by managing endpoints and allows connections approved for operating the UGV.

Keywords
unmanned ground vehicle, in-vehicle network security, automotive ethernet, software-defined networking

* 국방과학연구소 지상기술연구원(*[1]교신저자)
- ORCID[1]: http://orcid.org/0000-0002-1038-3768
- ORCID[2]: http://orcid.org/0000-0001-7777-8089
- ORCID[3]: http://orcid.org/0000-0002-4886-1403

· Received: Apr. 27, 2021, Revised: Jun. 18, 2021, Accepted: Jun. 21, 2021
· Corresponding Author: Namgon Kim
Unmanned Ground System PMO Team 1, Ground Technology Research Institue, Yuseong P.O.Box 35, Daejeon, 34186, Korea
Tel.: +82-42-821-0704, Email: namgonkim@add.re.kr

Ⅰ. 서 론

위험지역에서 군인을 대신해 감시정찰 및 물자수송 등의 임무를 수행하는 군용무인차량은 인명피해 없이 원하는 임무를 수행할 수 있다는 점에서 미래 국방력의 중요한 요소가 될 것으로 예상된다. 군용무인차량은 원격지의 통제차량과 무선통신으로 연결되어, 통제차량내에 위치한 운용자가 영상정보를 통해 전장상황을 확인할 수 있고, 운용자의 제어에 따라 전장을 이동하며 필요한 임무를 수행한다. 이를 위해 차량의 내부에는 다양한 임무장치들이 연결되는데, 최근의 군용무인차량들은 기존의 차량내부 네트워크 기술인 CAN, LIN, FlexRay 등에 비해 대역폭과 활용성이 높은 이더넷 기반으로 차량내부 네트워크를 구축하고 있다.

군용무인차량내부에서 이더넷을 사용하게 되면 기존의 차량용 표준 네트워크 기술에 비해 높은 대역폭을 제공하며, 차량 내부 시스템의 복잡도를 감소시켜 저비용으로 구축가능하다는 장점이 있다. 하지만, 이더넷은 현재 LAN(Local Area Network), WAN(Wide Area Network)등에 적용되어 상용으로 많이 활용되는 기술이기 때문에 기존에 알려져있는 이더넷의 취약점에 기반한 공격에 노출될 가능성이 높다. 또한, 차량내부 ECU(Electronic Control Unit)들은 자원이 제약된 임베디드 시스템들이 대부분이기 때문에 보안 설계가 미흡하여 불법 접근/권한상승, 펌웨어 변조, 위장 ECU 등을 통한 다양한 공격에 취약하다[1]. 특히, 군용차량이 이러한 공격으로 인해 내부네트워크가 공격자에게 노출된다면 큰 전력손실을 야기할 수 있다. 차량의 각 기능부에 대한 제어권을 공격자에게 빼앗겨 차량자체가 적의 제어하에 놓일 수 있으며, 해킹의 시작점으로 활용되어 중요한 작전정보가 노출될 수 있다.

본 논문에서는 차량용 이더넷을 활용하는 군용무인차량의 내부네트워크 보안을 위해 SDN(Software-Defined Networking)기반의 차량내부 네트워크 보안 솔루션을 제안한다. SDN은 정해진 프로토콜에 기반하여 동작하는 기존의 이더넷과 달리 중앙의 네트워크 제어시스템상 응용에 의해 네트워크 동작이 새롭게 정의되는 네트워킹 구조이다[2]. SDN을 구성하는 네트워크 스위치는 네트워크에 흘러다니는 패킷들에 대해서 직접 동작을 결정하지 않고, 제어기를 통해 정의된 동작만 수행한다. 따라서, 이러한 SDN의 특징을 활용하여 차량 내부 네트워크를 구성하게되면 약속되지 않은 트래픽이 유입되는 것을 근본적으로 차단할 수 있다. 이는 기존의 방화벽 기반 방식에 비해 네트워크 구성이 단순하며 ECU의 부담을 줄일 수 있다는 장점이 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 이더넷 환경에서의 보안이슈들과 차량용 이더넷 분야에서 도입되고 있는 대응방안들을 설명한다. 3장에서는 군용무인차량의 내부네트워킹 동작과 보안 요구사항을 설명하고, 4장에서는 SDN을 기반으로 한 군용무인차량 내부네트워크 보안 솔루션을 제안한다. 5장에서는 제안한 솔루션이 이더넷 환경의 보안이슈들에 대해 대응가능함을 실험을 통해 검증하고, 6장에서 결론 및 향후연구에 대해서 기술한다.

Ⅱ. 관련연구

2.1 이더넷의 보안 취약점들

이더넷은 현재 가장 널리 이용되는 기술이기 때문에 그 보안 취약점이 잘 알려져 있고, 이를 활용한 다양한 공격에 노출되기 쉽다. 이더넷은 브로드캐스트 방식을 통해 네트워크에 속한 모든 단말들이 서로를 발견하고 연결을 생성할 수 있는 구조이다. 이는 네트워크를 트래픽 기밀성 공격에 취약하게 만드는데, 만약 공격자가 네트워크 스위치의 비어있는 포트에 대한 물리적인 접근에 성공한다면 네트워크에 쉽게 참여할 수 있게 된다. 네트워크에 대한 접근권한을 갖게 된 공격자는 쉽게 네트워크 상에 메시지를 보내고, 그 응답을 분석함으로써 단말들의 IP 주소를 포함한 네트워크 토폴로지와 구조를 파악할 수 있게되고 이를 활용하여 다양한 형태의 공격을 시작할 수 있게 된다. 뿐만 아니라 단순히 브로드캐스트 되는 트래픽들을 엿듣는 수준을 넘어, MAC flooding 공격 등을 통해 네트워크의 모든 프레임을 도청(Eavesdrop)할 수도 있게된다.

이더넷 환경에서 ARP(Address Resolution Protocol)

나 DHCP(Dynamic Host Configuration Protocol)와 같은 일상적으로 이용되는 프로토콜을 이용한 공격은 잘 알려져 있으며 관련도구 또한 인터넷상에서 쉽게 구할 수 있다. 예를 들어 ARP Cache Poisoning은 ARP 응답에 대해 내용 검증을 수행하지 않는 ARP 프로토콜의 취약점을 이용하여 ARP 캐시테이블을 오염시켜 상대방의 데이터 패킷을 중간에서 가로채는 공격이다. 또한, 다른 단말로 가는 DHCP서버 요청에 응답하여 네트워크 트래픽을 제어하는 것도 가능하다. 이러한 기본적인 공격들은 상위 공격을 수행하기 위한 것으로, 이 공격이 성공하면 기존의 단말들간의 세션을 가로채는 세션 하이재킹 공격과 도청되었던 메세지를 수정하여 재송신하는 재생 공격까지 가능해진다.

이더넷 환경은 매체를 공유하는 특성상 가용성 공격, 즉 시스템이 가진 자원을 부족하게 하여 의도된 서비스를 지속해서 제공할 수 없도록 하는 공격에도 취약할 수 밖에 없다. 내부 네트워크에 공격자가 접근하게 되면 TCP의 취약점을 활용한 TCP Syn Flooding과 같은 공격 뿐 아니라 단순하게 대량의 UDP 트래픽을 통해 서버의 가용 대역폭을 없애는 형태의 서비스거부(DoS, Denial of Service)공격도 차단하기 쉽지 않다.

2.2 차량용 이더넷 보안

차량용 이더넷이 도입되면서 다양한 형태의 이더넷 보안 관련 연구와 표준화들이 수행되고 있으며, 이더넷 환경에서의 공격 가능성을 줄이고, 또한 공격당했을 때에도 그 전파범위를 줄이기 위한 방안들을 제안하고 있다.

JASPAR(Japan Automotive Software Platform and Architecture)[3]은 일본의 차량 내부 소프트웨어 플랫폼 표준화 단체로 차량 내부 통신에 참여하는 모든 레벨에서 방화벽을 포함하는 차량용 이더넷 구성을 제안하고 있다. 먼저 차량 네트워크의 핵심인 중앙의 게이트웨이에 차량의 내부와 외부를 구분하고, ACL, VLAN filtering, 인증, 통신 감사 등의 기능을 통해 외부에서 유입되는 비정상 데이터를 거를 수 있는 방화벽 도입을 제안한다. 차량 내부에서 ECU와 직접 연결되는 스위치에도 말단 노드가 해킹되더라도 외부를 공격하는 것을 방지하기 위해 게이트웨이에 포함되는 방화벽과 동일한 기능을 수행하도록 요구한다. 마지막으로 말단 노드마다 모두 방화벽을 설치할 것을 권하고 있다.

[4]에서는 네트워크 환경 중심, 데이터 중심으로 나누어 차량용 이더넷의 보안 전략을 제시한다. 네트워크 환경을 고려한 보안 전략으로 당분간은 기존 CAN과 같은 버스 형태의 전통적인 데이터 통신이 이루어지는 구간과 이더넷을 통해 외부로 데이터를 주고받는 네트워크 구간이 혼재할 것으로 예상하고 있다. 이에 따라 이더넷 스위치 상에서 각 네트워크 구간을 VLAN으로 철저히 격리하고 방화벽 적용을 통한 강력한 접근제어를 제안한다. 또한 데이터 중심의 보안 전략으로 차량 내부 네트워크 구간들에 흐르는 데이터의 성격에 따라 적용할 보안의 수준을 다르게 지정하는 전략을 권하고 있다.

[5]에서는 현재의 차량용 이더넷 환경의 단점으로 차량 내부 컴포넌트에 대한 업데이트가 어렵다는 점을 꼽았다. 이로 인해 차량 설계시의 최신 기술이 차량 운행되는 시점에 적용되는 최신 기술이 될 수밖에 없고, 시간이 지나면 차량에 새로운 취약점이 발견될 수 있으나, 조치가 적용되지 못한다. 이를 극복하기 위해, 침입탐지시스템과 방화벽 뿐만 아니라, 원격 펌웨어 업데이트를 통한 보안관련 기능 최신화 방안을 적용할 것을 제안하고 있다. [6]에서는 기존보다 사용자와 차량 간 네트워크 연결이 활발한 자율주행자동차에 대한 보안 강화를 위한 침입탐지시스템을 제안하였다. 사용자가 지정해둔 rule 옵션을 관리하여 지정된 기준치에 부합하지 않는 비정상적인 접근은 차단시키는 방식을 제안하였다. 침입탐지시스템들에 대한 연구는 지능이 더욱 강화되는 형태로 발전하고 있다. 순환형 학습모델을 적용하여 높은 탐지성능을 보이는 침입탐지시스템이 있으며, [7]에서는 통신이 중첩된 환경에서의 침입탐지시스템의 성능향상을 위해 네트워크 세션들 간의 연관도를 고려함으로써 기존의 순환형 학습모델을 가진 침입탐지시스템에서 탐지하지 못했던 공격들에 대한 탐지성능 향상 기법을 제안하고 있다.

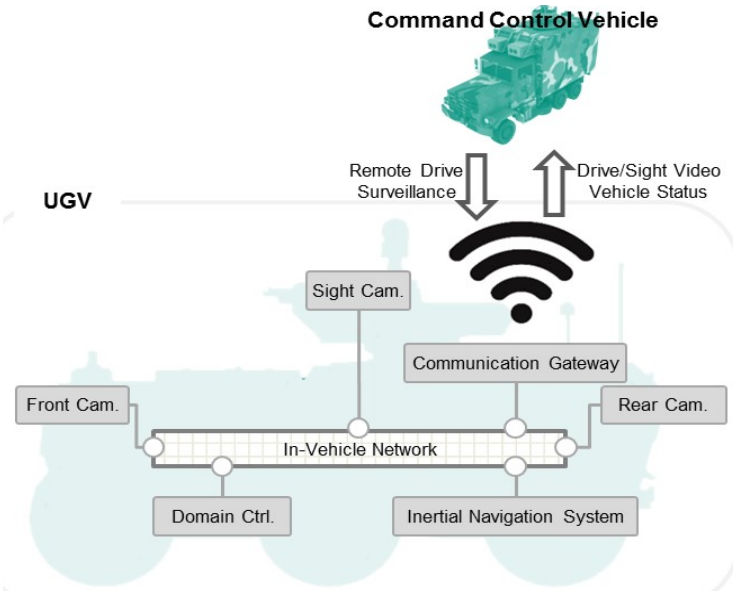

그림 1. 군용무인차량의 운용구조
Fig. 1. An operational architecture of an UGV

III. 군용무인차량의 네트워킹 보안

3.1 군용무인차량 운용구조

무인차량은 그림 1과 같이 원격지의 통제차량과 무선통신을 통해 연결되어, 통제차량이 보내는 제어 정보를 바탕으로 원격/자율 주행하며 감시정찰 등의 임무를 수행한다. 통제차량은 무인차량이 보내는 주행영상과 감시영상, 항법정보를 실시간으로 수신하여 무인차량의 작전환경을 파악하며, 운용자는 수신한 정보를 바탕으로 작전환경에 대한 원격주행과 정찰임무를 수행하게 된다.

또한, 통제차량은 무인차량이 지속적으로 보내는 자신의 상태정보를 바탕으로 현재 무인차량이 임무 수행에 적합한 상태인지를 판단할 수 있다. 이를 수행하기 위해 무인차량 내부에는 무선통신기, 차량제어장치, 전·후방 주행영상 및 감시 영상시스템 등 다양한 장치가 차량내부네트워크를 통해 서로 연결된다[8].

무인차량의 운용을 위해 차량내부에는 다양한 트래픽들이 존재한다. 운용자는 무인차량을 운용할 때 실시간 영상을 기반으로 조종장치를 이용하여 주행/임무장치 운용에 대한 원격 제어 명령을 전송한다. 특히 영상은 운용자가 무인 차량으로부터 받을 수 있는 유일한 피드백 데이터이므로 영상 트래픽은 다른 트래픽과 비교하여 매우 높은 수준의 실시간 송/수신 및 동기화가 보장되어야 한다. 무인차량의 영상정보들은 차량제어장치의 통제없이 바로 통제차량으로 전달되지만, 제어명령이나 상태정보들은 차량제어장치를 통해 취합된 이후 전달된다.

3.2 보안 요구사항

무인차량에 대한 보안공격을 최소화하기 위해서는 외부의 공격자들이 내부로 접근할 수 있는 방법을 최소화하고, 내부에 침입한다 하더라도 피해범위를 최소화할 수 있는 방안이 마련되어야 한다. 다행히 무인차량은 외부와의 접촉점이 무선통신을 통한 원격 접근 외에는 없기 때문에 외부 네트워크에서의 접근방법은 최소화되어 있다. 하지만, 만약 공격자가 물리적인 접근을 통해 무인차량의 내부 네트워크에 접근하게 된다면, 2.1절에서 언급한 모든 공격들의 대상이 될 수 있기 때문에 이들을 고려한 보안방안이 필요하다.

먼저, 허가되지 않은 외부 접속을 차단하고, 내부 구성품들 간의 연결도 허가된 연결 외에는 차단해야 한다. 즉, 이더넷의 가장 큰 특징인 브로드캐스트 특성에 대한 활용을 최소화하는 것이 기밀성 공

격 차단을 위한 가장 중요한 수단이 된다. 다음으로, 내부 장치들이 약속된 형태의 트래픽들만 네트워크에 내보내도록 제어해야 한다. 군용무인차량이 다른 차량들과 다른 점은 외부의 상용서비스와의 연결이 없고, 구성품들의 통신이 미리 정의되어있기 때문에, 정의되지 않은 통신을 필터링하여 차단하기 용이하다는 것이다. 따라서, 불필요하거나 비정상적인 네트워크 사용을 최소화함으로써 무결성 공격을 차단할 수 있다. 마지막으로 가용성 공격을 막기 위해서는 무인차량 내부에서 이용되는 트래픽 분류별로 QoS 요구사항을 사전에 정의하고, 다른 트래픽들로 인해 QoS 요구사항이 침해되는 것을 차단할 수 있어야 한다. 예를 들어 영상데이터 트래픽이 늘어난다해도 제어명령의 트래픽 수신에 문제가 발생하지 않도록 제어할 수 있어야 가용성 공격에 대한 차단이 가능하다.

Ⅳ. 군용무인차량을 위한 내부네트워크 보안 솔루션

본 절에서는 위의 군용무인차량 네트워크 보안요구사항을 만족시키기 위해 SDN기반의 내부네트워크 보안솔루션을 제안한다.

4.1 SDN

기존의 이더넷 장비들은 정해진 프로토콜 동작을 기본으로 수행한다. 반면에 SDN(Software-Defined Networking)은 네트워크 운영체제라고 불리는 SDN 제어시스템 위에서 동작하는 응용프로그램에 따라 네트워크의 동작이 결정된다. 패킷이 스위치의 인터페이스를 통해 입력되면, 스위치는 해당 패킷의 플로우 정보(입력 인터페이스와 헤더정보의 조합)를 추출하여 스위치 내부의 플로우 테이블 내용과 비교한다. 플로우 테이블에는 플로우 정보와 해당 플로우에 대한 액션 정보가 담겨있는데, 만약 일치하는 플로우 정보가 발견된다면 해당 플로우를 정해진 액션으로 처리한다. 예를 들어 모든 ARP 패킷을 네트워크에 브로드캐스팅하라는 항목이 플로우 테이블에 있다면, 스위치는 수신한 ARP 패킷을 입력 인터페이스를 제외한 나머지로 전달한다.

SDN 스위치는 항상 SDN 제어시스템과 보안채널을 유지하며, 플로우테이블내 항목과 일치하지 않는 패킷이 입력될 때 이를 SDN 제어시스템에 문의한다. SDN 제어시스템은 네트워크 운영체제라고도 불리는데, 네트워크를 구성하는 모든 SDN 스위치와 연결을 유지하고 각 스위치의 동작을 결정한다. SDN 제어시스템 상에는 다양한 응용프로그램이 수행되고, 이 응용프로그램이 패킷 플로우에 대한 동작을 결정한다. 예를 들어 L2 MAC Learning 응용은 SDN 제어시스템으로부터 전달받은 플로우정보를 바탕으로 MAC을 가진 단말이 어느 스위치 인터페이스에 연결되어 있는지를 관리할 수 있고, 이를 기반으로 네트워크 노드들간의 L2 레벨 연결을 제공한다.

스위치가 별도의 지능을 갖고 있지 않고, 입력되는 패킷에 대해서 플로우 테이블에 정해진 동작만을 수행하는 것은 보안측면에서 SDN의 장점이다. 기존의 이더넷 스위치는 인터페이스에 연결된 단말이 인가된 단말인지 여부에 대한 별도의 검증없이 해당 단말이 통신하고자 하는 대상의 위치를 파악하기 위해 ARP Flooding과 ARP Response를 처리하면서 기본적인 MAC Learning 동작을 수행한다. 하지만, 동일한 상황에서 SDN은 SDN 제어시스템 위에 L2 MAC Learning 응용이 동작하고, 해당 단말의 패킷을 처리하도록 구성되어 있지 않다면 단말이 스위치로 보내는 패킷을 전달되지 못는다. 이를 통해 SDN기반 네트워크에서는 비인가 노드의 접근을 근본적으로 차단할 수 있게된다.

4.2 제안하는 내부네트워크 보안솔루션

그림 2는 이러한 SDN의 장점을 활용한 군용무인차량 내부 네트워크 보안 솔루션의 구조이다. 제안하는 차량내부 네트워크 보안 솔루션은 SDN 제어시스템 위에 단말들에 대한 정보를 관리하는 인벤토리 관리기능, 인벤토리의 단말들을 가상네트워크에 할당하는 가상네트워크 관리기능, 그리고 각 가상네트워크에 보안정책과 QoS 정책을 관리하는 정책 관리기능을 포함하여 구축되었다.

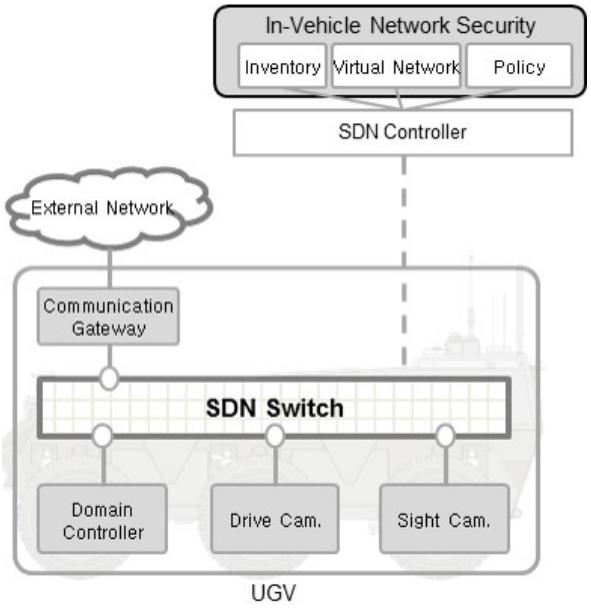

그림 2. 제안하는 군용무인차량 내부 네트워크 보안솔루션
Fig. 2. Proposed in-vehicle network security solution for UGV

먼저, 인벤토리 관리기능은 네트워크에 참여하는 모든 단말들에 대한 정보를 관리한다. 인벤토리에서 관리되는 정보에는 차량 내부 구성품과 차량에 연결되는 모든 단말에 대한 IP 주소 정보뿐만 아니라 스위치 연결정보를 포함한다. 이때 단말이란 동일한 물리 네트워크나 서브넷에 속한 단말들만을 지칭하는 것이 아니라, 통신의 대상이 되는 원격지의 단말을 포함한다. 새로운 단말이 네트워크에 참여하기 위해서는 해당 단말의 정보를 인벤토리에 추가하고, 관리자의 인증을 거쳐야 가능하다. 만약 단말의 정보가 네트워크 관리자의 별도 승인없이 변경(예, 단말의 IP 주소 변경)된다면, 공격자의 침입이 아닌 정상적인 사용자의 부주의에 의한 동작이라 하더라도 이 단말은 네트워크에 참여할 수 없게 된다.

가상 네트워크 관리기능은 인벤토리에 등록된 모든 단말에게 가상 네트워크를 할당한다. 가상 네트워크는 하나의 물리 네트워크를 다수의 논리적인 독립 네트워크로 나누는 기술이다[9]. 따라서, 물리적으로는 동일한 네트워크 스위치에 연결된 단말들이라 하더라도 서로 다른 가상 네트워크에 속한 경우 상호간에 통신이 불가능하다. 이더넷 환경에서의 가상 네트워크 기술의 대표적인 예로 VLAN(IEEE 802.1Q)이 있다. VLAN에서 가상 네트워크는 물리 스위치 인터페이스들의 집합으로 정의된다. 반면에 SDN에서 가상 네트워크는 단말과 단말들 사이 플로우의 집합으로 정의한다.

정책관리 기능은 각 가상 네트워크에 적용되는 보안정책과 QoS정책을 관리한다. 보안정책은 가상 네트워크내 단말들간의 연결 여부를 결정한다. 기존 이더넷 환경에서 하나의 VLAN에 속한 모든 단말들은 상호간에 연결성을 갖지만, SDN기반의 가상 네트워크에서는 동일한 가상 네트워크에 속해도 허용된 단말들 사이의 통신만 가능하게 제어할 수 있다. 이를 바탕으로 가상 네트워크에 할당된 보안정책을 모두 허용할 것인지, 선택된 단말간 연결만 허용할 것인지, 모두 불허할 것인지 정의할 수 있다. 모두 허용의 경우에는 가상 네트워크에 속한 단말들 사이의 통신을 모두 허용하고, 선택적 허용의 경우에는 연결을 허용할 단말들의 정보를 별도로 관리한다.

가상 네트워크에 대한 QoS 정책은 대역폭에 대한 보장을 제공한다. 하나의 가상 네트워크의 대역폭 사용량이 높은 상태에서는 다른 가상 네트워크의 대역폭 사용이 제한될 수 밖에 없다. 이를 방지하기 위해 가상 네트워크마다 QoS 정책을 할당하여 최소 요구사항의 대역폭 활용을 지원한다. 가상 네트워크에 대한 기본 QoS 정책은 최선(best-effort) 정책으로 별도의 대역폭 보장이나 제한없이 이용하는 형태이다. 다음으로 최대제한정책은 해당 가상네트워크의 최대 사용량을 설정된 대역폭으로 제한하여 임계치를 넘는 사용량은 제한한다.

V. 구현 및 검증

5.1 실험환경 구성

제안한 네트워크 가상화를 통한 차량내부 네트워크 보안 기능을 검증하기 위해 실험환경을 그림 3과 같이 구성하였다. 차량간의 통신 상황을 검증하기 위해 SBC(Single Board Computer)를 이용하였다. SBC는 CPU로 Intel Xeon E3-1505L v5@2.00GHz x4 cores, 메모리는 16GB, Intel I210 Gigabit NIC으로 구성되어있다. 운영체제는 CentOS 7을 이용하였고, 내부 네트워크 스위치인 SDN 스위치는

OpenvSwitch v2.9를 SDN 제어시스템으로 오픈소스인 ONOS[10]를 이용하여 구현하였다.

SBC내 가상머신으로 차량제어장치와 주행·감시 영상시스템 그리고 통신 게이트웨이로 동작하는 무선통신기를 에뮬레이션하여 SDN 스위치에 연결하였고, 외부와의 연결은 모두 무선통신기를 통하도록 구성하였다.

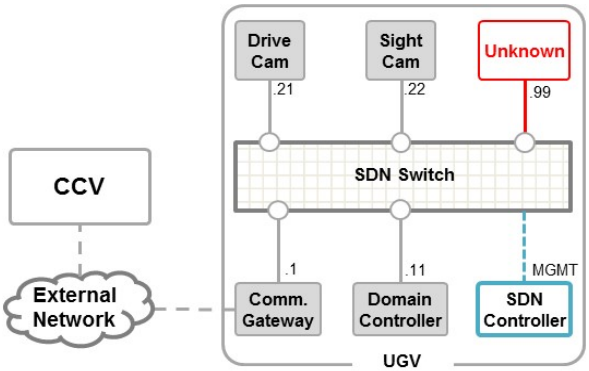

그림 3. 검증을 위한 실험환경구성
Fig. 3. Experiment configurations for the verification

SDN 제어기는 관리 인터페이스를 통해 SDN 스위치와 연결한 후, 차량내부 단말들의 정보를 인벤토리에 등록하였다. 가상 네트워크는 원활한 원격주행 및 감시를 수행할 수 있도록 영상 트래픽과 제어 트래픽 상호간의 영향을 최소화하기 위해 표 1과 같이 영상과 제어를 위한 가상 네트워크를 분리 구성하였다. 주행영상시스템과 감시영상시스템이 통제차량으로 보내는 영상데이터 전송을 위해 가상네트워크1을, 차량제어장치가 운용자의 주행정찰 명령을 수신하기 위해 가상네트워크2를 구성하였고, 가상네트워크마다 보안정책과 QoS정책을 설정하였다.

표 1. 실험을 위한 가상네트워크 및 정책설정
Table 1. Virtual networks and policy configurations for the experiment

Num.	Sender	Receiver	Policy	
			Security	QoS
1	Drive Cam.	Comm. GW	Selective	Max 3Mbps
	Sight Cam.	Comm. GW		Max 3Mbps
	CCV	Drive Cam.		Best Effort
	CCV	Sight Cam.		Best Effort
2	CCV	Domain Ctrl.	Allow All	Best Effort

5.2 실험 결과

이더넷 환경에서 보안공격의 시작점이 될 수 있는 미등록 단말의 네트워크 연결 차단여부를 검증하기 위해 인벤토리에 등록되지 않은 단말을 내부 네트워크스위치에 연결하였다. 이 단말에 네트워크에 접속 가능한 IP주소를 부여하여 기존 이더넷 환경이라면 네트워크의 브로드캐스트 트래픽들은 수신 가능하도록 구성하였다.

그림 4는 그 결과를 나타낸 것으로 차량제어장치에는 트래픽 송수신이 정상적으로 이루어지고 있으나, 미등록 단말에는 수신 패킷이 하나도 발생하지 않았음을 확인할 수 있다.

다음으로 인가되지 않은 상대방과의 연결을 보안정책을 통해 차단할 수 있는지를 검증하기 위해 동일한 가상네트워크 내에 존재하는 단말들간의 연결을 시험하였다. 동일한 가상네트워크에 있는 주행영상시스템과 감시영상시스템, 그리고 무선통신기 사이의 연결을 시험하였고 그림 5는 그 결과를 보여준다.

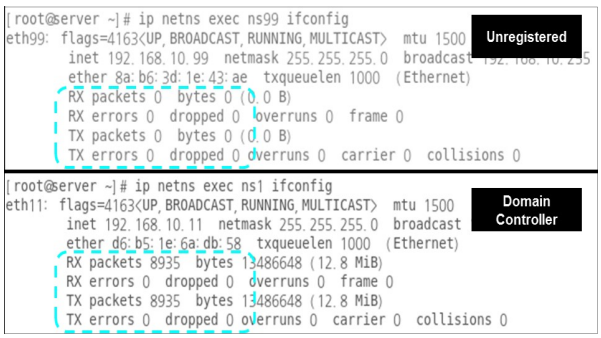

그림 4. 미등록 단말의 네트워크 연결결과
Fig. 4. Result of attaching unregistered endpoints

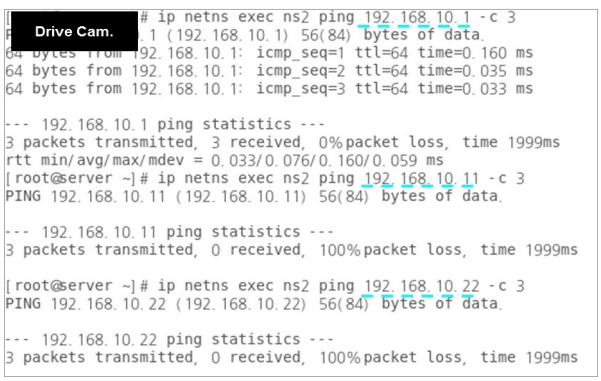

그림 5. 가상네트워크를 통한 장치간 연결 제한 결과
Fig. 5. Result of unauthorized connection restrctions between endpoints with virtual networks

마지막으로 가용성공격이 발생했을 때 가상네트워크의 QoS정책으로 대응이 가능함을 확인하기 위해, 주행영상시스템에서 할당된 대역폭 이상의 트래픽을 발생시켜 다른 장치의 트래픽 송신에 영향을 주는지를 확인하였다. 정상적인 상황에서는 주행영상시스템과 감시영상시스템은 720p의 HD비디오스트림 전송을 위해 2Mbps의 대역폭을 사용하고, 차량제어장치는 통제차량으로 200Hz의 주기로 상태정보송신을 지속하며 256Kbps의 대역폭을 사용한다. 주행영상시스템에서 추가로 10Mbps의 비정상 트래픽을 추가로 발생시켰을 때 발생하는 각 구성품의 패킷 손실을 측정하였고, 그 결과는 표 2와 같다. QoS적용 전에는 모든 장치가 보내는 트래픽이 65% 이상 손실되었으나, 가상네트워크를 통한 QoS정책 적용 후 비정상 트래픽이 발생한 주행영상시스템의 패킷손실율은 81%로 상승하였으나, 차량제어장치와 감시영상시스템의 패킷손실은 0%로 영향을 받지 않았음을 확인할 수 있었다.

표 2. 가용성 공격으로 인한 패킷손실
Table 2. Packets lost due to the availability attack.

Unit	Without QoS		With QoS	
Domain Ctrl.	69%	907/1,309	0%	0/1,307
Drive Cam.	65%	8,865/13,607	81%	10958/13,607
Sight Cam.	74%	10,092/13,607	0%	0/13,606

Ⅵ. 결 론

본 논문에서는 SDN 기술을 활용하여 군용무인차량 내부 네트워크 보안 솔루션을 제안하였다. 기존의 이더넷과 다르게 제어시스템에 의해 정의된 동작만을 수행하는 SDN의 특징을 활용하여 군용무인차량에 필요한 단말들의 정보를 관리하고, 인가된 통신만을 허용하는 보안 정책과 QoS 정책을 통한 대역폭 제어로 이더넷 환경에서 발생가능한 공격들을 추가적인 네트워크 방화벽이나 ECU내 방화벽을 도입하지 않고도 차단할 수 있음을 확인하였다.

군용무인차량의 원격운용을 위해서는 무인차량의 영상과 상태정보, 통제차량으로부터의 제어정보가 상호간에 실시간성을 해치지 않으면서 손실없이 전달되어야 한다. 제안하는 솔루션을 통해 주행, 감시 등의 역할별로 구성품들을 구분하여 가상 네트워크를 구성하고, 동일한 가상 네트워크 내에서도 불필요한 연결은 보안정책을 통해 차단함으로써 일부 구성요소에 대한 보안공격이 차량 전체로 전파되는 가능성을 줄일 수 있다. 또한, 각 구성품의 사용량에 기반한 QoS 정책을 적용한다면 가용성 공격 발생시에도 최소한의 피해로 차량의 운용을 지속할 수 있을 것이다.

향후 제안한 SDN기반 네트워크 보안 솔루션을 실제 군용무인차량 적용을 위해 SDN 자체가 지닌 보안취약점으로부터 자유로운 SDN 도입 방안에 대한 연구를 진행할 계획이다.

References

[1] Z. El-Rewini et. al., "Cybersecurity challenges in vehicular communications", Vehicular Communications, Vol. 23, Jun. 2020.

[2] N. McKeown et. al., "Openflow: enabling innovation in campus networks", Sigcomm Comput. Commun., Vol. 38, No. 2, pp. 69-74, Mar. 2008. https://doi.org/10.1145/1355734.1355746.

[3] M. Kataoka, "Cyber security study for automotive ethernet in Japan automotive industry", in Proc. of 7th IEEE-SA Ethernet & IP Automotive Technology Day, San Jose, CA, USA, Nov. 2017.

[4] D. Ahn and H. Kim, "A survey of automotive ethernet security", in Proc. of KSAE Annual Autumn Conference and Exhibition, Nov. 2018.

[5] Y. Lee, "Ethernet based in-vehicle network and security", Journal of the Korean Society of Automotive Engineers, Vol, 40, No. 12, pp. 36-40, Dec. 2018.

[6] E. Jang and S. Shin, "Proposal of new data processing function to improve the security of self-driving cars' systems", Journal of the Institute of Internet, Broadcasting and Communication (IIBC), Vol. 20, No. 4, pp.81-86, Aug. 2020. https://doi.org/10.7236/JIIBC.2020.20.4.81.

[7] M. Lee, "LSTM model based on session management for network intrusion detection", Journal of the Institute of Internet, Broadcasting and Communication(IIBC), Vol. 20, No. 3, pp.1-7, Jun. 2020. https://doi.org/10.7236/JIIBC.2020.20.3.1.

[8] T. K. Kang, H. Kang, D. Y. Jung, and J. W. Kim, "Threat identification and risk analysis based on EVITA project for military UGV", in Proc. of the Autumn Conference of the Korea Institute of Military Science and Technology, pp. 169-170, Nov. 2017.

[9] S. Kim and S. Chong, "SDN-based policy driven network slicing system", in Proc. of Symposium of the Korean Institute of Communictions and Information Sciences, Jan. 2018.

[10] ONOS(Open Network Operating System), https://onosproject.org. [accessed: Apr. 26, 2021]

저자소개

김 남 곤(Namgon Kim)

2006년 2월 : 광주과학기술원 정보통신공학과(공학석사)
2012년 8월 : 광주과학기술원 정보통신공학과(공학박사)
2012년 9월 ~ 2019년 12월 : (주)케이티 융합기술원 연구원
2019년 12월 ~ 현재 : 국방과학연구소 연구원
관심분야 : 네트워크가상화, In-Vehicle Network, 무인로봇

성 기 열(GiYeul Sung)

1989년 2월 : 경북대학교 전기공학과(공학사)
1991년 2월 : 경북대학교 전기공학과(공학석사)
2010년 2월 : 충남대학교 전자공학과(공학박사)
1991년 ~ 현재 : 국방과학연구소 연구원
관심분야 : 영상신호처리, 컴퓨터비전, 패턴인식

김 도 종(DoJong Kim)

1987년 2월 : 경북대학교 전자공학과(공학석사)
2001년 2월 : KAIST 전기전자공학과(공학박사)
1987년 ~ 현재 : 국방과학연구소 연구원
관심분야 : 로봇시스템 개발, 안정화시스템 개발, 표적탐지/인지/추적