논문 18-43-06-13 The Journal of Korean Institute of Communications and Information Sciences '18-06 Vol.43 No.06
https://doi.org/10.7840/kics.2018.43.6.995

국방 IoT 데이터의 임무 중요도를 고려한 신뢰 보장 다중 경로 라우팅 프로토콜

금 두 호◆, 김 다 빈*, 고 영 배°

Trust Guaranteed Multi-Path Routing Protocol by Considering Mission-Critical IoT Data

DooHo Keum◆, Dabin Kim*, Young-Bae Ko°

요 약

국방 IoT 네트워크 환경에서는 다양한 스마트 센서 및 디바이스로부터 발생하는 대량의 데이터를 신뢰성 있게 전달하기 위한 라우팅 기술이 요구된다. 특히, 군 환경은 데이터의 기밀성, 중요성, 긴급성을 강조하여 임무 중요도(Mission-Criticality)가 높은 데이터를 보다 신속하고 안전하게 전달 할 수 있어야 한다. 이를 위해 기밀 데이터를 탈취하거나 폐기하는 악의적인 공격을 수행하는 노드를 탐지하고 배제하여 데이터의 전송 신뢰성을 보장할 수 있는 네트워킹 기술 연구가 필요하다. 본 논문에서는 국방 IoT 환경에서 악의적인 공격을 수행하는 노드를 탐지하는 기술을 개발하고 임무 중요도가 높은 국방 IoT 데이터일수록 종단 간 경로 신뢰성이 높은 경로를 선정하는 신뢰 기반 다중 경로 라우팅 기술을 제안한다. 본 제안 기술은 OPNET 시뮬레이터를 통해 그 성능을 검증하였고, 기존 다중경로 라우팅 기술 대비 향상된 네트워크 성능 결과를 보이는 것을 확인하였다.

Key Words : Military-IoT, Mission-Criticality, Trust worthiness, Trust-Guaranteed Multipath Routing Protocol

ABSTRACT

In the Military IoT network environment, a reliable routing protocol is required to transmit huge amount of data generated from various smart sensors and devices. In particular, the military environment emphasizes the confidentiality, importance, urgency of data so that high mission-critical data should be transmitted more quickly and safely. This requires a networking technology research that can detect and exclude nodes performing malicious attacks that steal or discard confidential data to ensure the transmission reliability of the data. In this paper, we proposed a novel trust guaranteed routing scheme to detect malicious attack nodes and select highly-enough reliable paths for the mission-critical Military IoT data. We implemented our proposed scheme through OPNET simulator and validate its performance, compared to the existing schemes, in terms of delay, throughput, and so on.

※ 본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크기술 특화연구센터 사업의 일환으로 수행되었습니다.(UD160070BD)

◆ First Author : (ORCID:0000-0002-8267-2331)Ajou University Department of Computer Engineering, dooho1000@ajou.ac.kr, 학생회원

° Corresponding Author : (ORCID:0000-0002-8799-1761)Ajou University Department of Computer Engineering, youngko@ajou.ac.kr, 종신회원

* (ORCID:0000-0003-2009-4529)Agency for Defense Development, dabin912@gmail.com

논문번호 : KICS2018-04-091, Received April 19, 2018; Revised June 12, 2018; Accepted June 15, 2018

Ⅰ. 서 론

국방 IoT (M-IoT : Military IoT)란 다양한 스마트 센서를 이용해 전장 감시, 물품관리, 병사의 위치 및 상태 등의 정보들을 실시간으로 수집함으로써 작전상황에서 신속한 정보 분석과 예측을 통해 아군의 전술 네트워크의 기술우위를 선점할 수 있게 하는 새로운 기술을 말한다. 최근 DARPA, NATO를 주축으로 국방 IoT 기술을 현 전술체계에 효과적으로 적용하기 위한 다양한 기술 연구 및 개발이 대두되고 있다[1,2]. 미래 국방 IoT 환경에서는 대량의 센서 디바이스에서 발생되는 Massive-IoT 데이터부터 신속하고 신뢰성 있게 전송되어야 하는 Critical-IoT 데이터까지 다양한 트래픽이 대규모로 혼재되어 유통될 것으로 예측된다.

자원 제약적 특성을 갖는 국방 IoT 환경에서는 무선 채널 및 단말의 자원 제약 문제로 인해 네트워크 혼잡, 패킷 충돌 등의 문제가 발생할 수 있으며 이로 인해 중요 전술 데이터의 신뢰성 있는 전송을 보장하기 어려운 문제가 발생할 수 있다. 특히 블랙홀 공격(Black-hole attack), 그레이 홀 공격(Gray-hole attack)[3] 등과 같이 악의적인 노드의 공격으로 네트워크 내부에서 유통되는 중요 데이터가 임의로 폐기될 경우 임무 중요도가 높은 작전 데이터가 소실되어 네트워크의 신뢰성이 감소하는 문제가 발생할 수 있다. 따라서 이러한 문제를 효과적으로 전송하기 위해서는 전술 엣지 네트워크의 환경을 고려한 신뢰보장 네트워킹 기술이 필요한 실정이다. 본 논문에서는 대규모 국방 IoT 환경에서 중요도가 높은 데이터의 전송 신뢰성을 보장하기 위한 신뢰 기반의 다중 라우팅 기술에 대한 연구를 제안한다.

본 논문의 제안 기법은 국방 전술 IoT 데이터를 임무 중요도에 따라 우선순위를 부여한 후, 이를 경로 신뢰도(PTV : Path Trust Value) 메트릭을 기반으로 생성된 다중 경로에 차등적으로 전송함으로써, 트래픽 부하분산과 전송지연을 줄인다. 즉, 각 노드가 이웃 노드의 패킷 전송행위를 관찰하여 악의적인 행위를 수행하는 노드를 데이터 전송 경로에서 배제함으로써 공격에 의한 데이터 손실 확률을 감소시키고 네트워크의 성능을 보다 향상시킨다. 제안 기술의 특징은 다음과 같이 기술할 수 있다.

- 노드의 신뢰도 평가를 통해 악의노드를 탐지함으로써 악의노드가 포함되어 있지 않은 k개의 다중 신뢰 경로를 탐색한다.
- k개의 신뢰보장 다중경로에 대해 전술 데이터의 임무 중요도에 따라 전송 경로를 차등 선택함으로써 높은 임무 중요도를 갖는 데이터가 가장 높은 신뢰 경로로 전송 되도록 한다.
- 다중 경로 데이터 분산 전송을 통해 네트워크 부하 분산 효과를 보장할 수 있다.
- 제안 기법은 OPNET 시뮬레이터를 통해 그 성능을 검증하였고 비교 기술들 대비 성능 우위를 보인다.

Ⅱ. 관련연구

신뢰 평가 (Trustworthiness estimation)는 단말 간 안전하고 신뢰가 보장된 통신을 위해 통신 단말의 신뢰도(Trustworthiness)를 평가하는 기술로 다양한 방향의 연구가 진행되어 왔다. 특정 노드의 패킷 전송 행위를 관찰하여 노드의 신뢰도를 평가하는 방법이 가장 널리 사용되고 있고, 각 네트워크의 특성을 반영하여 에너지 사용량, 이동성, 네트워크 위상 변화 등을 반영할 수 있다. 본 장에서는 기존 모바일 애드혹(MANET: Mobile Adhoc NETwork) 환경과, IoT 환경에서 주로 활용되는 신뢰 평가 방법 및 신뢰측정 메트릭에 대해 소개하고 제안하는 기법에서 사용되는 신뢰 평가 방법에 대해 기술한다.[3-6]

2.1 신뢰 평가 방법

직접 신뢰평가 (Direct Observation)는 네트워크상의 모든 노드들이 자신의 이웃노드들의 패킷 포워딩 및 드롭 등의 전송 행위를 관찰하여 신뢰도를 측정하는 방법이다. 주로 패킷을 수신한 노드로부터 ACK 수신 여부 혹은 정상적인 패킷 포워딩 동작을 오버히어링 함으로써 신뢰 값을 계산한다.

간접 신뢰평가 (Indirect Observation) 방법은 타깃 노드에 대해 자신이 측정한 신뢰 값을 다른 노드에게 추천해주는 방법으로서 주변노드가 전파하는 신뢰 값을 종합하여 타깃노드에 대한 신뢰도를 계산한다. 각 노드는 주변노드로부터 타깃노드에 대한 간접 신뢰 값을 수신하면 직접 신뢰 평가를 하지 않고도 타깃노드에 대한 신뢰 값을 얻을 수 있다. 하이브리드 신뢰 평가 방법은 각 노드들이 직접 신뢰평가로 측정한 타깃노드에 대한 신뢰 값과 주변노드로부터 추천받은 간접 신뢰 평가 값을 기반으로 타깃노드에 대한 신뢰도를 측정한다. 신뢰 값을 계산하는 방법으로는 모든 노드로부터 타깃노드에 대한 가중 신뢰 값을 (Weighted Trust) 수집한 후 그 평균값을 취하는 "가중 평균(Weighted Average)" 방법, 모든 노드로부터 타깃노드에 대한 신뢰 전파 (Trust Report)를 수집한 후 값 들 중 가장 큰 값을 취하는 "낙관적 또는 점진

적 접근법(Optimistic or Greedy approach)"방법 등이 있다.[6]

2.2 신뢰 값 메트릭(Trust metric)

신뢰 값 메트릭이란 실제 타깃노드에 대한 신뢰도를 정량적으로 표현하기 위해 사용하는 값으로서, 일반적으로 [0, 1] 혹은 [-1, 1] 사이의 값으로 표현한다. 신뢰 값은 1에 가까울수록 신뢰할 수 있는 노드임을 의미하고 -1이나 0에 가까울수록 신뢰할 수 없는 노드임을 의미한다. 신뢰 값을 측정하기 위해 주로 사용되는 방법으로는 송신노드가 패킷을 전송 한 후 다음 홉의 노드가 패킷을 포워딩 했는지에 대한 여부를 관찰하여 정상적으로 패킷을 포워딩한 비율(PFR: Packet Forwarding Ratio)을 계산하는 방법이 있다. 또한 지연시간, 잔여 에너지, 작업 처리 능력 등의 신뢰 값 요소를 복합적으로 고려하여 계산하는 방법과 베이지안 추론(Bayesian inference), 퍼지 논리(Fuzzy logic) 등을 적용하여 데이터 전송 성공률에 대한 신뢰 값을 측정하는 방법 등이 있다.[3,5] 본 논문에서는 제안 기법에 대한 성능을 검증하기 위해 주로 사용되는 패킷 포워딩 비율(PFR)을 신뢰 값으로 계산하고 이를 메트릭으로 활용하였다.

2.3 신뢰 기반 라우팅 기술

신뢰 기반 라우팅 기술은 신뢰 평가 및 요소 등으로부터 도출된 신뢰 값을 활용하여 경로 탐색 및 유지할 수 있는 기술이다. 본 논문에서는 MANET 및 IoT 환경에서의 신뢰보장 라우팅 기술에 대한 연구를 소개한다.[3,7,9]

AOTDV (Ad hoc On-demand Trusted-path Distance Vector routing)[7]는 AOMDV (Ad hoc On-demand Multipath Distance Vector routing)[8]를 확장한 신뢰 기반 다중 경로 라우팅 기술을 제안한다. AOMDV는 MANET 환경의 대표적인 반응적(Reactive) 방식의 라우팅 프로토콜인 AODV를 다중 경로 라우팅으로 확장한 연구로서 경로 탐색 시 링크 비중첩(link-disjoint)한 다중 경로를 탐색하는 것이 특징이다. 따라서 AOTDV의 기본적인 라우팅 경로 탐색 방법은 AOMDV와 유사한데, 경로탐색요청 패킷인 RREQ(Route Request) 패킷을 수신한 목적지노드가 k 개의 경로탐색응답 패킷인 RREP (Route Reply)를 전송하여 다중 경로를 생성하는 과정에서 차이점이 존재한다.

AOTDV는 라우팅 메트릭으로 홉 카운트와 경로 신뢰도(PTV) 값을 모두 고려한다. 경로 신뢰도 값을 계산하기 위해서는 각각의 노드에 대한 신뢰 평가가 필요한데, AOTDV에서는 직접신뢰평가 방법을 이용해 단위 시간당 타깃노드가 정상적으로 패킷을 포워딩 한 비율을 컨트롤 패킷과 데이터 패킷을 모두 고려하여 측정한다. 이를 기반으로 경로 신뢰도 값은 RREP 패킷을 전송하는 경로 상의 모든 노드들의 신뢰 값을 누적 곱하고 각 노드는 라우팅 테이블에 경로 신뢰도 값을 업데이트하여 관리한다. 다중 경로 생성이 완료된 후, 소스노드는 중요 데이터 패킷 전송을 위해 탐색된 경로의 신뢰 값을 확인하고 중요 데이터별 요구하는 신뢰 값이 만족하는 신뢰 경로로 해당 데이터를 전송할 수 있는 스킴을 제안한다. AOTDV는 데이터의 중요도를 고려하여 신뢰성이 확보된 경로를 통해 전송 할 때 안전한 통신을 할 수 있지만 긴급하고 중요한 정보를 신속하게 전달하기에는 한계가 있다. 본 논문에서는 이러한 한계를 극복하기 위하여 중요한 데이터일수록 최적의 경로를 통해 데이터를 전송하는 스킴을 소개하고 이에 대한 효율성을 성능 비교 결과를 통해 보여준다.

IoT 환경을 고려한 신뢰 기반 기술로는 표준 라우팅 프로토콜인 RPL (IPv6 Routing Protocol for Low-Power and Lossy Network)을 기반으로 신뢰 요소 메트릭을 반영한 연구가 진행되었다.[9] RPL은 저전력 임베디드 디바이스인 리프노드로부터 베이스 스테이션 역할을 하는 루트노드까지의 상향 라우팅에 중점을 두고 설계되었으며 루트노드를 중심으로 DODAG(Destination Oriented DAG)를 구성한다. DODAG의 경로를 구성하기 위해 DIO (DODAG Information Object)라는 컨트롤 패킷을 주기적으로 전송하고 패킷 안에 들어 있는 OF(Object Function), DODAG ID, RANK 등의 정보를 통해 토폴로지 내 노드의 라우팅 테이블을 업데이트 한다. 표준 OF에서는 ETX(Expected Transmission Count)나 에너지 등의 메트릭을 고려하여 저 전력 저 손실 기능을 수행할 수 있도록 정의하고 있다. [9]에서는 OF에 추가로 ERNT(Extended RPL Node Trustworthiness)라는 메트릭을 제안함으로써 신뢰성을 고려한 새로운 경로 선정 기법을 제안한다. 특히, ERNT에 대한 신뢰를 평가할 때 정직성(Honesty), 에너지, 비이기성(Unselfishness)이라는 세 가지 요소를 모두 고려하여 직접신뢰평가와 간접신뢰평가를 수행한다. 신뢰 경로 선정은 경로 상에 있는 노드 신뢰도 중 최솟값을 정하여 경로 신뢰도를 정하고 경로들 간 경로 신뢰도 중 최댓값을 정하여 경로를 선정한다. 그러나 국방 IoT 환경에 이러한 기법을 적용할 때 다차원 신뢰 평가에

대한 오버헤드가 비교적 높고 모든 데이터를 단일 경로를 통해 전송하기 때문에 대량의 데이터를 효과적으로 처리하기 어려운 한계가 있다. 신뢰평가에서의 오버헤드 문제를 해결하기 위해 MANET 환경에서는 다양한 신뢰 평가 요소를 복합적으로 계산하면서 경량화를 고려한 신뢰 향상 라우팅 프로토콜 연구가 진행되었다.[3] [3]는 자원 제약이 많은 디바이스를 고려한 신뢰 평가를 위해 수동적이고 지역적인 모니터링을 하는 신뢰 프레임워크를 사용하며 데이터에 따라 처리하는 경로 유지 메커니즘을 통해 라우팅 오버헤드와 경로 탐색 주기를 줄이는 방법을 제안한다. 또한 신뢰 값을 얻기 위해서 직접평가, 노드 활동 정도, 이전 신뢰 기록 등을 복합적으로 고려한 다차원의 신뢰 속성을 퍼지 AHP 스킴으로 계산하였으며 보다 정확한 신뢰 값을 얻기 위한 방법을 제안한다. 국방 IoT 환경에 본 기법을 적용할 시 임무 중심 데이터에 대한 신뢰성을 고려하지 않기 때문에 요구되는 신뢰성을 보장하기는 어렵지만, 최근 각각의 환경 특성에 맞게 다차원 신뢰 속성을 고려하여 신뢰 값을 도출하는 연구들이 진행되고 있다.[4] 예를 들어 친밀감, 관계 정도 등의 사회적 요소를 고려해서 신뢰 값을 얻거나 UAV(Unmanned Aerial Vehicle)나 IoT 디바이스의 배터리 상태, 속도 등을 복합적으로 고려하여 신뢰 값을 도출하는 방법 등이 있다. 하지만 국방 IoT 환경을 고려한 복합적인 신뢰 평가에 대한 연구가 미비하므로 앞으로 중요한 연구 이슈로 기대된다.

Ⅲ. 제안기법

본 장에서는 국방 IoT 데이터의 임무 중요도 수준에 따라 데이터의 중요도가 높을수록 신뢰성을 보장할 수 있는 신뢰 기반 다중 경로 라우팅 기술을 설명한다. 제안 기법 MC-AOTDV(Mission-Critical AOTDV)는 AOMDV의 다중 경로 구성과정을 기반으로 동작하며 신뢰도 측정을 통해 악의노드를 탐지하고 중요 데이터의 신뢰성을 보장한다. 신뢰도 평가 및 관리, 경로를 선정하는 방법에 대해 ① 신뢰 평가 기법, ② 신뢰 경로 탐색, ③ 경로 선정 및 유지 방법으로 구분하여 설명한다.

3.1 신뢰 평가 방법

주변노드에 대한 신뢰도를 평가하기 위해 간단하면서 주로 활용되는 패킷 포워딩 비율(PFR)을 계산하여 수행한다. 패킷 포워딩 비율은 송신노드가 패킷을 전송하고 수신노드가 해당 패킷을 정상적으로 포워딩하였는지 여부를 송신노드가 확인하여 계산하는 방식으로 악의노드가 수신 패킷을 임의로 폐기하거나 전송하지 않는 등의 악의 행위를 탐지하는 지표로 사용한다. 정상적인 패킷 포워딩 여부를 확인하기 위해 무차별 모드(Promiscuous Mode)를 통해 모든 데이터 전송을 오버히어링 하며, 신뢰 값은 단위 시간을 설정하여 주기적으로 계산하도록 한다. 패킷 포워딩 비율은 아래 수식 (1)과 같이 계산되며 $N_A(t)$는 단위시간 동안 송신노드가 전송한 전체 패킷의 수, $N_F(t)$는 실제로 포워딩된 패킷의 수를 의미한다.

$$PFR(t) = \frac{N_F(t)}{N_A(t)} \tag{1}$$

위 수식을 이용하여 송신노드 a는 수신노드 b에 대한 노드 신뢰도 (NTV : Node Trust Value)값을 아래의 수식 (2)를 통해 산출할 수 있다.

$$NTV_{ab}(t) = w_1 \times CPFR_{ab}(t) + w_2 \times DPFR_{ab}(t) \tag{2}$$

NTV_{ab}는 노드 a가 측정한 이웃노드 b의 신뢰도로서, 컨트롤 패킷에 대한 포워딩 비율과(CPFR: Control PFR) 데이터 패킷에 대한 포워딩 비율(DPFR: Data PFR)을 모두 고려하여 계산한다. 이때 노드 a는 노드 b가 포워딩하는 패킷들 중 오직 자신이 전송한 패킷만을 선별하여 패킷 포워딩 비율을 계산할 수 있어야 한다. 이를 위해 본 논문에서는 컨트롤 및 데이터 패킷 헤더에 이전 노드 id 정보를 추가함으로써 노드 b가 전송하는 패킷이 자신으로부터 수신했던 것인지 혹은 다른 이웃노드로부터 수신했던 것인지 확인할 수 있도록 하였다. 블랙홀, 그레이홀 공격 등과 같이 패킷을 임의로 폐기하는 악의적 행위를 할 경우 해당 노드에 대한 NTV 값이 감소하므로 일정 임계 값 이하로 떨어지면 악의노드로 간주할 수 있다.

본 논문에서는 신뢰도 계산을 위한 가중치 값 w_1, $w_2(w_1, w_2 \geq 0,\ w_1+w_2=1)$ 을 각각 0.5로 설정하여 노드 신뢰도 평가 시 컨트롤 패킷과 데이터 패킷 포워딩 비율을 동일하게 적용하였다. 위 방식을 통해 도출된 각 노드의 NTV 값은, 이후 신뢰 경로 탐색 시 경로 신뢰도 값을 계산하는데 활용된다.

3.2 신뢰 경로 탐색

본 논문에서 제안하는 신뢰 경로 탐색은 애드 혹

환경에서의 다중 경로 라우팅 기법인 AOMDV와 유사한 방법으로 동작하지만, 임무 중요도에 따른 데이터 중요도 별로 경로 사용을 달리한다는 점에서 차이가 있다. 다중 신뢰 경로 탐색을 위한 라우팅 메트릭으로써 경로탐색 메시지를 전송하는 노드들의 NTV 값을 이용해 수식 (3)과 같이 경로 신뢰도 값 (PTV: Path Trust Value)을 계산한다.

$$PTV = \prod NTV_{ab} (0 \leq PTV \leq 1) \quad (3)$$

경로 탐색 시 RREQ (Route REQuest) 메시지가 전파되면서 각 노드의 NTV 값이 곱해지고 수식 (3)과 같이 경로 신뢰도 값 PTV를 계산한다. 만약 탐색된 종단 간 경로상에 블랙홀, 그레이홀 등의 공격을 수행하는 악의노드가 하나 이상 존재할 경우 PTV 값이 감소하게 된다.

복수개의 RREQ를 수신한 목적지노드는 무분별한 신뢰 경로 생성을 방지하기 위해 단위 시간 동안 받은 PTV 값 중 가장 큰 값인 최적 값(PTV^{opt})을 기준으로 상위 k 개의 경로에 대해 RREP를 생성한다. k 값을 정하기 위해서 표 1과 같이 5개의 경로 신뢰도 레벨(PTL_i)을 정의하며 신뢰도가 높은 PTL_1 순부터 PTL_5 까지 각 구간을 0.2 단위로 구분한다.

목적지노드는 수신한 PTV^{opt} 값이 포함되는 범위의 신뢰경로 레벨 i에 대해 6 − i개의 RREP를 전송한다. 그 이유는 최소 한 개 이상의 경로 생성을 필수적으로 보장하기 위해서이다. 최종적으로 RREP를 수신한 송신노드는 생성된 k 개의 경로를 라우팅 테이블에 업데이트하고 임무 중요도에 따라 신뢰된 경로를 선정하기 위한 작업을 수행한다.

표 1. 경로 신뢰도 레벨 및 경로 신뢰도 범위
Table 1. Path Trust Levels and PTV Range

Path Trust Levels(PTL_i)	PTV Range
1	0.8 < PTV ≤ 1.0
2	0.6 < PTV ≤ 0.8
3	0.4 < PTV ≤ 0.6
4	0.2 < PTV ≤ 0.4
5	0.0 ≤ PTV ≤ 0.2

3.3 경로 선정 및 유지

신뢰 경로 선정은 임무 중요도에 따라 차등적으로 경로를 선정하도록 하며 임무 중요도가 높은 데이터일수록 보다 최적의 경로를 사용하여 신뢰성을 보장하도록 한다. 기존 MANET 환경에서의 다중 경로 라우팅 연구는 크게 두 가지로 구분된다. 첫 번째는 데이터 패킷의 전송 신뢰성을 보장하기 위해 같은 패킷을 다중 경로로 동시에 전송하는 기법이 있고 두 번째는 다중 경로 중 가장 좋은 경로를 사용하다가 병목현상, 링크 단절 등에 의해 링크 품질이 저하되었을 때 대체 경로로 활용하는 기법이다. 본 제안기법은 데이터의 임무 중요도 별로 다중 경로를 선정하는 스킴을 제안하여 병목현상, 링크 품질 저하 문제를 해결하고 중요 데이터 일수록 신뢰된 경로로 전송하고자 한다. 데이터를 신뢰성 있게 전송하기 위해서는 중요도 별로 어떤 경로를 사용할지 정해야 하는데 이를 위해 전송신뢰도($Trans_{tos}$)가 필요하다. 전송신뢰도는 수식 (4)와 같이 계산하고, 표 2와 같이 전송신뢰도와 맞는 경로 신뢰도 레벨로 ToS 데이터를 전송한다. ToS(Type of Service)는 서비스의 종류를 의미하며 중요 데이터 순으로 ToS 1부터 5까지 각 데이터의 중요도를 구분한다.

$$Trans_{tos} = PTV^{opt} \times DMV_{tos} \quad (4)$$

본 논문에서는 Mission Criticality 수준인 ToS값에 대응하는 데이터를 전송하기 위해 데이터의 임무중요도(DMV : Data's Mission-critical Value)를 다음과 같이 정의한다.

DMV_1: 1.0, DMV_2: 0.95, DMV_3: 0.9,
DMV_4: 0.85, DMV_5: 0.8

DMV를 다음과 같이 정의한 이유는 PTV^{opt}가 1이라고 가정할 때 링크 상태가 좋은 경우이기 때문에 모든 ToS 데이터를 가장 좋은 경로를 통해 전송할 수 있어야 한다. 이를 위한 전송신뢰도를 계산할 때 DMV_5가 0.8이어야 하며 다섯 단계로 균등하게 하기

표 2. PTV^{opt}가 0.65일 때 $Trans_{tos}$별 계산 및 PTL_i
Table 2. $Trans_{tos}$ calculation and PTL_i when PTV^{opt} is 0.65

ToS	$Trans_{tos}$	PTL_i
1	0.65× 1.0 = 0.65	2
2	0.65 × 0.95 = 0.617	2
3	0.65 × 0.9 = 0.585	3
4	0.65 × 0.85 = 0.553	3
5	0.65 × 0.8 = 0.52	3

위해 0.05단위로 할당한다.

이를 적용할 때 PTV^{opt} 값이 0.65라면 표 2와 같이 전송신뢰도가 계산되고 경로 신뢰도 레벨은 $Trans_1$값이 속한 PTL_2 부터 순서대로 정해진다. 그림 1과 같이 중요도가 높은 ToS1, 2는 보유한 경로 중 가장 신뢰도가 높은 PTL_2을 선정하고 ToS 3,4,5는 두 번째로 신뢰도가 높은 경로 PTL_3을 선정하여 데이터를 전송하게 된다.

신뢰 경로 유지는 데이터를 신뢰성 있게 전송하기 위해 데이터 패킷과 컨트롤 패킷 정보를 주고받으며 경로 신뢰 값을 업데이트 하는 방식으로 유지된다. 신뢰 값은 주기적으로 업데이트 되며 상황 적응적으로 경로에 대한 신뢰 상태를 확인 할 수 있고 이를 통해 주요 데이터를 신뢰 경로로 전송할 수 있다. 그림 2와 같이 최적 경로 신뢰도가 0.65에서 0.95로 바뀌었을 때 최적 신뢰 경로 정보가 업데이트 되고 표 3과 같이 전송신뢰도가 계산되며 경로 신뢰도 레벨은 $Trans_1$값이 속한 PTL_1부터 순서대로 정해진다. 그림 2와 같이 중요도가 높은 ToS 1,2,3,4는 최적 경로

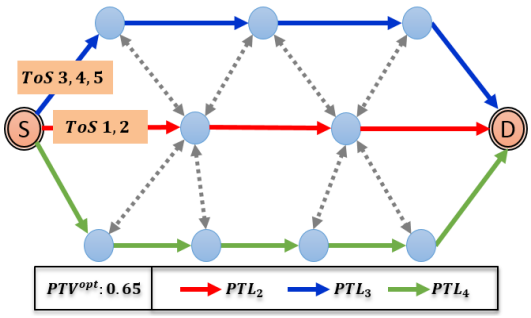

그림 1. PTV^{opt}가 0.65일 때 ToS 데이터 별 경로 선정
Fig. 1. Select route by ToS Data when PTV^{opt} is 0.65

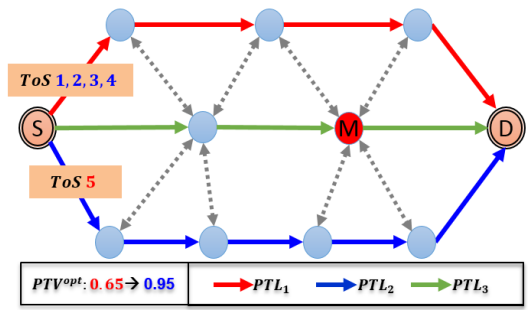

그림 2. PTV^{opt} 값이 업데이트 될 때 ToS 데이터 별 경로 선정
Fig. 2. Select route by ToS Data when PTV^{opt} is updated

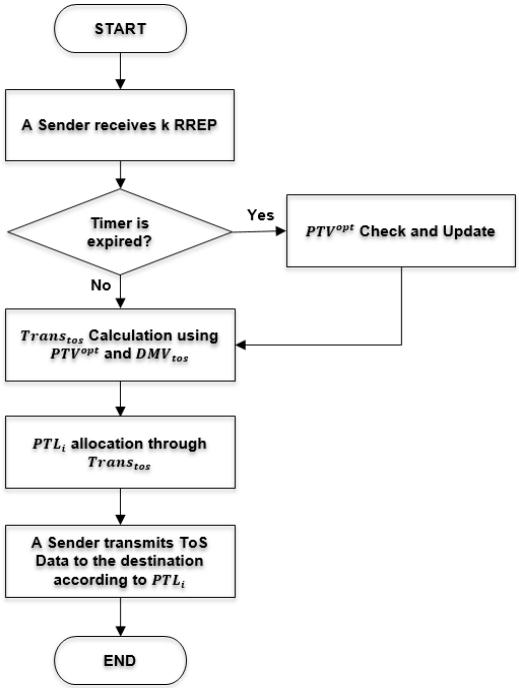

그림 3. 경로 선정 및 유지에 대한 플로 차트
Fig. 3. Flow Chart for Route selection and maintenance

를 사용하게 되고 비교적 중요도가 낮은 ToS 5는 2순위 경로를 통해 전달하게 된다. 그림 3은 신뢰 경로 선정과 유지에 대한 플로 차트를 개략적으로 나타낸다. 송신노드가 k개의 RREP를 수신 후 경로가 생성되고 주기적으로 PTV^{opt}가 업데이트 된다. 신뢰 경로 선정을 위해 전송신뢰도가 수식 (4)와 같이 계산되며 결과 값과 신뢰도 범위가 맞는 PTL_i이 정해진다. 송신노드는 PTL_i 경로에 따라 각 ToS 데이터를 목적지로 전송하게 된다. 이러한 신뢰 경로 선정 및 유지 제안기법은 국방 IoT 환경과 같이 대량의 데이터가 활용되거나 다변적인 상황에서 발생할 수 있는 링크 품질 저하와 병목현상 등의 상황에 대해 신속하게

표 3. PTV^{opt}가 0.95일 때 $Trans_{tos}$별 계산 및 PTL_i
Table 3. $Trans_{tos}$calculation and PTL_i when PTV^{opt} is 0.95

ToS	$Trans_{tos}$	PTL_i
1	0.95× 1.0 = 0.95	1
2	0.95 × 0.95 = 0.902	1
3	0.95 × 0.9 = 0.855	1
4	0.95 × 0.85 = 0.807	1
5	0.95 × 0.8 = 0.76	2

대처할 수 있고 임무 중요도가 높은 데이터의 신뢰성을 보장할 수 있다.

Ⅳ. 성능 평가 및 검증

본 장에서는 제안기법의 성능을 확인하기 위해 시뮬레이션 환경을 표 4와 같이 설정하여 분석한다. 성능 분석은 OPNET 네트워크 시뮬레이터에서 구현 및 검증하였으며 제안 기법 MC-AOTDV을 AOMDV, AOTDV 라우팅 프로토콜과 비교 분석한다. 국방 IoT 데이터의 정보는 방사선, 화학 감지센서, 바이오 측정 센서, 음성, 영상 등의 종류, 사이즈, 발생 주기를 고려하고[10-12] CBR 트래픽 모델로 고정하여 설정하였다. 실험노드는 총 15개 중 14개의 신뢰노드와 50% 확률로 그레이 홀 공격을 수행하는 1개의 악의노드를 배치하였고 양방향 패킷 전송을 통해 신뢰 평가를 수행하도록 한다. MAC 프로토콜은 CSMA/CA를 사용하고 PHY는 802.11b 2Mbps로 정하였으며 성능평가 척도로는 PDR(Packet Delivery Ratio), 지연시간(Delay), 지터(Jitter), 처리량(Throughput)을 비교 분석하였다. PDR은 소스노드에서 목적지노드까지 송신한 패킷 양과 수신한 패킷 양의 비율로 계산하고 지연시간은 소스노드에서 목적지노드까지 패킷이 전달된 지연시간으로 계산되며 지터는 패킷들이 전송 될 때 송신노드에서 보내질 때의 시간 간격과 수신노드에 도착할 때 시간 간격 차이로 나타낸다. 처리량은 지정된 시간 내 전송된 패킷들을 처리한 단위량으로 계산한다.

그림 4에서는 경과 시간에 따른 패킷 전달 비율을 나타낸다. AOTDV와 MC-AOTDV는 92% 이상의 높은 패킷 전달 비율을 보이는 반면 AOMDV의 경우 50% 정도의 비교적 낮은 PDR를 보여준다. AOTDV

표 4. 시뮬레이션 환경
Table 4. Simulation environment

Parameters	Values
Simulator	OPNET 17.5
Simulation time	500s
Routing Protocol	AOMDV, AOTDV and MC-AOTDV
Number of nodes	15
Number of Malicious node	1
Traffic Type (Avg. Packet size)	VoIP G.723.1 (24 bytes)
	Lighting Sensor (100 bytes)
	Fire alarm, Health Sensor (120 bytes)
	Video Surveillance H.264 (500 bytes)
	CCTV (2000 bytes)
Packet generation rate	110Kbps
Trust update time	0.3s
MAC Protocol	CSMA/CA
PHY	802.11b 2Mbps

와 MC-AOTDV는 신뢰 기반 메트릭을 사용함으로써 악의노드의 행위를 탐지하고 해당 경로를 배제한 후 신뢰된 경로를 선정하기 때문에 높은 패킷 전달 비율을 확인할 수 있다. AOMDV의 경우, 신뢰 기반 메트릭을 사용하지 않고 홉 카운트를 고려한 메트릭으로 경로를 선정함으로써 악의노드 공격 행위에 그대로 노출되어 낮은 패킷 전달 비율을 보이게 된다. 그림 5는 경과시간에 따른 평균 지연시간을 나타내며 MC-AOTDV가 AOTDV에 비해 약 1.26ms 낮은 평균 지연 시간을 보여준다. MC-AOTDV는 악의노드를 탐지한 후 데이터의 중요도에 따라 다중 경로를 선정하여 데이터를 전송할 수 있기 때문에 단일 경로만을 사용하여 전송할 때 발생할 수 있는 병목 현상, 큐잉 지연 시간 등을 줄이고 보다 신뢰된 경로를 통해 데이터 전송을 할 수 있다. AOTDV의 경우는 악의노드를

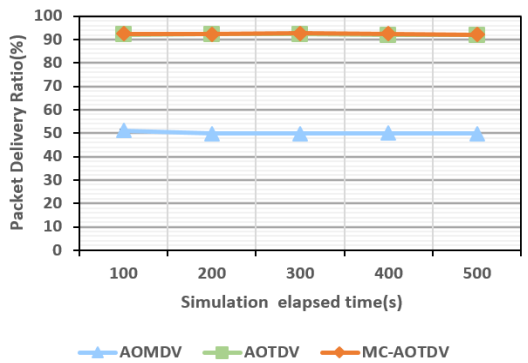

그림 4. 경과 시간에 따른 패킷 전달 비율
Fig. 4. Packet delivery ratio over elapsed time

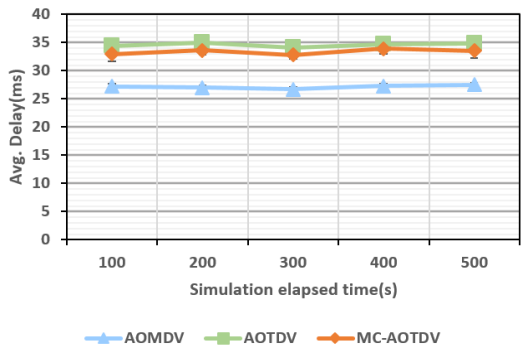

그림 5. 경과 시간에 따른 평균 지연 시간
Fig. 5. Average delay over elapsed time

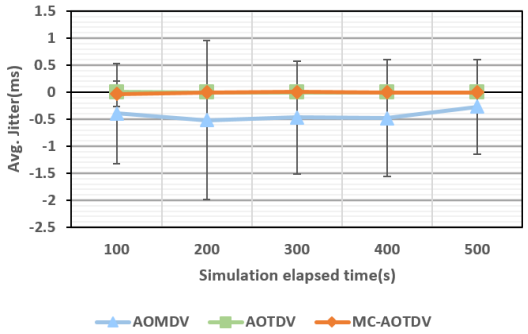

그림 6. 경과 시간에 따른 평균 지터
Fig. 6. Average jitter over elapsed time

탐지한 후 홉 카운트 또는 신뢰 값을 고려하고 하나의 경로를 선정하여 전송하기 때문에 보다 높은 평균 지연시간이 걸린 결과를 확인할 수 있다. AOMDV의 경우에는 홉 카운트 기반의 메트릭을 사용하여 데이터를 전송하기 때문에 가장 짧은 경로로 전송을 하여 MC-AOTDV와 AOTDV보다 낮은 지연시간을 보여준다. 하지만 측정된 지연시간은 전송이 성공한 패킷만을 측정한 결과로 데이터의 신뢰성을 보장한다고 보기 어렵다. 그림 6의 경우는 경과 시간에 따른 평균 지터 값을 나타낸다. 결과 값은 OPNET 시뮬레이터에서 통계량(Statistic)으로 측정한 값이며 지터에 대한 계산은 다음과 같은 식으로 계산될 수 있다.

Jitter = (현재시간 - 이전 패킷의 수신 시간)
- (패킷을 송신한 시간 - 이전 패킷을 송신한 시간)

지터 값은 이전에 송신한 패킷이 병목현상, 폐기 등으로 인해 도착 수신 시간이 증가하게 되면 음수가 될 수 있다. 예를 들어 패킷을 수신한 노드의 현재 시간이 5초, 이전 패킷을 받은 수신 시간이 4.5초, 송신노드가 패킷을 송신한 시간이 3초, 이전 패킷을 송신한 시간이 2초라면 (5-4.5) - (3-2) = -0.5라는 음수 값이 된다. 그림 6의 AOMDV는 악의노드로 인해 목적지까지 가는 패킷이 50% 확률로 폐기되어 목적지에서 받는 이전 패킷의 수신 시간이 증가하게 되므로 음수 값을 갖는 결과가 나타난다. 또한 표준편차 (Standard Deviation) 폭이 MC- AOTDV와 AOTDV에 비해 현저하게 크기 때문에 안정적이지 못한 경로를 통해 데이터를 전송한다고 볼 수 있다.

반면 MC-AOTDV와 AOTDV는 표준편차가 0에 가까운 지터 값으로 안정적인 경로를 통해 데이터를 전송한다고 할 수 있다. 그림 7은 경과 시간 내에 전송된 패킷의 평균 처리량 결과를 보여준다. 처리량은 단위 시간 동안 패킷의 크기와 발생 주기, 오버헤드(ACK, 백오프 등) 등의 계산을 통해 도출되며 본 실험에서는 표 1과 같이 다양한 국방 IoT 데이터를 고려한 데이터 크기와 주기를 설정하여 실험하였다. 그 결과, MC-AOTDV와 AOTDV는 평균적으로 약 1500kbit/sec를 처리한 반면에 AOMDV는 악의노드로 인해 패킷을 처리하지 못하여 평균적으로 약 900kbit/sec 이하의 처리량을 보여준다. 그림 8은 AOTDV 논문에서 예시로 소개한 데이터 패킷의 요구 신뢰도를 적용하여 데이터를 전송할 때 MC-AOTDV와 종단 간 지연시간(End-to-End Delay)에 따른 누적 분포함수 (CDF : Cumulative Distribution Function) 비교 결과를 나타낸다. CDF는 중요 데이터 ToS 1, 2에 대해 측정했으며 종단 간 지연시간에 따른 수신한 패킷 양의 비율로 계산된다. AOTDV의 경우 예시로 소개한[17] "Extremely important data"를 ToS 1로 정하고 0.9이상의 요구 신뢰도가 만족해야만 전송할 수 있도록 하였으며 "Important data"를 ToS 2로 정하고 0.75이상의 요구 신뢰도가 만족해야 전송할 수 있도

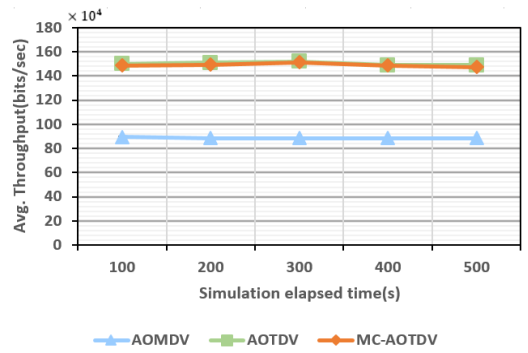

그림 7. 경과 시간에 따른 평균 처리량
Fig. 7. Average throughput over elapsed time

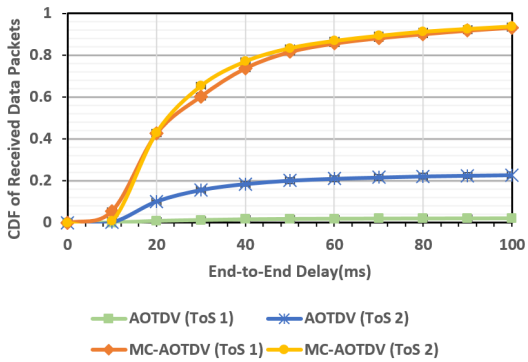

그림 8. 종단간 지연시간에 따른 CDF
Fig. 8. CDF of end-to-end delay

록 하고 있다. 그 결과, MC-AOTDV는 중요 데이터 ToS 1, 2를 100ms안에 90%이상 수신하여 데이터의 신뢰성을 보장하는 결과를 보이는 반면 AOTDV는 요구하는 신뢰도가 만족할 때 전송할 수 있기 때문에 일정 시간동안 중요 데이터에 대해 낮은 수신 양과 데이터를 수신하기 위해 많은 지연시간이 걸리는 결과를 확인할 수 있다. 군 IoT 환경에서는 중요 데이터에 대해 신속하고 정확한 정보 전달이 필수적이므로 MC-AOTDV와 같이 데이터의 신뢰성을 보장하면서 전송할 수 있는 기술이 적합하다고 볼 수 있다.

V. 결 론

본 논문은 국방 IoT 네트워크 환경에서 악의노드를 탐지하고 임무 중요도를 고려하여 데이터를 전송하는 신뢰 기반 다중 경로 라우팅 기술을 제안한다. 임무 중요도가 높은 데이터는 신뢰성과 기밀성이 보장되어야 하고 신속하게 전송되어야 하기 때문에 신뢰성을 보장하기 위한 연구가 필수적이다. 본 논문에서 제안한 기법은 임무 중요도가 높을수록 데이터를 안전하고 신속하게 전송할 수 있도록 하였으며 타 기법과 비교해 성능 우의를 보인다. 향후 연구로 국방 IoT 환경의 특성을 고려하여 신뢰도를 평가하기 위한 신뢰 모델을 정립하고 신뢰성 있는 다중 경로를 통해 데이터를 안전하고 신속하게 전송할 수 있는 기술을 연구할 계획이다.

References

[1] George I. Seffers, *NATO Strudying Military IoT Applications(2017)*, Retrieved Apr. 12, 2018. from https://www.afcea.org/content/Article-nato-studying-military-iot-applications.

[2] Nicholas Fearn, *US Army is using IoT tech and data to transform warfare(2017)*, Retrieved Apr. 12, 2018. from https://internetofbusiness.com/us-army-iot-warfare/.

[3] H. Xia, J. Yu, C.-L. Tian, Z.-K. Pan, and E. Sha, “Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks,” *J. Network and Computer Appl.*, vol. 62. pp. 112-127, Jan. 2016.

[4] J. Guo, I.-R. Chen, and J. J. P. Tsai, “A survey of trust computation models for service management in internet of things systems,” *Computer Commun.*, vol. 97, pp. 1-14, Jan. 2017.

[5] K. Govindan and P. Mohapatra, “Trust computations and trust dynamics in mobile ad hoc networks : A survey,” *IEEE Commun. Survey & Tuts.*, vol. 14, no. 2, pp. 279-298, Second Quarter, 2012.

[6] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, “Quantifying trust in mobile ad-hoc networks,” *Int. Conf. Integration of Knowledge Intensive Multi-Agent Syst.*, pp. 65-70, Waltham, USA, Apr 2005.

[7] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, “Trust-based on-demand multipath routing in mobile ad hoc networks,” *IET Inf. Secur.*, vol. 4, no. 4, pp. 212-232, Dec. 2010.

[8] Mahesh K. Marina and Samir R. Das, “Ad hoc on-demand multipath distance vector routing,” *Wireless Commun. and Mob. Comput.*, vol. 6, pp. 969-988, Oct. 2006.

[9] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “New trust metric for the RPL routing protocol,” *ICICS*, pp. 328-335, Irbid, Jordan, May 2017.

[10] D. H. Keum, D. Kim, and Y.-B. Ko, “A trust-based multipath routing by considering mission criticality levels of military IoT data,” *The Korea Inst. Military Sci. and Technol.*, pp. 1492-1493, Jeju Island, Korea, Jun 2017.

[11] S. Muralidharan, A. Roy, and N. Saxena, “MDP-IoT : MDP based interest forwarding for heterogeneous traffic in IoT-NDN environment,” *Future Generation Computing Syst.*, vol. 79, pp. 892-908, Feb. 2018.

[12] Denise E. Zheng and William A. Carter, *Leveraging the Internet of Things for a More Efficient and Effective Military,* Center for Strategic & International Studies(CSIS), 2015.

금 두 호 (DooHo Keum)

2015년 8월 : 아주대학교 정보통신공학과 석사

2015년 9월~현재 : 아주대학교 컴퓨터공학과 박사과정

<관심분야> 신뢰 보장 네트워킹, 전술 네트워크, 사물인터넷(IoT), 인지무선통신

김 다 빈 (Dabin Kim)

2010년 2월 : 서울여자대학교 콘텐츠디자인학과 학사

2017년 2월 : 아주대학교 컴퓨터공학과 박사

2017년 3월~2018년 4월 : 아주대학교 정보통신연구소 박사후 연구원

2018년 5월~현재 : 국방과학연구소 연구원

<관심분야> Named Data Networking, MANET, 전술 네트워크, 신뢰 보장 네트워킹, 무선 네트워크

고 영 배 (Young-Bae Ko)

1991년 2월 : 아주대학교 컴퓨터공학 학사

1995년 2월 : 아주대학교 경영정보학(MIS) 석사

2000년 7월 : Texas A&M University (College Station) 컴퓨터공학 박사

2000년 8월~2002년 8월 : 미국 IBM T.J Watson 연구소 전임연구원

2002년 9월~2011년 : 아주대학교 정보통신대학 정보컴퓨터공학부 조/부교수

2012년~현재 : 아주대학교 정보통신대학 소프트웨어학과 정교수

<관심분야> 신뢰 보장 네트워킹, 전술 네트워크, 이동 애드혹 네트워크, 사물인터넷(IoT)