자동차 보안에서의 Secure Timing 메커니즘

강민재 [1], 오현영 [2*]
[1] 가천대학교 AI 소프트웨어학부 학부생
[2] 가천대학교 AI 소프트웨어학부 교수

lusalome2003@gachon.ac.kr, hyoh@gachon.ac.kr

Secure Timing Mechanism in Automotive Security

Minjae Kang, Hyunyoung Oh
Dept. of AI Software, Gachon University

요 약

본 논문은 자동차 보안에서 Secure Timing 의 중요성과 다양한 시간 동기화 방법들을 분석한다. 기존의 일반적인 Secure Timing 방법들과 자동차 환경에서의 차이점을 설명하고, 실시간성 및 보안 요구사항을 충족하기 위한 자동차 보안에 특화된 방법들을 소개한다.

1. 서론

현대 자동차 시스템은 자율 주행, 차량 간 통신(V2V), 차량-인프라 통신(V2I) 등의 발전으로 인해 점점 더 복잡해지고 있으며, 이로 인해 보안 위협 역시 증가하고 있다. 이러한 시스템에서는 수많은 전자 제어 장치(ECU)와 센서들이 네트워크로 연결되어 실시간으로 데이터를 교환하며 작동하는데, 이 과정에서 Secure Timing(보안 시간 동기화)이 매우 중요한 역할을 한다. Secure Timing 은 네트워크 상의 모든 요소들이 동일한 시간에 정확하게 동기화되도록 하여, 시스템의 무결성과 신뢰성을 유지하는 핵심 보안 요소이다.

자동차 보안에서 Secure Timing 이 보장되지 않으면, 공격자는 네트워크의 시간 정보를 조작하거나 왜곡함으로써 시스템의 정상적인 동작을 방해할 수 있다. 이러한 타임스탬프 조작은 자율 주행 차량의 경로 탐색 오류, 안전 시스템의 비정상적 작동, 그리고 차량 간 통신의 지연 등 심각한 결과를 초래할 수 있다. 따라서 Secure Timing 은 자동차 시스템의 보안과 안전성을 유지하기 위한 핵심 요소이다.

본 논문에서는 일반적인 컴퓨팅 환경에서의 시간 동기화 방법과 이를 자동차 보안 환경에 적용할 때의 차이점을 비교하며, 자동차 환경에 적합한 보안 시간 동기화 메커니즘을 알아보고자 한다.

2. 일반적인 컴퓨팅 환경의 Secure Timing 방법

2.1 NTP(Network Time Protocol)

NTP(Network Time Protocol)는 대규모 네트워크에서 컴퓨터들이 정확한 시간을 동기화하기 위해 사용하는 프로토콜로, 특히 Coordinated Universal Time(UTC)을 기준으로 여러 서버와 클라이언트가 동일한 시간을 유지하도록 돕는다. NTP 는 네트워크의 변동에도 불구하고 밀리초 단위의 시간 정확성을 유지할 수 있도록 설계되었으며, 인터넷과 같은 복잡한 환경에서의 시간 동기화 문제를 해결하는 데 중요한 역할을 한다.

NTP 의 동작 방식은 서버와 클라이언트 간에 교환되는 네 가지 타임스탬프를 기반으로 한다. 클라이언트는 요청과 응답 메시지에 포함된 타임스탬프를 바탕으로 왕복 지연 시간(δ)과 클록 오프셋(Θ)을 계산하여 시간을 동기화한다. 왕복 지연 시간은 메시지가 오가는 데 걸리는 시간을 의미하며, 클라이언트가 네트워크의 지연을 파악하는 데 사용된다. NTP 는 대칭적(peer-to-peer) 동작 방식을 채택하여, 여러 서버와 클라이언트가 동시에 시간 정보를 주고받을 수 있는 구조를 제공한다. 이를 통해 네트워크 장애가 발생하더라도 다른 경로를 통해 시간을 동기화할 수 있으며, 안정적이고 정확한 시간 동기화를 유지한다[1]. 그러나 NTP 는 인증 메커니즘이 약해 스푸핑이나 중간자 공격에 취약하다는 한계가 있다.

2.2 Network Time Security (NTS)

NTP(Network Time Protocol)는 보안 조치 없이 시간 정보를 전송하기 때문에 중간자 공격이나 타임스탬프 조작에 취약하다. 이러한 문제를 해결하기 위해 Network Time Security (NTS)가 도입되었다. NTS 는 TLS(Transport Layer Security)를 사용해 서버와 클라이언트 간 안전한 통신을 설정하고, NTP 메시지의 무결성과 인증을 보장한다.

NTS 는 먼저 대칭 키를 설정한 후, NTP 메시지에 고유 식별자와 암호화된 쿠키를 포함시켜 메시지를 안전하게 전송한다. 이를 통해 서버는 클라이언트의 메시지를 검증하고, 안전한 응답을 전송한다. 특히, 쿠키 메커니즘을 통해 서버의 stateless 운영이 가능해져 DDoS 공격에 대한 내성이 강화된다. NTS 는 기존 NTP 구조를 크게 변경하지 않으면서도 강력한 보안을 제공하지만, 추가적인 연산으로 인한 오버헤드가 발생할 수 있다[2].

2.3 Dynamic Network Time Protocol (DNTP)

DNTP 는 변화하는 네트워크 환경에서 NTP 의 정확도를 개선하기 위해 제안된 방법이다. DNTP 는 실시간 RTT(Round-Trip Time) 측정과 동적 임계값 조정을 통해 네트워크 지연 변화에 적응적으로 대응한다[3]. 구체적으로, DNTP 는 RTT 샘플의 표준편차(σ)를 계산하고, 이를 바탕으로 동적

* 교신저자

임계값 D = k × σ (k 는 스케일링 팩터)를 설정한다. 시간 오프셋은 offset = RTT/2 - D 로 계산되며, 이를 통해 네트워크 상태 변화에 따른 지터를 보정한다. DNTP 는 특히 자동차 네트워크와 같이 동적인 환경에서 기존 NTP 보다 안정적인 성능을 보이지만, 지속적인 RTT 모니터링으로 인한 추가적인 연산 부하가 발생할 수 있다는 한계가 있다.

3. 자동차 환경에서의 Secure Timing 요구

일반적인 시스템에서 Secure Timing 은 데이터 전송 보안을 강화하는 데 주로 사용되며, 실시간 반응이 필수적이지 않다. 반면, 자동차 시스템은 실시간 작동이 매우 중요하며, 충돌 방지 시스템이나 ABS 같은 기능은 짧은 시간 내에 반응해야 한다. 타이밍의 미세한 지연도 심각한 사고로 이어질 수 있다.

또한, 일반 시스템은 충분한 계산 자원과 전력 공급을 통해 복잡한 암호화 알고리즘을 처리할 수 있지만, 자동차는 제한된 자원과 전력 때문에 경량화된 Secure Timing 방법이 필요하다. 일반 네트워크는 중앙 집중식 구조로 관리가 가능하지만, 자동차는 분산된 ECU 들 간의 정확한 동기화가 필수적이다.

4. 자동차 환경에 적용 가능한 Secure Timing 방법

4.1 Precision Time Protocol (PTP)

Precision Time Protocol (PTP)는 IEEE 1588 표준에 기반한 고정밀 시간 동기화 프로토콜로, 마이크로초 단위의 정확성을 제공한다. PTP 는 마스터-슬레이브 계층 구조를 통해 노드 간의 시간을 동기화하며, 특히 공장 자동화, 금융 시스템, 자동차 보안 환경에서 자율 주행, V2V 통신 등의 실시간 데이터 동기화에 적합하다[4].

PTP 의 작동 방식은 다음과 같다. 먼저, Best Master Clock (BMC) 알고리즘을 사용하여 네트워크 내에서 가장 정확한 시계를 가진 Grandmaster Clock 을 선택한다. PTP 는 시간 동기화를 위해 2-Step Sync 방식을 사용한다. SYNC 메시지는 마스터의 시간을 전송하며, FOLLOW_UP 메시지가 SYNC 메시지 이후에 전송되어 정확한 타임스탬프를 전달한다. 이를 통해 슬레이브는 네트워크 지연을 최소화하면서 마스터와 시간을 정확히 동기화할 수 있다.

보안 측면에서 PTP 는 기본적으로 인증 메커니즘이 없어 스푸핑 공격에 취약하다. PTP 에 대한 주요 공격 벡터로는 1) 가짜 마스터 공격, 2) 지연 조작 공격, 3) Sync 스푸핑 공격 등이 있다. 이를 방지하기 위해 IEEE 1588-2019 에서는 AUTHENTICATION TLV 를 도입하여 메시지 인증을 지원한다. 또한, IPsec 이나 MACsec 과 같은 하위 계층 보안 프로토콜과의 결합을 통해 추가적인 보안을 제공할 수 있다.

4.2 Time-Sensitive Networking (TSN)

Time-Sensitive Networking (TSN)은 IEEE 802.1 표준에 기반한 네트워크 기술로, 실시간 애플리케이션에서 정확한 시간 동기화, 지연 시간 보장, 패킷 손실 최소화를 목표로 한다. TSN 은 고도의 정확성과 신뢰성이 요구되는 산업 자동화, 자동차 제어, 오디오 및 비디오 제작과 같은 분야에서 널리 사용되며, 자동차 보안 환경에서도 실시간 통신과 정확한 데이터 처리를 제공할 수 있어 적합하다[5].

TSN 의 동작 방식에서 가장 중요한 요소는 시간 동기화이다. 네트워크 내 모든 장치는 IEEE 1588 Precision Time Protocol (PTP)을 사용하여 마이크로초 단위의 정밀도로 동기화된다. 또한, TSN 은 대역폭 예약과 패킷 스케줄링을 통해 특정 데이터 흐름에 대해 사전 예약된 대역폭을 사용하여 지연 시간과 혼잡을 최소화한다. 패킷 복제 및 제거 메커니즘을 통해 TSN 은 네트워크 장애 시에도 데이터 손실을 방지한다.

보안 측면에서 TSN 은 기본적으로 물리적 보안과 네트워크 분리에 의존한다. 그러나 TSN 네트워크의 개방성 증가로 인해 새로운 보안 위협이 발생할 수 있다. 주요 보안 이슈로는 1) 시간 동기화 공격, 2) 구성 변조 공격, 3) QoS 남용 등이 있다. 이를 해결하기 위해 IEEE 802.1X 를 통한 인증, MACsec 을 통한 암호화, SDN 기반의 동적 접근 제어 등의 방법이 제안되고 있다.

5. 결론

본 논문에서는 자동차 보안에서 Secure Timing 의 중요성과, 이를 구현하기 위한 다양한 시간 동기화 프로토콜들을 분석하였다. NTP, NTS, DNTP 는 일반적인 네트워크 환경에서 신뢰할 수 있는 시간 동기화를 제공하는 중요한 프로토콜이지만, 자동차와 같은 실시간 및 고신뢰성이 요구되는 시스템에서는 한계가 존재한다. PTP 와 TSN 은 비록 자동차 환경에만 특화된 기술은 아니지만, 그들의 특성으로 인해 자동차 시스템의 요구사항을 충족시킬 수 있는 잠재력을 가지고 있다. 이러한 기술들은 자동차의 분산된 네트워크 구조에서 효율적인 시간 동기화와 실시간 통신을 제공할 수 있으며, 이를 통해 시스템이 정밀한 타이밍과 보안을 동시에 확보할 수 있는 가능성을 보여준다.

향후 연구에서는 이러한 기술들을 자동차 환경에 최적화하고, 실제 차량 네트워크에서의 구현을 통해 성능을 검증하는 것이 필요하다. 또한, 자동차 특유의 요구사항과 제약 조건을 고려한 추가적인 기술 연구가 요구된다. 또한, 신규 공격 벡터에 대한 대응 방안을 마련하고, 시스템의 보안을 강화하는 추가적인 기술 연구가 요구된다. 이를 통해 자동차 보안 시스템이 점점 더 복잡해지는 사이버 위협에 대응할 수 있을 것이다.

사사문구

이 논문은 2024 년도 정부(산업통상자원부)의 재원으로 한국산업기술기획평가원의 지원(No. RS-2024-00406121, 자동차보안취약점기반위협분석시스템개발(R&D))과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2022-00166529)을 받고 과기정통부 정보통신기획평가원의 정보보호핵심원천기술개발사업(No. RS-2024-00337414)으로 수행한 결과임.

참고문헌

[1] Mills, D. L., "Internet Time Synchronization: The Network Time Protocol," IEEE Transactions on Communications, 1991

[2] Langer, M., Behn, T., & Bermbach, R., "Securing Unprotected NTP Implementations Using an NTS Daemon," Ostfalia University of Applied Sciences, 2019

[3] Gamage, K.A.A.et al., “A Dynamic Framework for Internet-Based Network Time Protocol,” Sensors, 2024

[4] Itkin, E. & Wool, A., "A Security Analysis and Revised Security Extension for the Precision Time Protocol," IEEE Transactions on Dependable and Secure Computing, 2017

[5] Finn, N., "Introduction to Time-Sensitive Networking," IEEE Communications Standards Magazine, 2018