CAN에서 보안 게이트웨이를 이용한 침입탐지기법 제안

안수현[1)(*)], 김광조[1) 2)(†)]

카이스트 정보보호대학원[1)]/ 전산학부[1) 2)]

A Intrusion Detection Scheme in CAN using Security Gateway

Soohyun Ahn[1)(*)], Kwangjo Kim[1) 2)(†)]

Graduate School of Information Security[1)] / School of Computing, KAIST[2)]

요 약

ICT 기술의 발전은 많은 분야에 영향을 주었다. 그 중 자동차 분야 역시 ICT 기술과 접목되면서 많은 영향을 받았다. 이러한 영향으로 인해 자동차 네트워크인 Controller Area Network (CAN)가 등장하게 되었고 현재 가장 널리 사용되고 있다. 하지만 CAN이 가진 특징들로 인하여 스푸핑 및 Denial of Service (DoS) 공격이 쉽게 가능한 상황이며 실제로 여러 연구에서 이를 이용한 여러 가지 공격이 증명되고 있다. 이 공격들은 운전자에게 큰 위험을 야기 시킬 수 있으므로 이에 대한 대비가 시급한 상황이다. 따라서 본 논문에서는 스푸핑 및 DoS 공격을 탐지하고 방어할 수 있는 보안 게이트웨이를 제안한다.

I. 서 론

ICT 기술의 발전은 많은 분야에 영향을 주었다. 그 중 자동차 분야 역시 ICT 기술과 접목되면서 많은 영향을 받았다. 이로 인해 기계만으로 작동된다고 생각되던 자동차가 이제는 점점 발전하여 거의 모든 것이 전자식으로 바뀌게 되었다. 이러한 자동차의 전자화에 크게 기여한 것은 자동차 엔진, 브레이크, 트랜스미션 등을 제어 할 수 있게 해주는 Electronic Control Unit (ECU)의 등장이라 할 수 있다. 지금 현재 자동차 안에 ECU들은 대략 70여개로 자동차의 발전이 더욱 더 이루어질수록 ECU의 비중은 더 높아져 앞으로 100개 이상의 ECU들이 자동차 내부에 존재할 것으로 예측되는 상황이다. ECU로 인해 자동차의 조작이 편리해지긴 했지만 ECU들이 독립적으로 작동하지는 않기에 서로 유기적으로 작동하기 위한 자동차용 네트워크가 필요한 상황이 발생하게 되었다. 이러한 요구에 발맞추어 CAN, LIN, FlexRay로 대변되는 자동차용 네트워크 프로토콜이 개발되게 되었다. 그 중 CAN은 대표적인 자동차용 네트워크 프로토콜로 현재 대부분의 자동차에서 표준으로 사용하고 있다.

CAN의 도입으로 인해 자동차의 제어가 더 편리해지고 효율적으로 바뀌었지만 이러한 발전의 비례하여 CAN의 보안에 대한 대비는 연구가 거의 되지 않고 있는 상황이며 자동차 보안에 대한 인식도 중요하게 생각되지 않아 큰 문제가 발생하고 있다. 이렇게 자동차 해킹이 쉽게 가능한 것은 CAN이 근본적으로 보안상 취약한 특징들을 가지고 있기 때문이다. 이러한 시도는 최근 여러 연구[1][2][3]를 통해 실현 가능성이 입증되었으며, CAN에 대한 보안 대책이 큰 문제로 대두되게 만들었다. CAN에서의 보안 문제들을 해결하기 위해 다양한 연구들[4][5][6][7]이 진행되었지만 여러 부분에서 보완이 필요한 상황이다. 따라서 본 논문에서는 기존의 CAN에서 사용되는 게이트웨이를 변형한 보안 부분을 담당하는 보안 게이트웨이를 도입하여 스푸핑과 DoS 공격을 탐지하는 방법을 제안하고자 한다.

(*) 주저자: 안수현 (ahn1015@kaist.ac.kr)
(†) 교신저자: 김광조 (kkj@kaist.ac.kr)

본 논문의 구성은 다음과 같다. 2장에서 CAN과 CAN에서 가장 문제시 되고 있는 스푸핑과 DoS 공격에 대해 설명하며, 3장에서 보안 게이트웨이에 대해 설명한다. 마지막으로 4장에서는 결론을 맺는다.

II. 배경지식

2.1 CAN

CAN은 1986년 2월에 미국의 자동차 관련 업계 단체인 SAE (Society of Automotive Engineers : 자동차 기술자 협회)의 회의에서 독일의 Robert Bosch사가 제안하였다. Bosch사는 1991년에 현재의 사양인 CAN 프로토콜 사양 2.0을 발표하고 ISO (International Organization for Standardization : 국제표준화기구)에 제출하였다. 1993년 11월에는 정식 ISO 표준으로 'ISO 11989'이 공개되었고 물리계층의 전송속도는 최대 1.0Mbps로 정의 되었다. 또한 1995년에는 개정안이 제출되어 ISO 11898로 확장되고 29bit의 ID를 가진 CAN이 등장했다. 이것은 현재 'CAN 2.0B'로 불리고 있으며 [8]. CAN의 주요 특징은 아래와 같다.

1) 브로드캐스트 방식
2) CAN만의 자체적인 중재 기능 제공
3) 두 가지 레벨이 존재 (도미넌트, 리세시브)

2.2 스푸핑

2.1에서 설명한 CAN의 특징을 살펴보면 스니핑 공격에 취약한 환경임을 알 수 있다. 이것은 기본적으로 CAN이 브로드캐스트 환경이기에 발생하는 문제이다. 그러므로 공격자가 임의로 악의적인 ECU를 버스 상에 설치한다면 모든 메시지를 수집할 수 있다. 그리고 이 수집된 정보를 이용하여 가짜 메시지 또한 만들 수 있고 이를 버스 상에 흘러 보낼 수 있다. 즉, 스푸핑 공격이 쉽게 가능하다. 실제로 이를 악용하여 가짜 메시지를 보내 자동차의 브레이크, 운전대, 계기판 등을 임의로 조작 가능하다는 것이 여러 실험을 통해 입증 되었다.

2.3 DoS

CAN에서 제공하는 중재기능을 악용하면 DoS 공격 또한 쉽게 가능하다. 일단 공격자가 버스 상에 메시지를 수집하여 가장 높은 우선순위를 가진 ID를 알아낸다. 그리고 이 ID를 이용하여 가짜 메시지를 만들어 버스 상에 지속적으로 흘려주게 되면 공격자에 의한 가짜 메시지가 높은 우선순위를 가지고 있기 때문에 다른 메시지는 중재기능에 의해 전송이 되지 못하게 된다. 이러한 상태가 지속되면 버스에는 공격자의 메시지만이 남게 되어 아무런 메시지가 전달되지 못하게 되는 DoS 공격 상황이 된다. 이 공격 또한 여러 논문에서 실현 가능성이 입증되었다.

III. 보안 게이트웨이

본 장에서는 논문의 핵심이라고 할 수 있는 보안 게이트웨이에 대해서 설명한다. Fig 1은 보안 게이트웨이에 존재하는 컴포넌트들을 보여주고 있다. 각 컴포넌트의 역할은 아래와 같다.

· 탐지 컴포넌트
  스푸핑과 DoS 공격 탐지를 위한 컴포넌트

· 라우팅 컴포넌트
  다른 도메인으로의 메시지 전달을 위한 컴포넌트

· 매니지먼트 컴포넌트
  시드값, 검증 메시지 생성, 테이블 관리 등을 위한 컴포넌트

· CAN 컴포넌트
  CAN 통신을 위한 컴포넌트

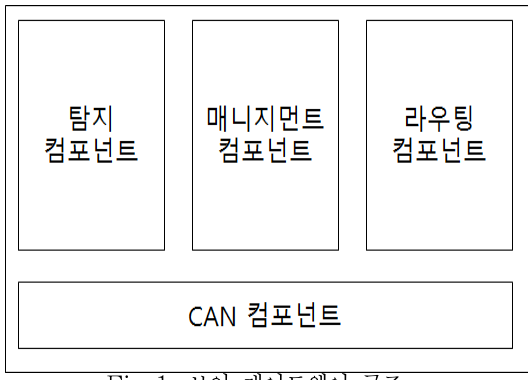

Fig 1. 보안 게이트웨이 구조

3.1 스푸핑 공격 방어

CAN에서는 다양한 ECU들이 존재하며, 이 ECU들은 특정한 목적을 위해 사용된다. 그리고 이 ECU들은 서로 연관이 되어 유기적으로 작동한다고 생각할 수 있다. 예를 들어 운전자가 좌 혹은 우 회전을 한다면 운전자는 브레이크, 운전대, 엑셀 순으로 행동을 수행하고 이 순서대로 ECU의 메시지들이 전달될 것이다. 결국 운전자의 행위에 의해 ECU들의 관계가 정해지고 메시지의 순서가 정해진다고 볼 수 있다. 이를 이용하면 메시지의 순서를 모니터링 한다면 스푸핑 공격을 탐지 할 수 있다.

보안 게이트웨이에서 연관된 메시지에 대한 정보를 테이블로 미리 저장하고 보안 게이트웨이는 탐지 컴포넌트를 통해 버스를 모니터링 하다가 테이블에서 각 행동과 관련된 첫 번째 메시지가 전송되면 다음 메시지를 관찰한다. 만약 예상된 메시지가 테이블과 다르다면 이를 공격으로 생각할 수 있다. 하지만 이러한 메시지가 정상적인 ECU에 의해 전송될 수 있으므로 이를 확인하는 과정이 필요하다. 이를 위해 해시 알고리즘 중 하나인 키 기반의 SipHash 알고리즘[9]을 사용한다. 보안 게이트웨이의 매니지먼트 컴포넌트에서 메시지의 해시값을 요청하여 메시지를 검증한다. 정상 ECU에 의한 메시지라면 유효한 해시값을 생성하므로 검증이 가능하지만 공격자는 해시에 사용되는 키 값을 알지 못하므로 해시 값 생성이 불가하므로 검증이 실패하게 된다. Table 1은 스푸핑 공격 탐지에 사용되는 행동들과 연관된 ECU들을 나타내고 있다.

3.2 DoS 공격 방어

DoS 공격을 방어하기 위해서 임시 ID를 사용한다. 스푸핑 공격에서와 마찬가지로 보안 게이트웨이는 탐지 컴포넌트를 이용하여 버스를 모니터링 한다. 이때 기존의 사용되던 탐지 방법인 빈도를 이용한 방법을 이용하여 탐지한다. 이 때, 모든 메시지가 아닌 가장 높은 우선순위를 갖는 ID의 메시지만을 모니터링한다. DoS 공격 탐지 시 보안 게이트웨이의 매니지먼트 컴포넌트에서 임시 ID를 만들기 위한 시드값을 생성한다. 이때, 매니지먼트 컴포넌트는 이 시드값을 이용하여 먼저 임시 ID와 원래 ID를 매칭 시킨 테이블을 만들어서 다른 도메인과의 통신에 지장이 없도록 한다. 또한, 시드값을 보내기 전에 임시 ID를 만드는 식을 이용하여 사전에 각 임시 ID들이 충돌이 없는지도 검사를 한다. 만약 충돌이 발생한다면 다시 시드값을 다시 만들고 이를 각 ECU에 전달한다. 그러면 각 ECU에서는 이를 바탕으로 새로운 ID를 생성한다. 이 때, 사용되는 식은 (자신의 ID+시드값)/n이다. 이 식에서 n은 도메인상의 노드 개수를 나타낸다. 결과값을 다시 SipHash의 넣는다. 최종적으로 64bit의 결과물이 나오는데 CAN에서 사용되는 메시지 ID가 11bit이기에 결과물의 이를 고려하여 결과값의 하위 11bit를 구한다. 그리고 이 11bit와 가장 높은 우선순위를 갖는 ID를 이용하여 나머지 연산을 한다. 이러한 연산을 하는 이유는 기본적으로 CAN에서 가장 높은 우선순위를 갖는 ID는 가장 작은 값을 가지므로 가장 높은 우선순위의 ID로 나머지 연산을 하면 항상 이 ID보다 작은 ID값이 나오게 된다. 그러므로 결국 생성되는 임시 ID들은 DoS 공격에 사용되는 ID보다 더 높은 우선순위를 갖게 된다. 이렇게 모든 ECU들이 ID들을 만들어 사용하게 되면 임시 ID들이 가장 높은 우선순위를 갖는 ID보다 이 임시 ID 들이 우선순위가 높기 때문에 DoS 공격은 아무런 효과가 없게 된다. DoS 공격이 멈춘 이후에는 다시 원래의 ID로 전환하여 원래의 네트워크 상태를 복구하면 된다. 그리고 다시 DoS 공격이 발생하게 되면 다시 랜덤 임시 ID를 사용하여 방어를 한다.

운전자의 행동들	관련된 ECU들
정상시	Electronic stability control ECU, (Transmission ECU),Engine Control Module ECU
좌/우 회전, 유턴	Electronic Brake Control Module ECU, Transmission ECU, Electric Power Steering ECU, Throttle ECU
시동	Engine Control Module ECU, Transmission ECU, Throttle ECU, Instrument cluster ECU
정지	Electronic Brake Control Module ECU, Transmission ECU, Engine Control Module ECU,
가속	Transmission ECU, Throttle ECU, Instrument cluster ECU
감속	Electronic Brake Control Module ECU, Transmission ECU, Instrument cluster ECU
주차/정차	Electronic Brake Control Module ECU, Transmission ECU, Engine Control Module ECU, Instrument cluster ECU, Electric Parking Brake ECU
라이트	Light Control Module ECU, Adaptive Front Lighting ECU, Instrument cluster ECU
후진	Electronic Brake Control Module ECU, Transmission ECU, Instrument cluster ECU, Electric Power Steering ECU, Transmission ECU
차선변경	Light Control Module ECU, Electric Power Steering ECU, Throttle ECU

Table 1. 스푸핑 공격 탐지에 사용되는 테이블

○: Good
△: Normal
×: Bad

	도입 비용 유무	기존 대비 트래픽 증가 유무	ECU 연산량 증가 유무	탐지율	기존 시스템에 미치는 영향	스푸핑 공격과 DoS 공격 동시 탐지	검증 유무
제안방식	**△**	**△**	**△**	**○**	**△**	**○**	**○**
IDS 방식	△	○	△	×	△	△	△
불법전송 차단 방식	○	○	○	△	△	×	×
MAC 방식	△	×	×	○	×	×	△
암호화 방식	△	×	×	○	×	×	△

Table 2. 기존 방식들과 제안 방식의 비교

IV. 결론 및 향후연구

Table 2는 기존의 제시되었던 방식들과 본 논문에서 제시한 방식을 비교한 비교표이다. 제안 방식은 기존의 다른 방식들에서 해결하고 있지 못하고 있는 트래픽, 연산량, 감지 정확도, 검증 부분 등에서 좋은 결과를 보여줄 것으로 예상된다.

향후 연구로는 본 논문에서 제안된 방식을 실제로 구현하여 탐지율, 트래픽 등에서 기존의 방식들보다 얼마만큼의 효율성을 갖는지 검증해보는 실험이 필요하다.

References

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, and S. Savage, (2010, May). "Experimental security analysis of a modern automobile." In *Security and Privacy (SP), 2010 IEEE Symposium on* (pp. 447-462). IEEE.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, and T. Kohno, (2011, August). "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In *USENIX Security Symposium*.

[3] I. Roufa, R. Miller, H. Mustafaa, T. Taylora, O. Sangho, W. Xu, M. Gruteserb, W. Trappeb, , and I. Seskarb, (2010, February). "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study". In *19th USENIX Security Symposium, Washington DC* (pp. 11-13).

[5] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi "A method of preventing unauthorized data transmission in controller area network." Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th. IEEE, 2012.

[6] M. Müter, and N. Asaj, (2011, June). "Entropy-based anomaly detection for in-vehicle networks." In *Intelligent Vehicles Symposium (IV), 2011 IEEE* (pp. 1110-1115). IEEE.

[7] M. Muter, A. Groll, and F. C. Freiling. "A structured approach to anomaly detection for in-vehicle networks." Information Assurance and Security (IAS), 2010 Sixth International Conference on. IEEE, 2010.

[8] C. W. Lin, and A. Sangiovanni-Vincentelli. "Cyber-security for the Controller Area Network (CAN) communication protocol." *Cyber Security (CyberSecurity), 2012 International Conference on*. IEEE, 2012.

[9] S. Michio, "자동차 네트워크 시스템", 성안당

[10] A. Jean-Philippe, and D. J. Bernstein. "SipHash: a fast short-input PRF." *Progress in Cryptology-INDOCRYPT 2012*. Springer Berlin Heidelberg, 2012. 489-508.