The Transactions of the Korea Information Processing Society
TKIPS Vol.13, No.10, pp.475~480
eISSN: 3022-7011
https://doi.org/10.3745/TKIPS.2024.13.10.475

Adaptive Secure Firmware Over The Air Update Mechanism for Lightweight Internet of Things

Seung Eun Lee† · Jin Min Lee†† · Il Gu Lee†††

ABSTRACT

As Internet of Things (IoT) technology is being used in all industries, the importance of secure and convenient firmware update technology is increasing. However, conventional FOTA (Firmware Over-The-Air) technology has a problem because the security is weak when updating firmware with a single path, and strong encryption technology cannot be utilized. Therefore, this study proposes a secure FOTA (S-FOTA) mechanism for lightweight IoT and adaptive S-FOTA ARQ (Automatic Repeat Request) mechanism. This adaptive S-FOTA ARQ mechanism considers the case where the original file cannot be recovered because of the increase in lost files due to the congested channel state and compares and analyzes the conventional method in terms of security, complexity, and transmission speed. Experimental results show that S-FOTA with 40 encrypted files reduced the attacker's attack success rate by at least 62.58% and up to 99.99%, and S-FOTA with 40% of the total number of encrypted file segments takes at least 996.39% more time on average and up to 3374.99% more time than conventional FOTA. In addition, the transmission speed of the adaptive S-FOTA ARQ mechanism was at least 63.16% and up to 2736.36% higher than that of the conventional S-FOTA, and at least 53.89% and up to 70.89% higher than that of the conventional ARQ mechanism.

Keywords : Firmware Over-The-Air, Shamir's Secret Sharing, Internet of Things, Adaptive FOTA

경량 사물인터넷을 위한 안전한 적응형 무선 펌웨어 업데이트 메커니즘

이 승 은† · 이 진 민†† · 이 일 구†††

요 약

최근 전 산업 분야에서 사물인터넷 (Internet of Things, IoT) 기술이 활용되면서 안전하고 편리한 펌웨어 업데이트 기술의 중요성이 커지고 있다. 그러나 종래의 FOTA (Firmware Over-The-Air) 기술은 단일 경로로 펌웨어를 업데이트하여 보안이 취약하고, 강력한 암호 기술을 활용할 수 없는 문제가 있다. 따라서 본 연구에서는 경량 IoT를 위한 안전한 FOTA (Secure FOTA, S-FOTA) 메커니즘과 혼잡한 채널 상태로 인해 유실되는 파일이 증가하여 원본 파일을 복구할 수 없는 경우를 고려한 ARQ (Automatic Repeat Request) 기반 적응형 S-FOTA 메커니즘을 제안하고, 종래의 방식과 보안성, 복잡도 및 전송 속도 측면에서 비교·분석한다. 실험 결과에 따르면 암호화 파일의 수가 40개인 S-FOTA는 공격 성공률을 최소 62.58%, 최대 99.99% 감소시켰으며, 암호화된 분할 파일의 수가 전체 분할 파일 수의 40%인 S-FOTA는 기존의 FOTA 대비 평균 소요 시간이 최소 996.39%, 최대 3374.99% 더 소요됨을 확인하였다. 또한 ARQ 기반 적응형 S-FOTA 메커니즘의 전송 속도는 기존의 S-FOTA 대비 최소 63.16%, 최대 2736.36% 더 높았으며, 기존의 ARQ 메커니즘 대비 최소 53.89%, 최대 70.89% 더 높았다.

키워드 : Firmware Over-The-Air, Shamir's Secret Sharing, 사물인터넷, 적응형 FOTA

1. 서 론

최근 사물인터넷 (Internet of Things, IoT) 기술이 전 산업 분야에 널리 활용되면서, IoT 펌웨어 업데이트 메커니즘의 보안이 중요해지고 있다[1]. IoT 장치는 리소스가 제한되므로 경량화된 암호를 적용하거나, 악성 트래픽을 준최적 탐지하여 프로토콜을 경량화하는 방법을 사용한다[2, 3]. 이렇게 경량화가 중요한 IoT 펌웨어를 무선으로 업데이트하는 FOTA (Firmware Over-The-Air) 메커니즘은 효율적인 비용으로 클라이

※ 본 논문은 2024년도 정부재원(과학기술정보통신부 여대학원생 공학연구팀 제 지원사업)으로 과학기술정보통신부와 한국 여성과학기술인육성재단의 지원(WISET 계약 제 2024-138호), 산업 통상자원부 및 한국산업기술진흥원이 지원(No.RS-2024-00415520)과 과학기술정보통신부 및 정보통신기획평가원의 지원(No.IITP-2022-RS-2022-00156310)을 받은 연구결과로 수행되었음.
※ 이 논문은 2024년 ASK 2024의 우수논문으로 "경량 IoT를 위한 안전한 무선 펌웨어 업데이트 메커니즘"의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 성신여자대학교 융합보안공학과 학사과정
†† 준 회 원 : 성신여자대학교 미래융합기술공학과 박사과정
††† 종신회원 : 성신여자대학교 융합보안공학과·미래융합기술공학과 교수
Manuscript Received : July 11, 2024
Accepted : September 6, 2024
* Corresponding Author : Il Gu Lee(iglee@sungshin.ac.kr)

언트를 업데이트하는 편리하고 안전한 방법으로 주목받고 있다[4]. FOTA 프로세스는 업데이트 파일 생성 과정과 파일 전송 프로세스 관리 과정 및 업데이트 수행 과정으로 구성된다[5]. 클라이언트는 FOTA 프로세스에 따라 서버가 무선으로 전송한 펌웨어 파일을 통해 펌웨어를 업데이트한다. 이러한 FOTA 메커니즘을 통해 서버는 여러 클라이언트를 동시에 업데이트할 수 있다. 종래의 FOTA 메커니즘은 서버가 클라이언트에게 단일 경로로 펌웨어 업데이트 파일을 전달하므로 파일 탈취 공격에 취약한 문제가 있지만, SSS (Shamir's Secret Sharing)를 적용하면 펌웨어 파일을 조각으로 분할한 후 다중 경로로 전달하여 이 문제를 해결할 수 있다. SSS를 이용하면 클라이언트는 파일 전달 과정에서 분할 파일 일부가 탈취되어 전체 분할 파일을 획득하지 못하더라도 원본 파일을 복구할 수 있다. SSS는 2차원 평면에서 k개의 점 $(x_1, y_1), \cdots, (x_k, y_k)$이 주어지면, 모든 i에 대해 $q(x)=y_i$를 만족하는 유일한 $k-1$차 다항식 $q(x)$가 존재하는 다항식 보간법에 기반한다. $a_o=D$인 $k-1$차 다항식 $q(x)=a_o+a_1x+\cdots+a_{k-1}x^{k-1}$에서, $D_1=q(1), \cdots, D_i=q(i), \cdots, D_n=q(n)$이므로, n개의 조각 중 k개를 획득한다면 다항식 $q(x)$를 복원할 수 있다. 이를 통해 $q(0)$ 값을 계산하면 원래 데이터 D를 얻을 수 있으므로 분할 파일의 일부 조각만 획득하더라도 원본 파일을 획득할 수 있다[6]. 그러나 SSS는 누구든 분할 파일을 일정 개수 이상 획득하면 원본 파일을 복구할 수 있으므로 클라이언트뿐만 아니라 공격자도 원본 파일을 복구할 수 있는 문제가 있다[7]. 따라서 본 논문에서는 SSS의 분할 파일 일부를 암호화하여 전달함으로써 공격자의 원본 파일 복구를 방지하는 안전한 FOTA (Secure FOTA, S-FOTA)를 제안한다. 또한 본 논문에서는 채널 상태가 혼잡하면 클라이언트가 파일을 전달받지 못하는 S-FOTA의 한계점을 보완하여 채널 상황에 따라 재전송하는 파일 크기를 조절하여 전송하는 ARQ (Automatic Repeat Request) 기반 적응형 S-FOTA 메커니즘을 제안하고, 종래의 방식과 보안성, 복잡도 및 전송 속도 측면에서 비교 및 분석한다.

본 논문의 주요 기여점은 다음과 같다.

- 경량 IoT를 위한 SSS와 부분 암호화 기반의 무선 펌웨어 업데이트 메커니즘을 제안한다.
- ARQ 기반 적응형 S-FOTA 메커니즘을 활용하여 채널 상황을 고려한 펌웨어 업데이트 메커니즘을 제안한다.
- 종래의 FOTA와 제안하는 S-FOTA, ARQ 기반 적응형 S-FOTA 메커니즘의 보안성과 복잡도 및 전송 속도를 비교하고 분석하는 프레임워크를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 기존의 FOTA와 SSS 기반 선행 연구를 분석한다. 3장에서 제안하는 S-FOTA와 ARQ 기반 적응형 S-FOTA 메커니즘을 설명하고, 4장에서 제안 방식과 종래 방식의 성능을 비교 및 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

무선 IoT의 보안성을 개선하기 위해 다중 인자 공유를 기반으로 하는 연구는 활발하기 진행되고 있다. Abdel Hakeem, S.A. 외 1인은 SSS 및 HMAC (Hash-Based Message Authentication Code)와 기반 임계 공유 비밀 프로토콜을 제안하였다. 본 논문의 제안 방식은 관리자가 비밀 키를 SSS에 기반하여 안전하게 전달하며, 다수의 차량이 그들이 공유받은 정보를 재조합하여 원래의 비밀 키를 복원할 수 있도록 작동한다. 복원된 키는 HMAC을 통해 기밀성을 보장받는다. 그러나 본 논문에서 제안한 방식은 키를 분할한 후 암호화하여 전달하지 않아서 공격자가 분할 키 조각을 일정 개수 이상 탈취하여 복구할 수 있다[8].

Duan, J. 외 2인은 개인 정보 보호를 위한 비밀 공유 기반 분산 학습 프레임워크를 제안하였다. 본 논문의 제안 방식은 비밀 공유를 통해 중간 매개변수를 분할하여 공유하여 효율적으로 개인 정보를 보호한다. 그러나 본 논문은 다수의 공격자가 협력하는 경우를 고려하지 않았다[9].

Subrahmanyam, R. 외 2인은 분산 환경에서의 타원 곡선 기반 비밀 공유 체계를 제안하였다. 본 논문은 타원 곡선 비밀 분배 방식 (Elliptic Curve Secret Sharing Scheme, ECSSS)을 활용한 키 분산 합의 프로토콜을 제안하여 연산의 복잡도를 낮췄다. 그러나 본 논문은 제안 방식과 기존 방식의 소요 시간을 비교하여 분석하지 않았다[10].

이승은 외 2인은 SSS를 활용하여 경량 IoT를 위한 부분 암호화 기반의 S-FOTA 메커니즘을 제안했다. 본 논문의 제안 방식은 펌웨어 파일을 조각으로 분할한 후 부분 암호화하여 다중 경로로 전달함으로써 공격자의 공격으로 인한 펌웨어 파일 유출을 예방할 수 있다. 그러나 본 논문은 채널 상태에 따른 파일 유실률 및 재전송 비용을 고려하지 않았다[7].

G. Kornaros 외 7인은 차량 시스템 대상의 공격 성공률을 낮추기 위한 CAN (Controller Area Network) 기반 차량 보안 메커니즘을 제안하였다. 본 논문은 하드웨어 방화벽과 함께 작동하여 신뢰할 수 있는 무선 펌웨어 업데이트 환경을 구축하였다는 기여점이 있다. 그러나 본 논문은 혼잡한 채널 상태로 인해 통신이 어려운 경우를 고려하지 않았다[11].

Xinchi He 외 3인은 스마트 계약을 통해 펌웨어 업데이트 메커니즘의 무결성을 보장하는 블록체인 기반 FOTA 메커니즘을 제안하였다. 본 논문은 블록체인을 사용하여 FOTA 메커니즘이 하나의 서버가 다수의 기기를 업데이트하는 중앙집중식 구조이므로 발생하는 공격 위협을 줄였다는 기여점이 있다. 그러나 본 논문은 블록체인을 사용하여 경량화된 IoT 환경에 적용하기 어렵다[12].

3. 안전한 무선 펌웨어 업데이트 메커니즘 및 ARQ 기반 적응형 S-FOTA 메커니즘

클라이언트는 SSS를 이용하여 분할 파일을 일정 개수 이상

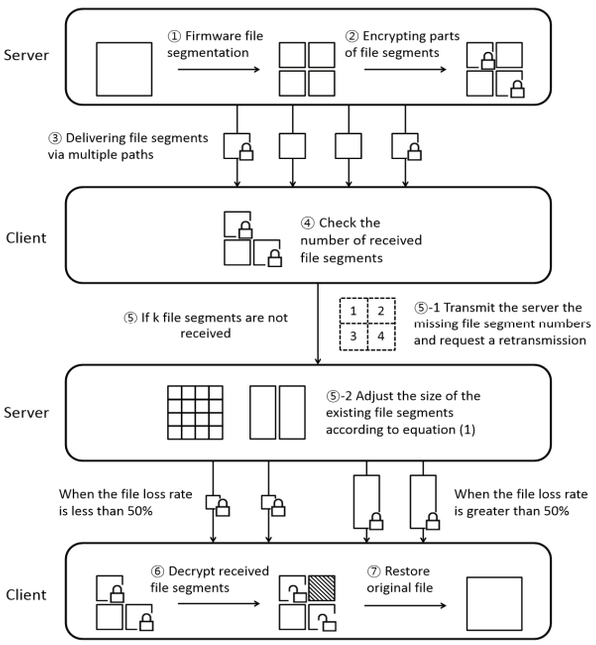

Fig. 1. Operation Process of Adaptive ARQ-Based S-FOTA Mechanism

획득하면 원본 파일을 복구할 수 있다. 그러나 기존의 SSS는 공격자도 클라이언트와 같이 일정 개수 이상의 분할 파일을 획득하면 원본 파일을 복구할 수 있는 문제점이 있다. 따라서 본 연구에서는 서버가 클라이언트에게 펌웨어 분할 파일의 일부를 암호화하여 전달함으로써 공격자가 암호화된 파일을 파일 복구에 사용하지 못하여 원본 파일을 복구할 수 없도록 하는 S-FOTA와, 채널 상황에 따라 재전송 파일 크기를 조절하여 전송하는 ARQ 기반 적응형 S-FOTA 메커니즘을 제안한다.

Fig. 1은 ARQ 기반 적응형 S-FOTA 메커니즘의 동작 과정을 나타낸 것이다. 펌웨어의 업데이트를 위해서, 먼저 서버는 SSS를 이용하여 펌웨어 업데이트 파일을 분할하고, 분할 파일을 부분 암호화한다. 부분 암호화된 분할 파일은 다중 경로를 통해 클라이언트에게 전달된다. 공격자는 부분 암호화된 분할 파일을 복호화하여 원본 파일 복구에 사용하지 못하므로 파일 탈취 공격의 발생 위험이 감소한다. 클라이언트는 전체 분할 파일 n개 중 전달받은 분할 파일의 개수가 원본 파일을 복구하는 데 필요한 k개 이상일 경우 분할 파일 중 부분 암호화된 파일을 복호화하고 원본 파일을 복구한다. k의 범위는 $(0 < k \leq n)$이며, 복구에 필요한 분할 파일 중 한 개라도 전달받지 못하면 펌웨어를 업데이트할 수 없다. 만일 전달 과정에서의 파일 유실로 인해 클라이언트가 k개 이상의 분할 파일을 획득하지 못한다면, 클라이언트는 자신이 받지 못한 파일 조각 번호와 재전송 요청을 서버에게 전송한다. 서버는 클라이언트가 받지 못한 파일 조각 개수를 기반으로 파일 유실률을 계산한다. 본 논문에서는 파일 유실률이 50%인 경우 서버가 기존의 분할 파일과 동일한 크기의 파일을 재전송한다. 서버는 파일 유실률이 50% 미만인 경우 연산 비용을 낮추기 위

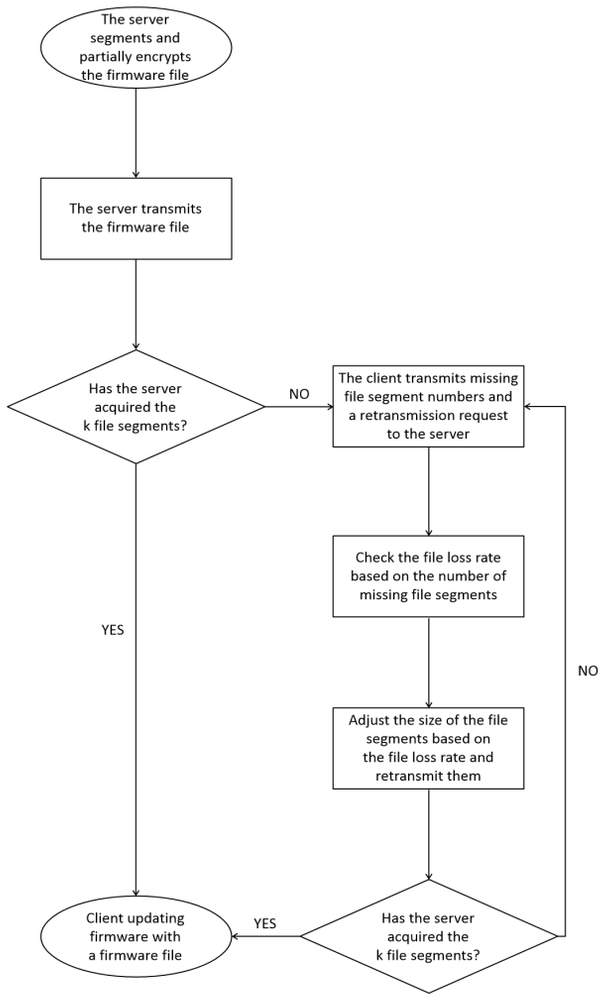

Fig. 2. Flowchart of Adaptive ARQ-Based S-FOTA Mechanism

해 기존의 분할 파일들을 통합하여 재전송 분할 파일 크기를 증가시켜 재전송하며, 파일 유실률이 50%를 초과하는 경우 파일 유실률을 낮추기 위해 클라이언트가 받지 못한 파일을 추가적으로 분할하여 재전송 분할 파일 크기를 줄여서 재전송한다. 예를 들어, 파일 유실률이 0%, 10%, …, 40%인 경우 재전송 시 파일 크기가 기존 분할 파일의 1.8배, 1.6배, …, 1.2배가 되도록 통합하여 전송하며, 파일 유실률이 60%, 70%, …, 90%인 경우 재전송 분할 파일 크기가 기존 분할 파일의 0.8배, 0.6배, …, 0.2배가 되도록 추가적으로 분할하여 전송한다. 파일 유실률이 100%인 경우는 분할 파일 크기에 상관없이 파일 전송이 불가능하므로 고려하지 않았다. 클라이언트는 기존에 전달받았던 분할 파일과 재전송받은 분할 파일 중 암호화된 것을 복호화하고, 전달받은 파일의 개수가 원본 파일 복구에 필요한 k개 이상이라면 원본 파일을 복구한다.

Fig. 2는 ARQ 기반 적응형 S-FOTA 메커니즘의 순서도를 나타낸 것이다. 먼저 서버는 S-FOTA 메커니즘을 이용하여 자신이 전송할 펌웨어 업데이트 파일을 조각으로 분할하고 일부를 부분 암호화한다. 그런 다음 서버는 분할 파일을 다중 경로

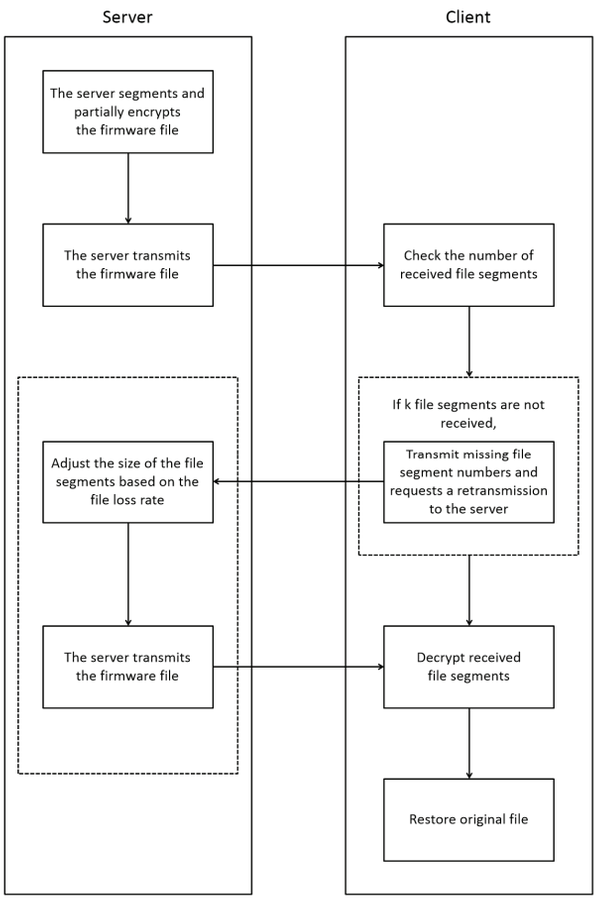

Fig. 3. Diagram of Adaptive ARQ-Based S-FOTA Mechanism

를 통해 클라이언트에게 전달한다. 클라이언트는 전체 분할 파일 n개 중 전달받은 분할 파일의 개수가 k개 이상일 경우 부분 암호화된 분할 파일을 복호화하여 원본 파일을 복구하고, 이를 이용하여 펌웨어를 업데이트한다. 그러나 서버가 클라이언트에게 분할 파일을 전달하는 과정에서 유실이 발생해 클라이언트가 전달받은 분할 파일로 원본 파일을 복구하는 데 실패한다면, 클라이언트는 자신이 전달받지 못한 분할 파일의 번호 정보를 포함한 재전송 요청을 서버에게 전달한다. 서버는 클라이언트가 전달한 미전달 분할 파일 번호의 개수 정보에 기반하여 파일 유실률을 계산하고 파일 크기를 조정한다. 서버는 클라이언트에게 미전달 파일을 다중 경로로 재전송하고, 클라이언트가 원본 파일을 복구할 수 있는 k개 이상의 분할 파일을 획득했을 때 부분 암호화된 파일을 복호화한 후 펌웨어를 업데이트한다. 그러나 클라이언트가 원본 파일 복구에 실패하면 클라이언트는 다시 자신이 전달받지 못한 분할 파일의 번호와 재전송 요청을 서버에게 전달한다.

Fig. 3은 ARQ 기반 적응형 S-FOTA 메커니즘의 다이어그램을 나타낸 것이다. 서버가 펌웨어 업데이트 파일을 분할한 후 부분 암호화하여 다중 경로로 클라이언트에게 전달하면, 클라이언트는 전달받은 분할 파일이 전체 분할 파일 n개 중 k개 이상인지 확인한다. 만일 k개 미만이라면 클라이언트는 전달받지 못한 분할 파일의 번호와 재전송 요청을 서버에게 전달하며, 서버는 클라이언트가 전달받지 못한 분할 파일의 개수를 토대로 파일 유실률을 계산하여 파일의 크기를 조정하여 재전송한다. 만일 클라이언트가 k개 이상의 파일을 획득하면 파일을 복호화하여 펌웨어를 업데이트한다.

4. 성능 평가 및 분석

본 연구는 FOTA 업데이트 환경을 모델링하고 실험하여 S-FOTA와 적응형 S-FOTA 파일 재전송 메커니즘의 성능을 비교 및 평가하였다. S-FOTA는 암호화 및 복호화 시 경량 암호 알고리즘인 LEA (Lightweight Encryption Algorithm)-128을 사용하였다. 모든 ARQ 메커니즘은 공격으로 인한 파일 유실을 고려하지 않기 위해 재전송 시 모든 분할 파일을 암호화하여 전달하였다.

Fig. 4는 기존의 SSS를 기반으로 하는 FOTA와 암호화된 분할 파일의 수가 20개, 40개, 60개인 S-FOTA의 공격자 수에 따른 공격 성공률을 비교한 실험 결과이다. 공격자의 공격 성공률은 공격자가 분할 파일을 탈취하여 원본 파일 복구에 성공하였을 확률이다. 실험에서는 원본 펌웨어 업데이트 파일을 총 100개의 분할 파일로 분할하였으며, 40개의 분할 파일을 획득했을 때 원본 파일을 복구할 수 있다. 실험 결과에 따르면, 기존의 SSS 기반 FOTA는 공격 성공률이 가장 높았다. 암호화 파일이 20개인 S-FOTA는 공격자 수가 40 미만일 때 공격 성공률이 0%이며, 40 이상일 때 기존의 FOTA 대비 공격 성공률이 최소 1.39% 최대 99.78% 감소했다. 또한 암호화 파일이 40개인 S-FOTA는 공격자 수가 50 미만일 때 공격 성공률이 0%이고, 50 이상일 때 기존의 FOTA 대비 공격자 공격 성공률이 최소 62.58%, 최대 99.99%로 감소했으며, 암호화

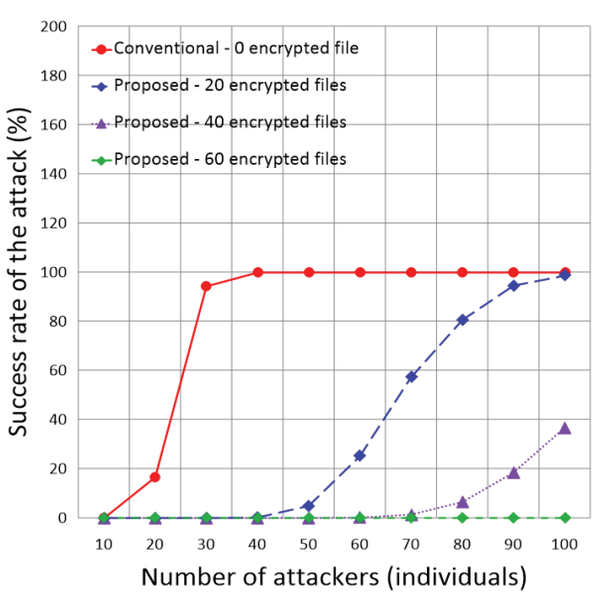

Fig. 4. Attack Success Rate based on Number of Attackers

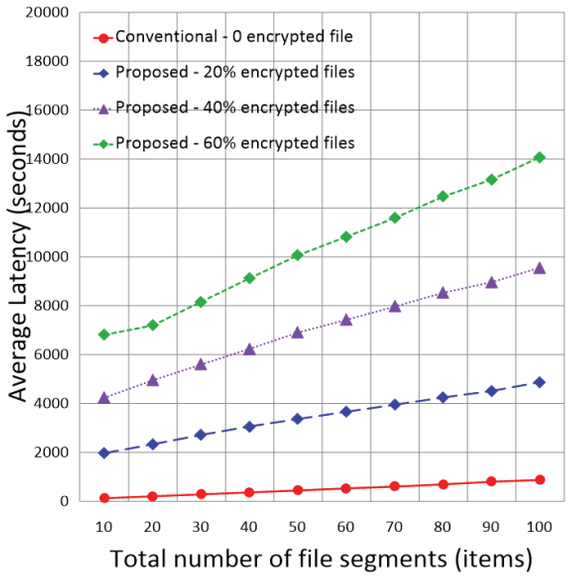

Fig. 5. Average Time Taken by Total Number of File Segments

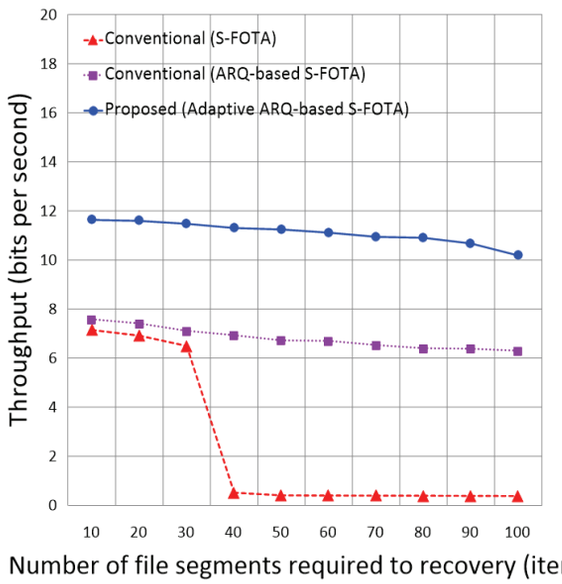

Fig. 6. Throughput Based on the Number of File Segments Required to Recover the Original File

파일이 60개인 S-FOTA는 공격자 공격 성공률을 100% 감소시켰다. 실험을 통해 S-FOTA는 원본 펌웨어 업데이트 파일을 부분 암호화하여 다중 경로로 전달하므로 기존의 FOTA 대비 공격 성공률이 낮아져서 보안이 개선됨을 확인했다.

Fig. 5는 기존의 FOTA와 암호화된 분할 파일의 수가 전체 분할 파일 수의 20%, 40%, 60%인 S-FOTA의 전체 분할 파일 수에 따른 평균 소요 시간을 비교한 그래프이다. 평균 소요 시간은 클라이언트가 서버로부터 파일을 전달받아 원본 파일을 획득하기까지 걸리는 시간이다. 실험 결과에 따르면 암호화된 분할 파일의 수가 전체 분할 파일 수의 20%인 S-FOTA는 기존의 FOTA 대비 평균 소요 시간이 최소 457.54%, 최대 1504.36% 더 걸렸으며, 암호화된 분할 파일의 수가 전체 분할 파일 수의 40%인 S-FOTA는 최소 996.39%, 최대 3374.99% 더 걸렸다. 또한 암호화된 분할 파일의 수가 전체 분할 파일의 60%인 S-FOTA는 기존의 FOTA 대비 평균 소요 시간이 1514.75%, 최대 5484.27% 더 걸렸다. 실험 결과를 통해 제안하는 S-FOTA는 펌웨어 업데이트 파일을 분할하고 부분 암호화하여 다중 경로로 전달하고, 원본 파일을 복구하는 과정에서 기존의 FOTA보다 시간이 더 소요됨을 확인하였다. 또한 암호화 파일의 수가 많을수록 암호화 및 복호화를 위한 평균 소요 시간이 증가했다.

Fig. 6은 S-FOTA와 기존의 ARQ 메커니즘, 제안하는 ARQ 기반 적응형 S-FOTA 메커니즘의 전송 속도를 비교한 실험 결과이다. 실험에서는 원본 펌웨어 업데이트 파일을 총 100개의 파일로 분할하였으며, 전송 과정에서 60%의 파일이 유실된다. 기존의 ARQ 메커니즘은 재전송할 때 기존에 분할했던 파일 크기와 동일한 크기의 파일을 재전송하며, ARQ 기반 적응형 S-FOTA 메커니즘은 파일 유실률이 50%인 경우를 기준으로 분할 파일의 분할 및 통합 여부를 결정한다. ARQ 기반 적응형 S-FOTA 메커니즘은 파일 유실률이 크다면 파일을 추가적으로 분할하고, 낮을 경우 파일을 통합하여 재전송하며, 파일 유실률이 50%인 경우 기존 분할 파일과 동일한 크기의 파일을 재전송한다. 실험 결과에 따르면, ARQ 기반 적응형 S-FOTA 메커니즘은 기존의 S-FOTA 대비 전송 속도가 최소 63.16%, 최대 2736.36% 더 높았다. 또한 ARQ 기반 적응형 S-FOTA 메커니즘은 기존의 ARQ 메커니즘 대비 전송 속도가 최소 53.89%, 최대 70.89% 더 높았다. 실험을 통해 재전송이 과정이 있는 메커니즘이 기존의 S-FOTA보다 원본 파일 복구 성공률이 높아 전송 속도가 높음을 확인하였으며, ARQ 기반 적응형 S-FOTA 메커니즘은 파일 유실률에 따라 재전송 분할 파일 크기를 조절하여 기존의 ARQ 메커니즘보다 전송 속도가 높음을 확인하였다.

5. 결 론

최근 사물인터넷이 일상생활과 산업에 널리 활용되면서 IoT 펌웨어 업데이트 메커니즘의 보안의 중요성이 강조되고 있다. IoT 펌웨어 업데이트 메커니즘으로 널리 활용되는 기존의 FOTA는 단일 경로를 활용하여 펌웨어를 업데이트하므로 파일 탈취 공격에 취약하다는 한계점이 있다. 따라서 본 논문에서는 펌웨어 파일을 조각으로 분할하여 부분 암호화한 후 다중 경로로 전달하는 S-FOTA와 클라이언트가 받지 못한 분할 파일을 채널 상태에 따라 파일 크기를 조절하여 전달하는 ARQ 기반 적응형 S-FOTA 메커니즘을 제안하였다. 실험 결과에 따르면 암호화 파일의 수가 40개인 S-FOTA는 공격 성공률을 최소 62.58%, 최대 99.99% 감소시켰으며, 암호화된 분할 파일의 수가 전체 분할 파일 수의 40%인 S-FOTA는 기존의 FOTA 대비 평균 소요 시간이 최소 996.39%, 최대 3374.99% 더 소요되었다. ARQ 기반 적응형 S-FOTA 메커니

즘의 전송 속도는 기존의 S-FOTA 대비 최소 63.16%, 최대 2736.36% 더 높았으며, 기존의 ARQ 메커니즘 대비 최소 53.89%, 최대 70.89% 더 높았다. 향후 연구에서는 채널 상태와 악의적인 공격자를 함께 고려하여 ARQ 메커니즘의 보안성을 높일 방법을 제안하고, 테스트베드를 구축하여 실험할 계획이다.

References

[1] S. El Jaouhari and E. Bouvet, "Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions," *Internet of Things*, Vol.18, 2022.

[2] J.-M. Lee, S.-Y. Kim, and I.-G. Lee, "Lightweight AES-based Whitebox Cryptography for Secure Internet of Things," *Journal of the Korea Institute of Informaiton and Communication Engineering (JKIICE)*, Vol.26, No.9, pp.1382-1391, 2022.

[3] S.-E. Joen, Y.-S. Oh, Y.-J. Lee, and I.-G. Lee, "Suboptimal Feature Selection Techniques for Effective Malicious Traffic Detection on Lightweight Devices," *Computer Modeling in Engineering & Sciences*, Vol.140, No.2, pp.1-19, 2024.

[4] T. Mirfakhraie, G. Vitor, and K. Grogan, "Applicable Protocol for Updating Firmware of Automotive HVAC Electronic Control Units (ECUs) Over the Air," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber*, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp.21-26, 2018.

[5] H. A. Odat and S. Ganesan, "Firmware over the air for automotive, Fotamotive," *IEEE International Conference on Electro/Information Technology*, *Milwaukee*, WI, USA, pp.130-139, 2014.

[6] A. Shamir, "How to share a secret," *Communications of the ACM*, Vol.22, No.11, pp.612-613, 1979.

[7] S.-E. Lee, J.-M. Lee, and I.-G. Lee, "Secure FOTA Update Mechanism for Lightweight IoT," *Proceedings of the Annual Symposium of Korea Information Processing Society Conference (KIPS) 2024*, Vol.31, pp.288-289, 2024.

[8] S. A. Abdel Hakeem and H. Kim, "Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication," *Sensors*, Vol.22, No.1,331, 2022.

[9] J. Duan, J. Zhou, and Y. Li, "Privacy-Preserving distributed deep learning based on secret sharing," *Information Sciences*, Vol.527, pp.108-127, 2020.

[10] R. Subrahmanyam, N. R. Rekha, and Y. V. S. Rao, "Authenticated Distributed Group Key Agreement Protocol Using Elliptic Curve Secret Sharing Scheme," *IEEE Access*, Vol.11, pp.45243-45254, 2023.

[11] G. Kornaros et al., "Towards holistic secure networking in connected vehicles through securing CAN-bus communication and firmware-over-the-air updating," *Journal of Systems Architecture*, Vol.109, 2020.

[12] X. He, S. Alqahtani, R. Gamble, and M. Papa, "Securing Over-The-Air IoT Firmware Updates using Blockchain," *Proceedings of the International Conference on Omni-Layer Intelligent Systems*, pp.164-171, 2019.

이 승 은

https://orcid.org/0009-0001-9706-4718
e-mail : rose6825@gmail.com
2022년 ~ 현 재 성신여자대학교 융합보안공학과 학사과정
관심분야 : Network, Vulnerability Analysis, and Penetration Testing

이 진 민

https://orcid.org/0000-0002-4337-1771
e-mail : 220237019@sungshin.ac.kr
2021년 성신여자대학교 융합보안공학과 (학사)
2023년 성신여자대학교 미래융합기술공학과 (석사)
2023년 ~ 현 재 성신여자대학교 미래융합기술공학과 박사과정
관심분야 : Communications, Network, and Security, Intelligence/security embedded IoT systems, Deep Learning/Machine Learning

이 일 구

https://orcid.org/0000-0002-5777-4029
e-mail : iglee@sungshin.ac.kr
2003년 서강대학교 전자공학(학사)
2005년 KAIST 정보통신(석사)
2016년 KAIST 전산학부(박사)
2005년 ~ 2017년 한국전자통신 연구원 선임연구원
2017년 ~ 현 재 성신여자대학교 융합보안공학과·미래융합기술공학과 교수
관심분야 : Convergence Security, Information Security, Wireless networks and Communication