ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 19-02-46
310

j.inst.Korean.electr.electron.eng.Vol.23,No.2,659~666,June 2019
http://dx.doi.org/10.7471/ikeee.2019.23.2.659

시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 방안

A Simulation-based Analysis and Verification Method for Network Vulnerability

이 현 진*★, 김 광 희*, 이 행 호**

Hyun-Jin Lee*★, Kwang-hee Kim*, Haeng-Ho Lee**

Abstract

MANET can be applied to various applications as it can autonomously configure the network with only mobile nodes. However, the network can be vulnerable to cyber attacks because it is organized in a distributed environment without central control or management. In this paper, we propose a simulation-based network security vulnerability analysis and verification method. Using this method, we simulated the routing message modification attack, Sybil node attack, and TLV message modification attack that may frequently occur in MANET, and confirmed that similar vulnerabilities can be occurred in the real system. Therefore, the proposed method can be used to improve the accuracy of the protocol design by verifying possible security vulnerabilities through simulation during the protocol design procedure.

요 약

MANET은 이동 노드들로 망을 자율적으로 구성할 수 있어 다양한 응용에서 적용되고 있다. 그러나 중앙의 제어나 관리 없이 분산 환경으로 망을 구성하여 사이버 공격에 취약할 수 있다. 본 논문에서는 시뮬레이션 환경에서 MANET 보안 취약점을 분석하고 검증할 수 있는 방안을 제안한다. 또한, 제안하는 방안을 적용하여 MANET에서 빈번하게 발생할 수 있는 라우팅 메시지 변조 공격, 거짓 노드 공격, TLV 메시지 변조 공격에 대하여 모의하고, 실 시스템에서도 유사한 취약점이 발생함을 확인하였다. 따라서 제안하는 방안은 사이버 공격자에 의해 발생 가능한 보안 취약점을 통신망 기술을 설계하는 과정에서 시뮬레이션을 통하여 검증함으로써 통신 기술 설계 정확도를 향상시키는데 활용될 것으로 예상된다.

Key words : Simulation, Vulnerability, Cyber Security, MANET, Network Security

Ⅰ 서론

MANET(Mobile Ad-Hoc NETwork)은 개방된 매체를 이용하여 이동이 가능한 환경에서 단말간 분산 제어를 통해 자율적으로 망을 구성할 수 있다. 이와 같은 특징으로 MANET 기술은 이동이 적은 센서망이나 IoT(Internet of Thing)망 뿐만 아니라 이동이 빈번한 군집드론(Spawn drone)망, 차량간통신(V2V; Vehicle-to-Vehicle)망에서도 적용되고 있다.

사이버 공격자는 MANET의 이러한 특징을 이용하여 MANET에서 사용되는 기술의 규격에 대한 지식만 가지고 있다면, 망에 쉽게 접근하여 라우팅 오작동 공격, 자원 잠식 공격, 제어 메시지 오작동

* Solvit System
** Agency for Defense Development
★ Corresponding author
E-mail : L33hyun@solvitsystem.co.kr, Tel : +82-2-6241-6667
※ Acknowledgment
Manuscript received Jun. 5, 2019; revised Jun. 19, 2019; accepted Jun. 27, 2019.

에 의한 공격 등을 야기할 수 있다. 특히, IoT는 비교적 단순한 기능을 가진 다수의 단말들이 Ad-Hoc으로 망을 구성할 수 있어 사이버 공격에 쉽게 노출될 수 있다[1]. 특히, 한국인터넷진흥원의 조사에 따르면 IoT 공격 사례가 급격히 증가하고 있으며, 2019년에는 IoT를 겨냥한 사이버 위협이 7대 사이버 공격에 포함될 것으로 예상하고 있다. 따라서 IoT를 이루는 MANET망에서의 사이버 보안은 매우 중요한 이슈이다.

MANET의 보안 취약점을 제거하기 위하여 다양한 기술들이 제안되고 있고 규격화가 진행되고 있다[3-5]. 그러나 MANET 기술을 설계하는 시점에 발생 가능한 취약점을 식별하고 검증하는 것이 어렵다는 한계가 있다. 따라서 대다수의 사례에서는 실제 사이버 침해가 발생한 후에 대응 기술을 추가 개발하여 보완하는 방향으로 접근하고 있다.

본 논문에서는 위와 같은 한계를 극복하기 위하여 사이버 공격이 발생하기 이전 기술을 설계하는 시점에 시뮬레이션을 통하여 발생 가능한 사이버 공격을 식별하고, 해당 사이버 공격이 발생했을 때 단말 또는 네트워크에 야기되는 문제를 검증할 수 있는 방안을 제안하고자 한다. 제안하는 시뮬레이션 기반의 보안 취약점 식별 및 검증 방안은 통신망 분석 시뮬레이터인 Riverbed Modeler를 기반으로 개발하였다[6].

그림 1은 제안하는 시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 도구의 운용 개념을 나타내고 있다. 먼저 분석대상 MANET 환경에서 단말을 배치하고 단말간에 메시지를 송수신하는 것을 모의한 후, 메시지 송수신 결과를 DB에 저장한다. 그 후 취약점 분석 운용 도구를 이용하여 사이버 공격 의도에 따라 DB에 저장되어 있는 메시지 중 일부를 변조시킨다. 마지막으로 동일한 MANET 환경에서 변조된 메시지를 단말간에 교환함으로써 사이버 공격에 취약할 가능성을 확인하고 이에 따른 네트워크 및 단말의 효과를 검증한다.

제안하는 시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 도구는 MANET 기술 개발 간에 다음과 같이 활용이 가능할 것으로 예상된다.

- 설계 단계 : 프로토콜 또는 운용 개념 상 발생할 수 있는 취약점 후보군을 시뮬레이션을 통하여 식별하여 설계에 반영

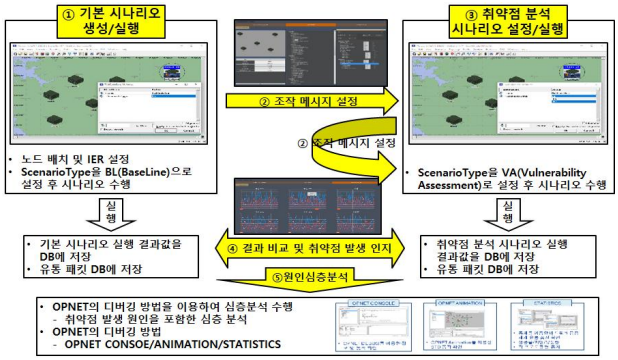

Fig. 1. The simulation-based network security vulnerability analysis and validation concepts.

그림 1. 시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 개념

- 구현 단계 : 취약점 발생 가능성이 높은 알고리즘에 대한 정보를 전달하여 취약점 방어가 가능하게 지원
- 시험 단계 : 시뮬레이션을 통하여 식별된 취약점에 대한 시험을 통하여 프로토콜의 안정성 향상

본 논문의 구성은 다음과 같다. 2장에서는 MANET에서 발생할 수 있는 사이버 공격 유형에 대하여 기술하고 3장에서는 제안하는 시뮬레이션 기반 취약점 분석 방안에 대하여 설명한다. 4장에서는 제안하는 방안을 활용하여 MANET의 대표적인 사이버 공격 유형 별 효과를 모의하고 유사한 공격을 실제 시스템에서 발생시켰을 경우의 결과와 비교 검증하여 제안하는 방안의 효용성을 확인하고 5장에서 결론을 맺는다.

II. 관련 연구

MANET에서 발생 가능한 사이버 공격은 통신 계층 별로 다음과 같다[7-9]. 응용 계층 공격은 일반적인 사이버 공격과 유사하므로 본 논문에서 추가적으로 언급하지는 않는다.

- 물리계층
  - 재밍(Jamming) 공격 : 물리적으로 통신을 마비시키는 공격
  - 조작(Tampering) 공격 : 하드웨어 탈취 후 내부 정보를 탈취하거나 시스템을 변조시키는 공격
- 데이터링크 계층
  - 정보 탈취 공격 : 프로토콜이 사용하는 시스템

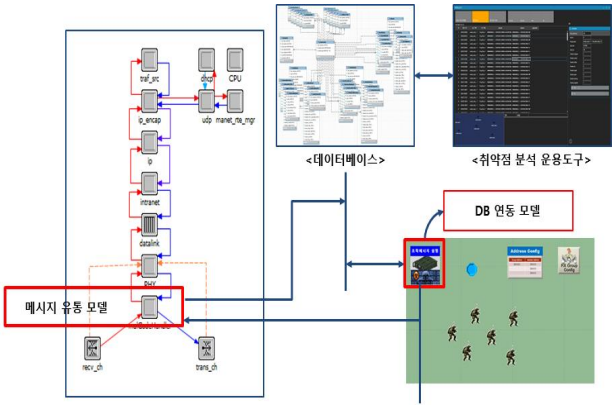

Fig. 2. DB interworking model workflow.
그림 2. DB 연동 모델 동작 흐름도

자원의 한계를 이용하여 대상 단말의 정보를 탈취하거나 파기하는 공격으로 ARP Spoofing, MAC Flooding, Port Stealing 공격 등이 이에 속함

- 도청(Eavesdropping) : 무선 네트워크에 돌아다니는 패킷의 내용으로 감추어진 정보를 획득하는 공격
- 서비스 거부 : 무선 링크의 자원을 잠식하여 통신을 마비시키는 공격

• 네트워크 계층

- 서비스 거부 공격 : 무선 링크의 비대칭성을 이용하여 네트워크에 혼란을 야기하는 공격으로 Hello Flooding, Routing Table Poisoning, Ping of Death, Smurf 공격 등이 있음
- 거짓 경로 공격 : 라우팅 정보를 변조시켜서 정보를 파기하거나 탈취하는 공격으로 Wromhole, Sinkhole, Grayhole 공격 등이 있음
- 시빌(Sybil) 공격 : 공격 단말이 다수의 거짓 단말을 생성하여 네트워크에 잘못된 정보를 보내는 공격
- 위치 공개 공격 : 공격 단말이 트래픽 분석 등과 같은 방법을 통하여 네트워크의 구조나 특정 노드의 위치를 탐색하는 공격
- 스푸핑 공격 : 인증된 IP 주소를 획득하여 대상 단말에 침투하는 공격

• 전송 계층

- 세션 탈취 공격 : 설정된 세션의 IP 주소와 시퀀스 번호를 탈취하여 특정 세션을 훔치는 공격
- 서비스 거부 공격 : TCP 세션의 논리적인 자원을 잠식하여 네트워크를 마비시키는 공격

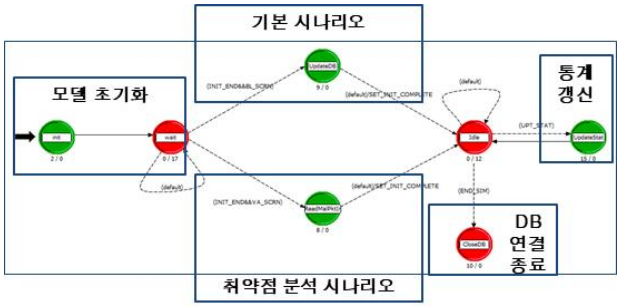

Fig. 3. State diagram of DB interworking model.
그림 3. DB 연동 모델의 상태 천이도

III. 시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 방안

본 논문에서 제안하는 시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 방안은 DB 연동 모델, 메시지 유통 모델, 취약점 분석 운용 도구로 구성된다. 다음은 개별 기능에 대한 상세 기능을 기술하고 있다.

1. DB 연동 모델

그림 2는 DB 연동 모델의 동작흐름도를 나타내고 있다. DB 연동 모델은 크게 3개의 기능을 수행한다. 첫 번째는 기본 시나리오에 대한 시뮬레이션을 수행할 때, 시나리오 이름과 망을 구성하고 있는 노드의 정보를 수집하는 기능이다. 두 번째는 취약점 분석 시나리오에서 DB에 저장된 조작된 메시지를 획득하여 메시지 유통 모델로 전달하는 기능이다. 마지막으로 시뮬레이션 결과를 수집하여 DB에 저장하는 기능이다.

그림 3은 DB 연동 모델의 상태 천이도를 나타내고 있다. 모델 초기화 상태에서는 DB 연동 세션을 연결하고 시나리오 유형을 식별한다. 기본 시나리오 처리 상태에서는 시나리오 정보와 단말 정보를 DB에 저장한다. 취약점 분석 시나리오 처리 상태에서는 계층 별 조작 메시지 정보를 수집하여 메시지 유형 별로 시뮬레이터 내부 패킷 테이블에 저장한다. 통계 갱신 상태에서는 각 계층 별 시뮬레이션 결과를 DB에 저장하며 DB 연결 종료 상태에서는 프로세스 종료 시 DB 연결을 해제하는 기능을 수행한다.

2. 메시지 유통 모델

메시지 유통모델은 시나리오 종류에 따라 취약점

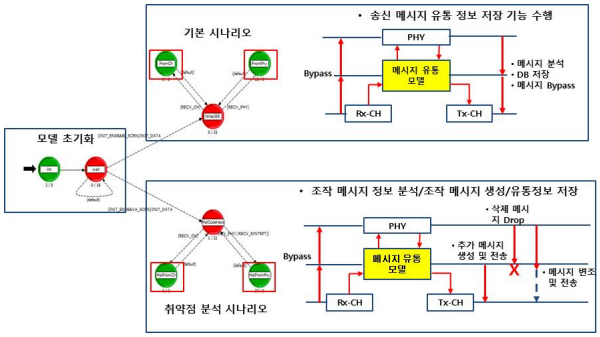

Fig. 4. Procedure for message transmission model according to the scenario type.
그림 4. 시나리오 유형에 따른 메시지 유통 모델의 수행 절차

분석 운용도구에서 유통되는 메시지에 대한 처리 기능을 제공하는 모델로 그림 4와 같이 시나리오 유형에 따른 메시지 처리를 수행한다.

시뮬레이션을 수행하면 시나리오의 유형을 식별하고 모델 상태를 초기화한다. 하위계층으로부터 수신된 메시지는 시나리오 유형에 무관하게 상위계층으로 바로 전달한다. 그러나 상위계층으로부터 전달된 메시지는 시나리오 유형에 따라 다른 절차를 수행한다. 기본 시나리오에서는 전달된 메시지를 통신 계층별로 메시지의 필드 값을 추출하여 취약점 분석 DB의 송신 패킷 정보 테이블로 전달한다. 만약 취약점 분석 시나리오일 경우 패킷에 대한 식별자를 생성한 후 DB 연동 모델에 의해 생성된 패킷 테이블을 검색한다. 검색에 실패할 경우 하위 계층으로 바로 전달하고, 검색에 성공하면 해당 메시지의 조작 필드를 식별하여 해당 필드에 명시된 조작을 수행한 후 전송한다.

그림 5는 메시지 유통 모델의 상태 천이도를 나타내고 있다.

3. 취약점 분석 운용 도구

취약점 분석 운용 도구의 주 기능은 정상 시나리오에서 유통된 메시지 정보를 기반으로 메시지를 추가하거나 수정, 삭제하는 것이다.

그림 6은 취약점 분석 운용 도구의 화면 구성을 나타내고 있다. ①은 취약점 분석 운용 도구의 메뉴로 메시지 조작, 분석 결과 가시화, 시나리오 불러오기, 시나리오 저장 등의 기능을 선택할 수 있다. ②는 메시지 목록을 도시화하는 화면으로 조작된 메시지 상태, 메시지 ID, 메시지 발생 시간, 메시지 송신 노드 및 수신 노드, 통신 계층 별 정보를

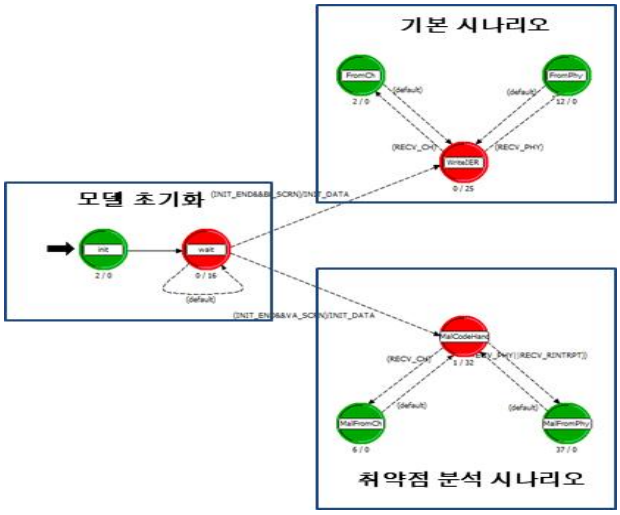

Fig. 5. State diagram of message transmission model.
그림 5. 메시지 유통 모델 상태 천이도

Table 1. Features per states for message transmission model.
표 1. 메시지 유통 모델 상태 별 특징

Process	내용
모델 초기화	• 프로세스 시작 및 파라미터 초기화 수행
기본 시나리오	• 하위 계층으로부터 수신한 패킷은 상위계층으로 전달 • 상위계층으로부터 수신한 패킷은 패킷에 대한 식별자를 생성하고 패킷의 계층 별 필드값을 추출하여 송신 패킷 정보 테이블에 저장
취약점 분석 시나리오	• 하위 계층으로부터 수신한 패킷은 상위계층으로 전달 • 상위계층으로부터 수신한 패킷은 송신 패킷의 ID를 생성한 후 DB 연동 모델에 의해 생성된 패킷 테이블을 검색 • 패킷 테이블 검색 결과 실패하거나 '변경'없음'의 경우 해당 패킷을 하위 계층으로 전달 • '추가' 및 '순서변경'으로 검색될 경우, 해당 패킷 정보 및 계층 별 필드 정보를 이용하여 패킷을 생성/삭제하고 하위 계층으로 패킷 전송

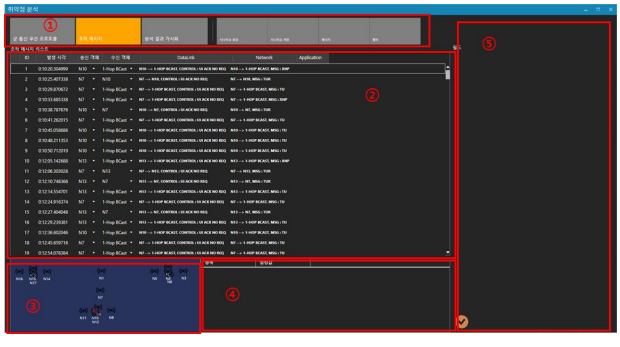

Fig. 6. Screen configuration of vulnerability analysis tool.
그림 6. 취약점 분석 운용 도구의 화면 구성

확인할 수 있다. ③은 노드 맵을 나타내는 화면으로 모든 노드의 상대 위치와 현재 선택된 메시지의 송/수신 노드를 가시화한다. ④는 노드 맵에서 선

택된 노드의 상세 정보를 도시하는 화면이다. ⑤는 메시지 목록에서 선택된 메시지의 세부 정보를 도시화하는 화면으로 계층 별 메시지 필드를 수정하는데 사용된다.

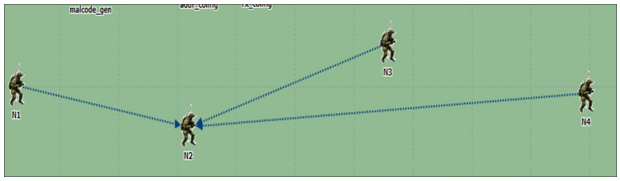

Fig. 7. Network topology for validating cyber attacks in MANET.
그림 7. MANET에서 사이버 공격 유효성 평가를 위한 네트워크 토폴로지

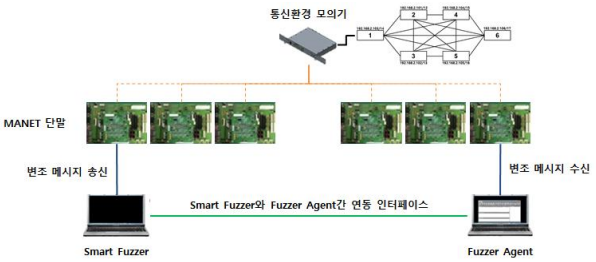

Fig. 8. Testbed configuration for cyber attacks verification.
그림 8. 사이버 공격 검증을 위한 테스트베드 구성

Ⅳ. 취약점 분석 결과

시뮬레이션 기반 취약점 분석 도구를 활용하여 MANET 환경에서 라우팅 정보 변조를 통한 서비스 거부 공격, Sybil 노드에 의한 라우팅 오동작 공격[9], TLV 메시지의 Length 필드 변조를 통한 호스트 오동작 공격의 공격[10]을 모의하였으며, 실시스템으로 구성된 테스트베드에서 해당 공격의 유효성을 검증하였다.

공격을 모의한 절차는 다음과 같다. 먼저 기본 시나리오에서 시뮬레이션을 수행하면서 송수신된 모든 패킷을 DB에 저장한다. 그리고 취약점 분석 운용 도구를 통해 송수신된 패킷 중 일부를 공격 유형에 따라 변조한 후 변조 시나리오로 시뮬레이션을 재수행한다. 이 경우, 메시지 유통 모델은 송수신되는 모든 패킷을 식별한 후 변조된 패킷이 존재할 경우 원 패킷 대신 변조된 패킷을 송수신함으로써 공격의 모의한다.

시뮬레이션 기반 취약점 분석 도구를 활용한 공격 유효성 확인은 그림 7과 같이 3홉으로 구성된 환경에서 수행하였다. 그리고 테스트베드는 그림 8

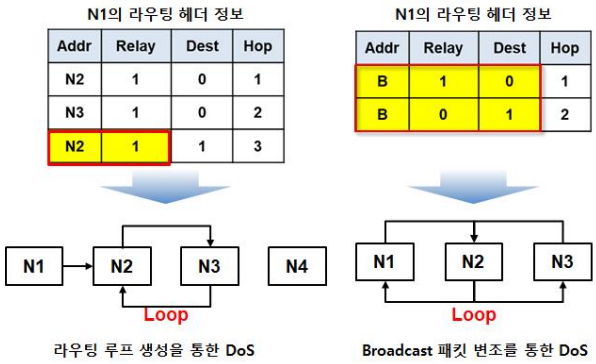

Fig. 9. Modifying routing information for denial of service attack.
그림 9. 서비스 거부 공격을 위한 라우팅 정보 변조

과 같이 6대의 MANET 단말을 망 구성 모의기에 연결하여 토폴로지를 구성한 후, 2대의 MANET 단말에 각각 Smart Fuzzer와 Fuzzer Agent를 연결하여 변조된 메시지를 송수신할 수 있도록 구성하였다.

1. 라우팅 정보 변조에 의한 서비스 거부 공격

서비스 거부 공격은 공격자 단말이 MANET 망에 등록되어 있는 다른 단말의 통신 기회를 박탈하여 연결을 단절시키는 공격 유형으로 라우팅 메시지 변조 공격과 매체 접근 거부 공격이 있을 수 있다. 특히, Source based Routing을 수행하는 경우 그림 9과 같이 Broadcast 패킷의 라우팅 정보를 변조하여 전송할 경우 전체 망에 대한 서비스 거부를 야기할 수 있으며 본 논문에서는 해당 공격 유형을 모의하였다.

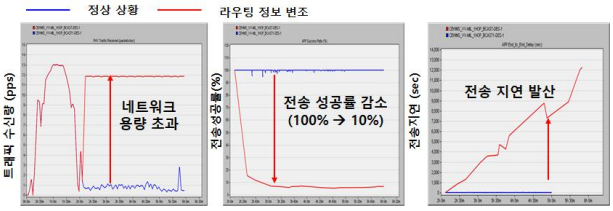

Fig. 10. Simulation results when the routing information of the broadcasting packet is modified.
그림 10. Broadcast 패킷의 라우팅 정보가 변조되었을 때의 모의 결과

그림 10는 Broadcast 패킷의 라우팅 정보 변조 유무에 따른 네트워크 전체의 트래픽 수신량, 전송 성공률, 전송 지연을 각각 나타내고 있다. 파란선과 빨간선은 각각 정상 상태와 공격 상태의 모의 결과

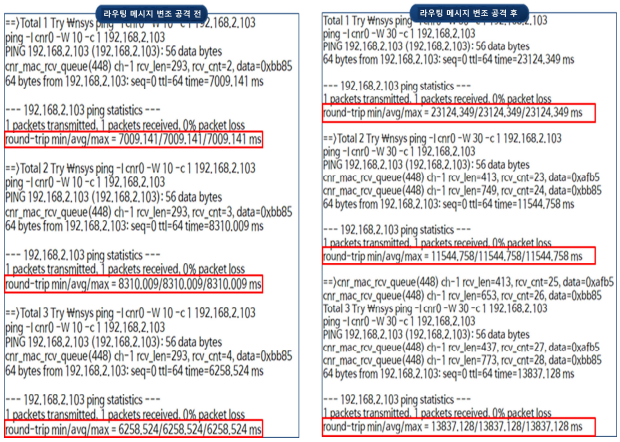

Fig. 11. RTT value according to the routing message modification attack at the testbed.
그림 11. 테스트베드에서 라우팅 메시지 변조 공격 따른 RTT 값

이다. 정상 상황에서는 부하, 지연, 전송성공률 측면에서 모두 안정적으로 유지되는 것을 확인할 수 있다. 그러나 라우팅 변조 공격시 네트워크 용량을 초과할 정도로 트래픽이 증가하여 전송 성공률이 10% 이하로 감소하고 전송에 성공한 패킷의 전송 지연도 발산하는 것을 확인할 수 있다.

테스트베드에서는 라우팅 메시지 변조를 통한 서비스 거부 공격의 유효성을 분석하기 위하여 3개의 단말이 1홉으로 구성된 환경에서 시험하였다. 그림 11은 공격 전 후 RTT(Round-Trip Time)의 변화를 나타내고 있다. 라우팅 변조 공격시 RTT가 2.24배 증가하는 것을 통하여 라우팅 메시지 변조를 통한 서비스 거부 공격이 가능함을 확인할 수 있다.

2. Sybil 노드에 의한 라우팅 오동작 공격

Sybil 노드에 의한 라우팅 오동작 공격은 망 정보 교환시 존재하지 않거나 존재하나 연결이 불가능한 노드의 정보를 전달함으로써 네트워크 토폴로지 구성을 오해하도록 만들어 통신이 불가능하게 하거나, 라우팅 테이블 구성 자체를 못하도록 하여 시스템을 마비시키는 공격 유형이다.

그림 12와 같이 N4 노드부터 N1 노드까지 1열로 구성되어 있을 때, N2 노드가 N1 노드에게 N3의 홉 수가 N4와 동일하게 2홉이고 이전 노드가 N4라고 잘못된 정보를 전달하면 N1은 라우팅 테이블을 구성할 때, N3의 이전 홉은 N4이고, N4의 이전 홉은 N3가 되어 라우팅 테이블 구성이 불가능하게

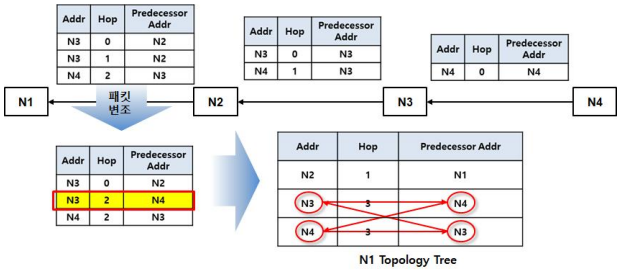

Fig. 12. Example of routing malfunction attack by a Sybil node.
그림 12. Sybil 노드에 의한 라우팅 오동작 공격의 예시

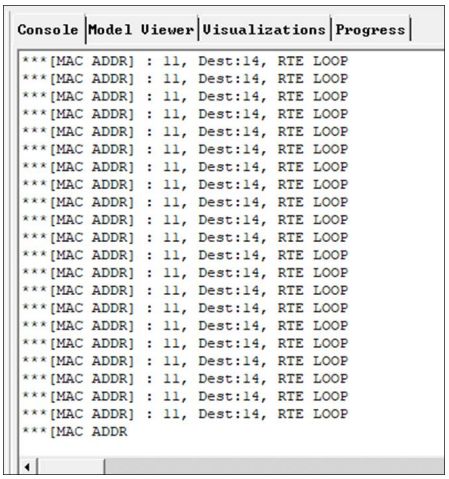

Fig. 13. Status of N1 node when Sybil node attack.
그림 13.거짓 노드 공격을 받았을 때 N1 노드의 상태

된다. 모의 결과 N1 노드는 라우팅 테이블 시 그림 13와 같이 무한 루프에 걸려 시뮬레이션이 더 이상 진행되지 않았다.

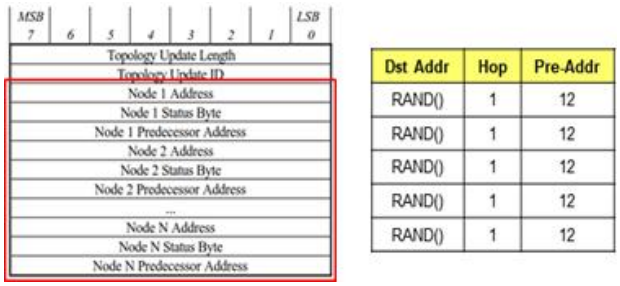

Fig. 14. Topology information sent by N2 node to N1 node for a Sybil node attack in a testbed environments.
그림 14. 테스트베드 환경에서 Sybil 노드 공격을 위해 N2 노드가 N1 노드로 전송한 토폴로지 정보

테스트베드에서도 4개의 노드를 일렬로 구성한 후 N2 노드에서 그림 14과 같이 구성하여 주기적으로 전달한 후 N1 노드의 상태를 확인하였다. 시

스템 로그 기록 확인 결과 N1 노드의 라우팅 테이블 크기가 그림 15과 같이 기하급수적으로 증가하였으며 최종적으로 시스템에 치명적인 에러가 발생하여 시스템이 재부팅되는 결과를 야기하였다.

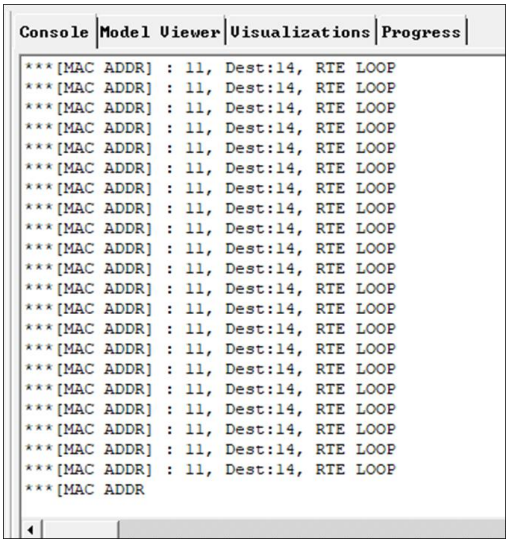

Fig. 15. Status of N1 node when Sybil node attack performed.
그림 15. Sybil 노드 공격이 수행되었을 때의 N1노드의 상태

3. TLV 메시지의 Length 필드 변조를 통한 SW 오동작 유도 공격

MANET 통신망에서 사용하는 많은 제어 프로토콜들은 메시지의 크기를 감소시키기 위하여 필요한 정보에 따라 메시지의 길이를 가변시킬 수 있는 TLV(Type-Length-Value) 형태를 많이 사용한다. 본 논문에서는 시뮬레이션 기반 취약점 분석 도구를 이용하여 가변 길이의 제어메시지를 전송할 때 Length 필드 값을 변조하여 이를 수신한 노드가 해당 메시지를 잘못 해석하도록 유도하여 시스템 오동작을 유도하는 공격에 대하여 모의하였다. 공격 대상 프로토콜은 MANET 망의 라우팅 프로토콜의 제어메시지였으며 공격 결과 그림 16과 같이 메시지 미 해석으로 인한 에러 및 시뮬레이션 중단이 발생하였다.

테스트 배드에서 동일한 형태의 공격을 수행한 결과 그림 17와 같이 무한 루프가 발생하여 시스템이 정지되는 것을 확인할 수 있었다. TLV 메시지의 Length 필드 변조 공격은 해당 형태로 제어메시지를 구성하는 프로토콜에서는 발생 가능성이 높은 유형의 공격이라고 할 수 있다.

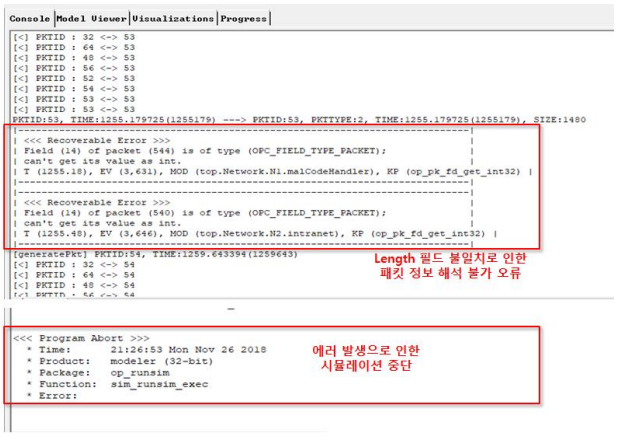

Fig. 16. Simulation status when message modification attack of TLV type message performed.
그림 16. TLV 유형 메시지의 변조 공격시 시뮬레이션 상태

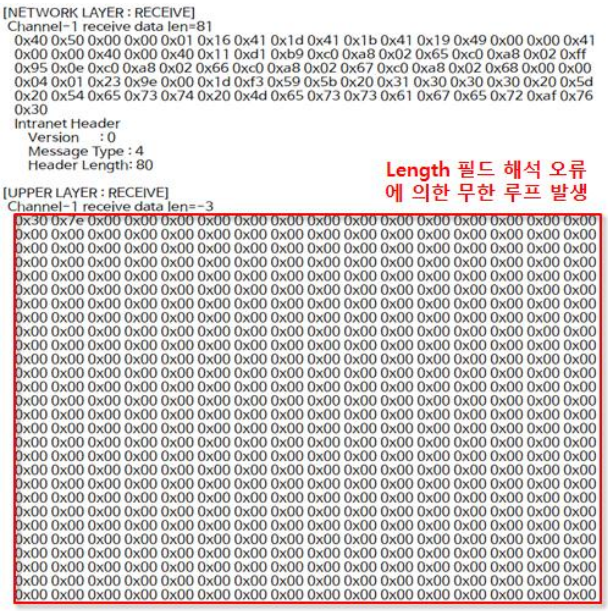

Fig. 17. Abnormal behavior due to message parsing error when the length field modification attack performed.
그림 17. Length 필드 변조 공격 시 메시지 해석 오류에 의한 비정상 동작

V. 결론

MANET 시스템에서 사이버 취약점을 식별하기 위해서는 실 시스템이 요구되어 개발 단계에서 이를 파악하고 대처하는 것이 어려울 뿐만 아니라, 실 시스템이 있어도 취약점 분석으로 인한 시스템 파괴 등을 야기할 수 있는 문제가 있다.

본 논문에서는 시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 도구를 제안하였다. 또한, MANET 망에서 발생 가능한 취약점을 식별하고

이에 따른 예상 결과를 시뮬레이션을 통해 확인한 후, 실 시스템에서도 유사한 문제가 발생할 수 있음을 확인하였다.

따라서 제안하는 시뮬레이션 기반 네트워크 보안 취약점 분석 및 검증 도구는 시스템 설계 단계에서 M&S를 기반으로 발생 가능한 보안 취약점을 식별하고 이에 따른 예상 결과를 식별함으로써 시스템 설계 및 구현 시 발생할 수 있는 문제를 사전에 파악하는데 활용될 수 있다.

References

[1] KISA, "2019년도 7대 사이버 공격 전망," http://www.kisa.or.kr/notice/press_View.jsp?cPage=1&mode=view&p_No=8&b_No=8&d_No=1739&ST=&SV=

[2] M. Antonakakis, et al. "Understanding the Mirai Botnet," *In Proc. of 26th USENIX Security Symposium*, 2017.

[3] B. Devi, et. al, "Analysis of MANET Routing Protocol in Presence of Worm-Hole Attack Using ANOVA Tool," *International Journal of Pure and Applied Mathematics*, vol.117, no.15, pp.1043-1055, 2017.

[4] Andrea Höller, "Advances in Software-Based Fault Tolerance for Resilient Embedded Systems," *Doctoral thesis, Graz University of Technology*, 2016.

[5] K. Kobara. "Cyber physical security for Industrial Control Systems and IoT," *IEICE Transactions on Information and Systems*, vol.E99.D no.4, pp.787-795, 2016.
DOI: 10.1587/transinf.2015ICI0001

[6] J. G. Ponsam, R. Srinivasan. "A survey on MANET security challenges, attacks and its countermeasures," *International Journal of Emerging Trends & Technology in Computer Science,* vol.3, no.1, pp.274-279, 2014.

[6] Riverbed Modeler, https://www.riverbed.com/sg/products/steelcentral/steelcentral-riverbed-modeler.html

[7] C. Alcaraz and J. Lopez, "A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol.40, no.4, pp.419-428, 2010. DOI: 10.1109/TSMCC.2010.2045373

[8] J. Lopez, R. Roman and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," *Foundations of Security Analysis and Design V,* vol.5705, pp.289-338, 2009.
DOI: 10.1007/978-3-642-03829-7_10

[9] Z. Trifa, M. Khemakhem, "Sybil Nodes as a Mitigation Strategy against Sybil Attack," *Procedia Computer Science*, vol.32, pp.1135-1140, 2014.
DOI: 10.1016/j.procs.2014.05.544

[10] D. York, *Seven Deadliest Unified Communications Attacks*. Syngress, 2010.

BIOGRAPHY

Hyun Jin Lee (Member)

2004 : BS degree in Electrical Engineering, Ajou University.
2006 : MS degree in Electrical Engineering, Ajou University.
2013 : Ph. D degree in Electrical Engineering, Ajou University.
2015~present : Senior Research Engineer, Solvit system.

Kwang-Hee Kim (Member)

1998 : BS degree in Computer Science & Engineering, InHa University.
1998~2005 : Research Engineer, LG Electronics
2005~2007 : Senior Research Engineer
2007~2008 : Principal Research Engineer, C-motech
2008~2011 : Principal Research Engineer, .GSI
2011~present : Director of Technique, Solvit System

Haeng-Ho Lee (Member)

1994 : BS degree in Computer Science, Korea Aerospace University.
1996 : MS degree in Computer Science, Korea Aerospace University.
1996~present : Principal Researcher, Agency for Defense Development