논문 19-45-02-23 The Journal of Korean Institute of Communications and Information Sciences '20-02 Vol.45 No.02
https://doi.org/10.7840/kics.2020.45.2.391

미션 크리티컬 전술 데이터 전송을 위한 고신뢰 저지연 다중경로 라우팅

금 두 호◆, 임 지 훈*, 고 영 배°

A Trusted Low-Latency Multipath Routing for Mission-Critical Tactical Data Transfer

DooHo Keum◆, Jihun Lim*, Young-Bae Ko°

요 약

전술 네트워크에서는 다양한 임무 중심 데이터와 이질적인 센서들로부터 발생하는 대량의 데이터를 신속하고 안전하게 전송하기 위한 라우팅 기술이 요구된다. 특히, 군 환경에서는 긴급성, 기밀성, 중요성을 강조하기 때문에 요구하는 데이터의 신뢰성 및 서비스 품질이 보장 되어야 한다. 이를 위해 기밀 데이터를 폐기하거나 조작하는 악의 노드들을 탐지하고 서비스 품질을 보장할 수 있는 네트워킹 기술 연구가 필요하다. 본 논문에서는 전술 네트워크 환경에서 악의적인 공격을 수행하는 노드를 탐지하고 임무 중요 데이터가 요구하는 조건을 만족시킬 수 있는 신뢰성 및 저지연 라우팅 기술을 제안한다. 본 제안 기술은 OPNET 시뮬레이터를 통해 성능을 검증하고 기존 다중 경로 라우팅 기술 대비 향상된 네트워크 성능 결과를 확인하였다.

Key Words : Tactical Network, Mission critical, Trustworthiness, Quality of Service, Trusted Low-Latency Multi-path routing

ABSTRACT

In the tactical network, a reliable routing protocol is required to quickly and safely transfer huge amounts of data from various mission critical data and sensors. In particular, the military environment emphasizes the urgency, importance, confidentiality of data so the reliability and quality of the required data must be guaranteed. This requires a routing protocol that can detect nodes performing malicious attacks that discard and modify confidential data to ensure the quality of service. In this paper, we proposed a trusted low-latency routing protocol that can detect malicious nodes and satisfy the requirements of mission critical data. The proposed scheme is verified through OPNET simulator and confirmed the improved network performance result compared to the existing schemes.

※ 본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크기술 특화연구센터 사업의 일환으로 수행되었습니다.(UD190033ED)

◆ First Author : Ajou University Department of Computer Engineering, dooho1000@ajou.ac.kr, 학생회원
° Corresponding Author : Ajou University Department of Computer Engineering, youngko@ajou.ac.kr, 종신회원
* Ajou University Department of Computer Engineering, limbee94@ajou.ac.kr
논문번호 : 201910-242-0-SE, Received October 20, 2019; Revised November 19, 2019; Accepted November 26, 2019

Ⅰ 서 론

미래 전술 네트워크는 사물인터넷 기술이 접목되고 무인체계의 중요성이 강조되면서 다양한 센서로부터 발생하는 대량의 데이터를 신속하고 정확하게 처리하기 위한 기술이 요구된다. 최근 전술 네트워크를 고려한 사물인터넷 기술은 병사들의 생존성 보장을 위한 센싱 기술, 적재적소 타격을 위한 IoT 기술, 상황인지-타격 자율화 시스템, 군수품 RFID 태그 및 군수관리 체계를 지원하기 위한 센싱 기술, 무인체계를 지원 및 통제하기 위한 기술들이 활발하게 연구되고 있다. 향후 미래 전술네트워크는 신속하고 정확한 지휘 통제를 하기 위해 다양한 IoT 센서들이 무인로봇, 발사포, 군수품 등에 부착되어 대량의 데이터를 발생할 것으로 예상되며 이를 지원하기 위해 신뢰성 있는 네트워킹을 위한 연구 개발의 중요성이 강조된다.[1-3]

그러나 전술 네트워크가 무인화되고 다양한 디바이스들이 증가함에 따라 서비스 품질이 저하되고 사이버 위협이 증가하고 있다. 악의적인 노드가 임무 중요 데이터를 수신 받고 이를 폐기 및 탈취하여 임무 중요 데이터가 손실되거나 디바이스 수가 증가함에 따라 자원 제약적인 네트워크 환경에서 통신 성능이 저하되는 문제가 발생할 수 있다.

이러한 문제를 해결하기 위한 종래 기술은 주변 노드의 패킷 전달 및 폐기 행위를 관찰하고 수집하여 평가하는 신뢰 값과 노드 간 예상 전송 시도를 카운트하는 ETX(Expected Transmission Count), 전파 지연(Propagation Delay), 전송 지연(Transmission Delay)을 함께 고려하여 신뢰성 및 서비스 품질의 라우팅 메트릭으로 활용하는 등의 연구가 진행되었다. 또한 전술 네트워크 환경에서는 QoS 문제를 해결하기 위해 데이터의 우선순위를 고려하여 대역폭 및 큐(Queue) 관리를 통해 병목현상을 해결하고 임무 중요도가 높은 데이터를 우선적으로 보장하고자 하였다. 종래 기술들은 주로 단일 경로에서 신뢰성을 확보하고자 했으며 다중 경로는 단절이 발생 하였을 때 대체 경로로 활용하는 방향으로 연구되었다. 하지만 대용량의 데이터가 발생 할 때 단일 경로를 통해 전송한다며 큐 관리, 대역폭 관리만으로 처리하기 어려운 상황이 발생할 수 있으며, 우선순위가 낮은 데이터의 경우 전송하지 못하는 상황도 발생 할 수 있다.

본 논문에서는 이러한 문제점을 해결하기 위해서 데이터별 신뢰도 및 QoS 요구사항을 만족하는 다중 경로를 통해 임무 중심의 전술 데이터를 분산하여 전송함으로써 데이터의 신뢰성 및 서비스 품질을 보장하고자 한다.

Ⅱ. 관련 연구

2.1 신뢰 평가 방법

신뢰 평가 방법으로는 주로 각 센서 노드가 직접적으로 신뢰 평가를 수행하는 직접 신뢰평가(Direct Observation or Direct Trust)가 있으며 이를 기반으로 서로 신뢰 평가 값을 추천을 해주는 간접 신뢰평가(Indirect Trust or Recommendation) 방법이 있다. 또한 직접 신뢰평가 방법과 간접 신뢰평가 방법을 함께 고려하여 적용하는 하이브리드 신뢰평가(Hybrid Trust) 방법이 있다.[4,5] 이러한 방법들은 각 연구 환경 및 목적에 따라 설정 될 수 있으며 본 논문에서는 직접 신뢰 평가를 통한 신뢰 평가 방법과 서비스 품질을 함께 고려한 방법을 연구한다. 직접 신뢰 평가는 주로 활용되는 패킷 포워딩 비율을 통해 계산한다. 패킷 포워딩 비율은 평가노드가 피평가노드에게 패킷을 전달하고 무차별 모드(Promiscuous Mode)를 통해 피평가노드가 패킷을 송신하는 행동을 관찰하여 포워딩 여부를 확인하고 전송한 횟수를 통해 계산될 수 있다. 간접 신뢰 평가 방법은 각 노드가 평가한 직접 신뢰 평가를 추천받아서 활용하는 방법이다. 추천을 받은 결과를 활용하여 직접 신뢰평가를 수행하지 않고 확인하고자 하는 노드의 신뢰 값을 얻을 수 있다. 하이브리드 신뢰 평가 방법은 직접 신뢰 평가 방법과 간접 신뢰 평가 방법을 모두 고려하여 계산하고 신뢰 값을 도출하는 방법이다. 높은 이동성을 가진 노드나 통신 환경이 좋지 않을 때 직접 신뢰 평가한 값만을 고려한다면 신뢰성이 떨어질 수 있지만 다른 노드들이 평가한 결과 값을 같이 고려하면 신뢰도의 정확도를 보다 높일 수 있다. 하지만 직접 신뢰 평가와 간접 신뢰 평가를 모두 고려하고 계산하는 방법에 따라 오버헤드가 발생 할 수 있기 때문에 고려하는 환경에 맞게 신뢰 평가 방법을 수행하도록 해야 한다.

2.2 신뢰 기반 라우팅

신뢰 기반 라우팅 방법으로는 신뢰 평가 방법을 통해 도출되는 값을 라우팅 메트릭으로 활용하여 경로를 선정 및 유지하는 내용을 다룬다. 본 절에서는 MANET 환경에서 신뢰 보장 라우팅 기술에 대한 연구를 소개한다.[6-9]

AOTDV[6](Ad hoc On-Demand Trusted-path Distance Vector routing) 기술은 AOMDV[7](Ad hoc On-demand Multipath Distance Vector routing)를 기

반으로 신뢰성을 고려하여 악의 노드를 탐지하고 성능을 검증한 논문이다. AOMDV의 경우 AODV에서 다중 경로를 생성 및 유지하기 위해 확장한 기술로 대표적인 다중 경로 기술로 분류 된다. AOTDV는 경로를 탐색 할 때 AOMDV 방식과 유사하게 동작하는데 경로 탐색 메시지 RREQ(Route Request)를 목적지 노드가 수신하고 k개의 RREP(Route Reply)를 전송하는 방법에서 차이점이 있다. AOTDV는 라우팅 메트릭으로 경로 신뢰도인 PTV(Path Trust Value)를 도출하기 위해 각 노드가 직접 신뢰 평가를 수행해야 하는데, 이를 위해 단위 시간당 노드가 패킷을 포워딩한 비율을 컨트롤 패킷과 데이터 패킷을 모두 고려하여 측정한다. 경로 신뢰도 값은 각 노드가 주기적으로 직접 신뢰 평가한 값을 목적지까지 전달하면서 누적 곱하여 도출한다. 하지만 하나의 경로를 통해 중요 데이터를 전달하기 때문에 링크 하나를 사용했을 때 발생할 수 있는 병목 현상과 같은 문제를 해결하기 어려운 점이 있다. MC-AOTDV는 이러한 문제점을 해결하기 위해 개발되었다. MC-AOTDV[8,9]은 중요데이터를 동시에 다중 경로를 통해 전송하는 알고리즘을 소개한다. 알고리즘은 국방 IoT 데이터를 중요도에 따라 구분하고 중요 데이터 일수록 신뢰성을 보장받을 수 있는 방법이다. 이 기술에서 소개하는 방법을 통해 부하분산 효과를 보면서 주요 데이터의 신뢰성을 보장 할 수 있었다. 하지만 MC-AOTDV는 단순하게 패킷을 일정 확률로 폐기시키는 그레이 홀 공격 노드만을 고려하여 제안되었기 때문에 패킷을 고의로 지연시켜서 임무 중심의 작전에 악영향을 끼칠 수 있는 공격에 노출된다. 본 논문은 이러한 부분을 고려하여 신뢰성 및 저지연 요소를 함께 고려한 라우팅 메트릭을 제안함으로써 성능을 검증하고 기존 기술과 비교 분석한다.

Ⅲ. 제안 기법

본 논문의 제안 기법은 1. 임무 중요 데이터 트래픽 별 요구사항 및 특성 정의, 2. 신뢰성 및 서비스 품질 다중경로 탐색 방법, 3. 신뢰성 및 서비스 품질 경로 할당 및 유지 방법으로 구성된다.

3.1 임무 중요 데이터 트래픽 별 요구사항 및 특성 정의

전술 네트워크 환경에서 신뢰성 및 서비스 품질 다중경로 라우팅 기법을 기술하기 위해 미 육군 FCS(Future Combat System)에서 활용되는 전술 데이터의 특징 및 요구사항을 활용한다. FCS의 서비스 클래스는 수개의 카테고리 및 클래스로 나눠지고 정보의 타입에 따라 긴급한 정보, 시간 제약 정보 순으로 우선순위를 분류하며 성능 요구사항을 규정한다. 또한 PHB(Per Hop Behavior)는 전송 우선순위에 따라 EF(Expedited Forwarding), AF(Assured Forwarding), BE(Best Effort) 등으로 구분 될 수 있으며 FCS 트래픽 속성에 따라 맵핑 된다. FCS 트래픽은 협업형 C2(Collaboration Command Control), 상황인식(Situational Awareness), 타깃 데이터(Target data), 화력요청(Fire request), 메디컬 상태(Medical state), 센서 테스킹(sensor tasking), 지역 데이터(Terrain data) 등으로 구분될 수 있으며 각 트래픽에 따라 음성, 영상, 문자, 대용량 데이터의 중요도가 정의될 수 있다.

그림 1은 임무 중요도(Mission Criticality) 전술 데이터의 타입을 구분하고 데이터를 전송하기 위해 요구되는 경로 신뢰도와 단-대-단 지연시간 특성을 정의한다.

Mission-Critical	FCS Traffic	Data Type	PTV Requirement	E2E Delay Requirement	Time attribute	PHB
A	Collaborate C2	Voice	PTV>=0.9	250ms	Real-time	EF
	Fire request					
	Medical status					
B	Collaborate C2	Video	PTV>=0.75	220ms	Real-time	AF4
	Situation awareness					
C	Situation awareness	Chat	PTV>=0.5	300ms	Non-Real	AF3
D	Damage Assessment	Sensor Data, Message	PTV>=0.25	1000ms	Non-Real	AF2
	Sensor tasking					
E	Terrain Data	Bulk Data	PTV>=0	300ms	Non-Real	AF1

그림 1. 임무 중요 데이터 트래픽 별 요구사항 및 특성
Fig. 1. Requirements and characteristics by mission critical data traffic

본 논문에서는 경로 신뢰도와 QoS 메트릭을 함께 고려하여 경로의 신뢰성 및 서비스 품질 값을 도출하고 임무 중요 데이터를 신뢰성 및 서비스 품질이 보장된 경로로 전송하고자 한다.

3.2 신뢰성 및 서비스 품질 다중경로 탐색 방법

신뢰성 및 서비스 품질 기반 다중경로 라우팅 기법의 경로 탐색 방법은 기존 애드 혹 환경에서의 다중경로 라우팅 기법인 AOMDV와 유사하게 동작하지만 신뢰된 경로를 탐색하는 방법과 전술 데이터의 임무 중요도에 따라 경로 구성 및 유지를 다르게 한다는 점에서 차이가 있다. 신뢰된 경로를 탐색하기 위해 게이트웨이 루트 노드가 각 센서 노드로 RREQ(Route REQeust) 메시지를 전송하고 센서 노드가 여러 개의 RREP(Route REPly) 메시지를 전송하면서 측정한 NTV(Node Trust Value)와 지연시간 정보를 전달한다. NTV는 무작위 모드(Promiscuous mode)를 통해 주변 노드의 행위를 관찰하여 신뢰 값을 도출하며 일반적으로 활용되는 패킷 포워딩 비율(PFR : Packet Forwarding Ratio)을 통해 아래와 같이 계산된다.[6]

$$NTV_{i,j}(t) = w_1 * CPFR_{i,j}(t) + w_{2*} DPFR_{i,j}(t) \quad (1)$$

i노드가 j노드를 평가한 컨트롤 패킷에 대한 포워딩 비율($CPFR_{i,j}(t)$: Control PFR)과 데이터 패킷에 대한 포워딩 비율 ($DPFR_{i,j}(t)$: Data PFR)을 모두 고려하여 계산된다. PFR은 아래와 같이 계산되며 여기서 $S_{i,j}(t)$는 단위시간(t) 동안 i 노드가 j에게 패킷을 송신한 전체 패킷 수를 의미하며 $F_{i,j}(t)$는 단위시간(t) 동안 j 노드가 포워딩한 패킷 수를 의미한다.

$$PFR^{d}_{i,j}(t) = \frac{F_{i,j}(t)}{S_{i,j}(t)} \quad (2)$$

그림 2는 계산된 NTV 값에 따라 분류되는 노드의 특성을 의미하며 NTV 값이 일정 한계점 이하인 노드는 악의 노드로 판단하여 블랙 리스트에 업데이트 되고 네트워킹을 위한 라우팅 과정에서 배제할 수 있다. 이는 사용자 및 운용자의 의도 또는 판례에 따라 다르게 운용할 수 있다.

Trust Level	NTV scope	Node attribute
1	1>NTV>=0.9	Complete trustworthy node
2	0.9>NTV>=0.75	Trustworthy node
3	0.75>NTV>=0.5	Low trustworthy node
4	0.5>NTV>=0.25	Suspect node
5	0.25>NTV>=0	Malicious node

그림 2. 노드 신뢰도 레벨에 따른 범위
Fig. 2. Scope for node trust level

이처럼 경로 상의 블랙홀(Black hole attack)이나 그레이홀(Grey hole attack)과 같이 패킷을 폐기하는 공격을 수행하는 악의 노드가 존재한다면 NTV 값이 낮아지므로 악의 노드로 판단하여 배제 및 공유하고 안전한 노드로 구성된 통신이 가능하다.

또한 게이트웨이 노드가 경로에 대한 신뢰값(PTV : Path Trust Value)을 계산하기 위해 각 센서들이 측정한 NTV 값을 누적 곱하여 아래와 같이 계산하고 게이트웨이까지 전달한다.[6]

$$PTV = \prod NTV (0 \leq PTV < 1) \quad (3)$$

지연시간의 경우 각 센서 노드들이 측정한 전송지연(Transmission Delay)와 전파지연(Propagation delay)을 고려하여 누적 합하여 게이트웨이까지 전송되도록 한다.

복수개의 RREQ를 수신한 센서 노드는 무분별한 경로 생성을 방지하기 위해 데이터의 신뢰도 레벨 수를 고려하여 최대 5개의 경로에 대해 RREP를 생성한다. 최종적으로 RREP를 수신한 루트 노드는 생성된 k개의 경로를 업데이트 하고 경로의 종단간 지연시간 (ω : End-to-End Delay)과 신뢰 값을 함께 고려하여 PQTV(Path QoS and Trust Value)를 아래와 같이 계산한다.

$$PQTV_r(t) = (\omega_r(s) \times (1 - PTV)) \quad (4)$$

따라서 각 경로의 신뢰성 및 서비스 품질을 확인할 수 있다. PQTV 값이 도출되면 그 중 가장 값이 작은 최솟값(min)이 경로 신뢰성 및 서비스 품질이 좋은 경로이며 경로 선정 알고리즘에 따라 임무 중요 전술 데이터를 신뢰성 및 서비스 품질이 보장된 경로로 전송할 수 있다.

3.3 신뢰성 및 서비스 품질 경로 할당/유지 방법

신뢰성 및 서비스 품질 경로 할당/유지하기 위해 주기적으로 컨트롤 메시지를 주고받으며 루트 노드인 게이트웨이는 각 경로를 업데이트하기 위한 정보를 알려주고 각 노드들은 자신들이 측정한 NTV 및 Delay 값을 주기적으로 목적지 게이트웨이에 전달하

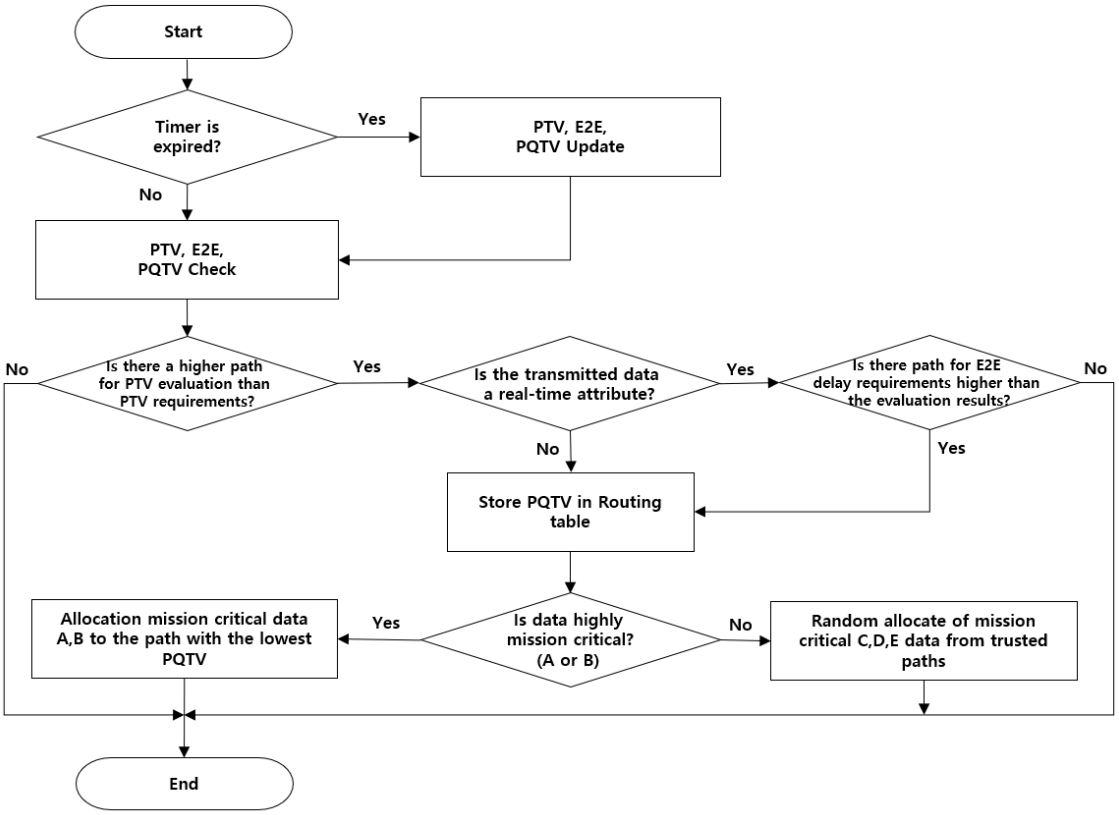

그림 3. 제안된 기법에서 요구조건을 만족하는 경로를 할당하기 위한 전체 과정
Fig. 3. The whole process for allocating paths satisfying the requirements in the proposed scheme

게 된다. 따라서 주기적으로 각 경로의 신뢰성 및 서비스 품질을 확인할 수 있다.

그림 3은 제안된 기법에서 요구조건을 만족하는 경로를 할당하기 위한 전체 과정을 나타낸다.

임무 중요 데이터를 전송하기에 앞서, 게이트웨이는 주기적으로 PTV, End-to-End Delay 값을 확인하고 조건에 맞는 경로에 대해 PQTV 값을 업데이트한다. 최종적으로 임무 중요도가 높은 데이터인지 여부를 확인하고 센서 노드가 데이터를 전송할 때 어떤 다중 경로를 선정해서 데이터를 전송해야 하는지에 대한 라우팅 테이블 정보를 센서 노드에 전송한다. 센서 노드는 이를 통해 임무 중요 데이터를 어떤 다중 경로를 통해 전송해야 하는지 확인하고 적응적으로 신뢰성 및 서비스 품질이 보장된 경로를 할당해 줄 수 있다.

본 논문에서는 각 임무 중요 데이터를 전송하기 위한 경로의 신뢰도를 판단하기 위해 데이터별 PTV 요구사항과 실제 측정된 PTV 값을 비교 한다. 중요한 데이터 일수록 악의 노드에게 노출되면 안 되는 중요 정보이기 때문에 경로에 대한 신뢰 값이 요구조건을 만족해야만 전송할 수 있도록 한다.

PTV가 만족한다면 보내고자 하는 데이터의 실시간성을 확인하고 실시간성 데이터에 대해 요구되는 지연시간과 측정된 지연시간을 비교한다. 군에서의 데이터 요구사항은 최악의 지연시간 등 통신이 어려운 성능의 수치를 기준으로 규정하고 있으며 이를 만족하지 못하면 음성 및 영상 등을 송수신할 때 통신에 큰 어려움이 있다고 판단한다. 따라서 본 논문에서는 요구사항을 만족하는 경로가 없을 경우 음성과 같이 실시간성 및 중요도가 매우 높은 임무중요데이터는 신뢰 경로가 보장될 때까지 네트워크 망을 통해 전송하지 않는다. 따라서 이 경우 운용자는 별도의 음성통신주파수를 이용하는 등 대안방안을 사용하여 통신해야 한다.

요구되는 성능을 만족하는 실시간성 데이터는 PQTV 값을 라우팅 테이블에 업데이트하고 성능을 만족하지 못하면 라우팅 테이블에 저장하지 않고 패킷을 송신하지 않는다. 요구되는 성능을 만족하는 경우

최종적으로 임무 중요도가 높은 데이터인지 여부를 확인하고 중요도가 높은 데이터는 저장된 PQTV 값 중 최솟값을 통한 경로를 선정하고 비교적 낮은 데이터는 조건을 만족하는 경로 중 PQTV를 랜덤으로 선정한다.

그 이유는 임무 중요도가 높은 데이터의 신뢰성 및 서비스 품질을 보다 보장하기 위함이며 상대적으로 중요도가 낮은 데이터도 요구조건을 만족하는 경로 중 랜덤하게 정하기 때문에 성능 상 신뢰성은 보장되기 때문이다. 본 논문에서는 임무 중요도가 높은 데이터를 A,B로 정하고 상대적으로 낮은 데이터를 C,D,E로 가정하였지만 이 또한 운용자의 의도 및 판례에 따라 운용할 수 있다.

그림 4는 센서 노드가 게이트웨이 노드에게 송신할 때 임무 중요 데이터 별 경로를 할당하는 예를 나타낸다.

PQTV 평가 결과로 1번 경로는 0.044, 2번 경로는 0.076, 3번 경로는 0.021, 4번 경로는 0.121, 5번 경로는 0.155 값이 나온다. 임무 중요 데이터 A를 전송할 수 있는 경로는 요구사항을 모두 만족한 3번 경로가 할당되었고, B의 경우는 1번 3번 경로가 요구사항을 모두 만족하는 경로이며 이 중 PQTV가 낮은 3번 경로를 선정하여 데이터를 전송하게 된다. C, D, E 데이터의 경우 요구사항을 만족하는 경로는 1,2,3번 경로이며 이 중 무작위로 선정되어 그림 4와 같이 경로 할당이 되어 전송 될 수 있다. 경로 4, 5와 같이 그레이홀 공격을 수행하거나, 패킷 전송을 지연시키는 공격을 수행하면 악의 노드로 탐지하여 배제되기 때문에 각 센서 노드들은 신뢰성 및 서비스 품질이 보장된 경로로 데이터를 전송할 수 있다.

Ⅳ. 성능 평가

본 장에서는 제안기법의 성능을 검증 및 평가하기 위해 시뮬레이션 환경을 표 1과 같이 설정하였다. 네트워크 시뮬레이터는 OPNET 18.0 버전을 사용하였으며 라우팅 프로토콜 AOMDV, AOTDV, MC-AOTDV[8]와 제안 기법을 구현 및 비교 분석하였다. 시뮬레이션 노드는 총 30개 노드를 배치하고 그 중에서 패킷을 50%확률로 드롭 하는 그레이홀 공격 노드 1개, 패킷 포워딩 시간을 지연시키는 악의 노드 1개로 총 악의 노드 2개를 고정 배치하여 설정하였다. 임무 중요도에 따른 데이터의 정보는 전술 네트워크 환경에서 고려되는 음성, 영상 데이터 등의 종류, 사이즈, 주기 등을 고려하여[3,10] CBR 트래픽 모델로 고정하여 설정하였다. MAC 프로토콜은 CSMA/CA를 사용하고 PHY는 군 환경에서의 자원 제약적인 무선통신 사항을 고려하여 SRW(Soldier Radio

표 1. 시뮬레이션 환경
Table 1. Simulation environment

Parameters	Values
Simulator	OPNET 18.0
Simulation time	180s
Routing Protocol	AOMDV, AOTDV, MC-AOTDV, Proposed scheme
Number of nodes	30
Number of malicious node	2
Traffic Type (Avg. Packet size)	VoIP G.723.1(24bytes)
	Video Surveillance H.264(500bytes)
	Chat(100bytes)
	Data, Message(120bytes)
	Bulk Data(2000bytes)
MAC Protocol	CSMA/CA
PHY	802.11b 2Mbps

Route	PTV Result	E2E Delay Result(s)	$PQTV_r(t)$	Mission Critical based route allocation
1	0.8	0.220	**0.044**	C, D
2	0.7	0.255	**0.076**	E
3	0.9	0.210	**0.021**	A, B
~~4~~	~~0.2~~	~~0.152~~	~~**0.121**~~	-
~~5~~	~~0.5~~	~~2.310~~	~~**0.155**~~	-

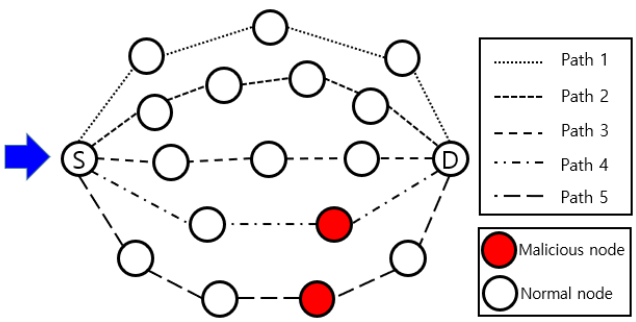

그림 4. 임무 중요 데이터 별 경로 할당 예
Fig. 4. Example of path allocation by mission critical data

Waveform)에서 운용하는 2Mbps로 설정하였다.[11] 성능평가 척도로는 PDR(Packet Delivery Ratio), 지연시간(Delay)를 비교 분석하였다. PDR은 소스 노드에서 목적지 노드까지 송신한 패킷 양과 수신한 패킷 양을 고려하여 계산되고 Delay는 송신 노드가 패킷이 송신한 시간부터 목적지 노드가 패킷을 수신한 시간까지의 종단간 지연시간을 측정하였다.

그림 5는 경과 시간에 따른 패킷 전달 비율을 나타낸다. 시뮬레이션 결과 AOMDV는 홉 카운트 기반의 라우팅 메트릭을 사용하기 때문에 경로 상의 패킷을 악의적으로 폐기하는 노드가 있을 경우 탐지하지 못하고 해당 경로를 통해 데이터를 전송하기 때문에 낮은 PDR을 보이는 결과를 확인하였다. AOTDV의 경우 경로 신뢰도 기반의 라우팅 메트릭을 사용하기 때문에 패킷을 임의적으로 폐기하는 그레이홀 공격을 수행하는 악의 노드를 탐지 및 배제하고 안전한 경로를 통해 데이터를 전송하기 때문에 AOMDV보다 높은 PDR 결과를 나타내지만 한 경로를 통해 데이터를 전송하기 때문에 전술 네트워크를 고려한 실험 환경과 같이 데이터 전송 비율이 높을 경우, 병목현상으로 인해 PDR이 60~70%로 전송되는 결과를 확인할 수 있다. 제안 기법의 경우 신뢰도 및 저지연 기반의 고신뢰 라우팅 메트릭을 사용하기 때문에 그레이홀 공격을 수행하는 악의 노드를 탐지할 수 있으며 고신뢰 다중 경로를 통해 부하 분산 효과를 보장받아 병목현상을 방지할 수 있기 때문에 AOTDV 보다 높은 PDR을 보이는 결과를 확인하였다.

그림 6는 경과시간에 따른 평균 지연시간을 나타낸다. AOMDV의 경우 홉 카운트를 고려한 메트릭을 사용하여 가장 홉 수가 적은 경로를 선정하고 데이터를 전송하기 때문에 제안기법과 AOTDV에 비해 평균 지연 시간이 가장 낮게 측정되는 결과를 확인할 수 있다. 하지만 PDR이 약 50%로 현저하게 낮기 때문에 신뢰성 있는 통신이라고 보기 어렵다. AOTDV의 경우 경로 신뢰도를 고려한 메트릭으로 경로를 선정하기 때문에 그레이홀 공격을 수행하는 경로는 탐지 할 수 있지만 패킷 포워딩 시간을 지연시키는 악의 노드가 있는 경로를 탐지하지 못하고 해당 경로를 통해 데이터를 전송하게 되어 지연 시간이 AOMDV, 제안기법과 대비했을 때 가장 오래 걸리는 결과를 나타낸다. 제안기법의 경우 경로 신뢰도 및 저지연 라우팅 메트릭을 사용하기 때문에 그레이홀 공격과 패킷 포워딩 지연 공격을 수행하는 노드가 있는 경로를 탐지 및 배제하고 신뢰된 경로를 사용하여 데이터 패킷을 전송하게 된다. 따라서 AOTDV보다 지연 시간이 더 짧은 다중 경로를 통해 데이터를 전송하는 결과를 확인할 수 있다.

그림 7은 임무 중요 데이터 ToS 1,2의 평균 지연시간에 대해 MC-AOTDV와 제안기법을 비교 분석한 결과를 나타낸다. MC-AOTDV의 경우 경로 신뢰도 기반의 라우팅 메트릭을 고려하여 다중 경로를 선정하기 때문에 임무 중요도가 높은 데이터라도 패킷 포워딩을 지연시키는 악의 노드가 존재하는 경로가

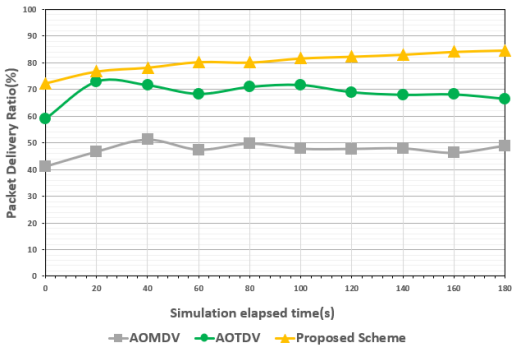

그림 5. 경과 시간에 따른 패킷 전달 비율
Fig. 5. Packet delivery ratio over elapsed time

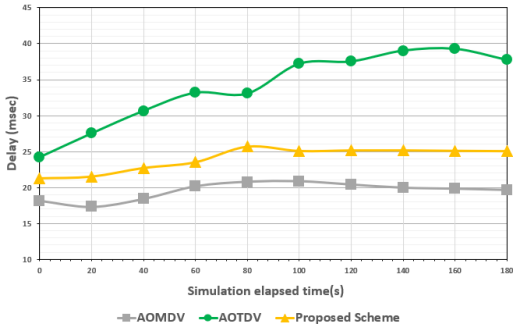

그림 6. 경과 시간에 따른 평균 지연 시간
Fig. 6. Average delay over elapsed time

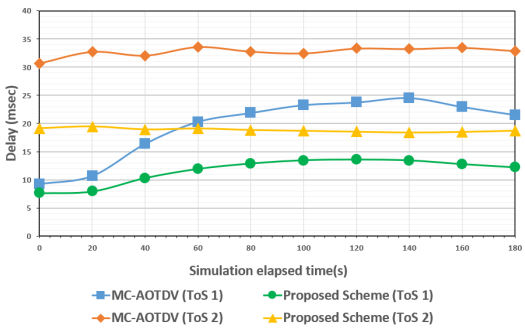

그림 7. 임무 중요데이터 ToS1,2에 대한 평균 지연시간
Fig. 7. Average delay for ToS 1,2 over elapsed time

가장 신뢰된 경로라고 오판하여 데이터를 전송하기 때문에 제안기법과 대비하여 지연시간이 오래 걸리는 결과를 확인할 수 있다. 임무 중요 데이터 마다 요구되는 지연시간과 만족해야 하는 서비스 품질이 있는데 저지연 요소를 고려하지 못했을 경우 음성이 끊겨서 들리거나, 인식하기 힘든 영상의 품질을 수신한다면 임무를 수행할 때 많은 제약이 초래될 수 있다. 또한 크기가 큰 데이터의 경우 서비스 품질을 만족하지 못하면 데이터를 전송하지 않고 다른 데이터의 전송을 위해 링크의 대역폭을 줄여주는 방법도 고려될 수 있다. 제안기법의 경우 경로 신뢰도 및 저지연 기술을 고려한 라우팅 메트릭이 동작하기 때문에 패킷을 임의로 드롭하는 악의 노드와 패킷 포워딩 시간을 지연시키는 악의 노드가 포함된 경로를 탐지 및 배제하고 고신뢰 경로를 통해 임무 중요 데이터를 우선적으로 전송하기 때문에 ToS 1, 2 데이터 모두 MC-AOTDV에 비해 낮은 지연시간을 보이는 결과를 확인하였다. ToS 1, 2데이터가 같은 경로를 사용할 때에도 지연시간에 차이를 보이는 이유는 ToS 1은 음성 데이터, ToS 2는 비교적 크기가 큰 영상 데이터를 발생시켜 실험하였기 때문에, 전송/전파 지연, 큐잉 지연 등의 요소에 따라 ToS 1이 ToS2보다 지연시간이 낮은 결과를 확인할 수 있다.

V. 결 론

본 논문은 전술 네트워크 환경에서 악의 노드를 탐지하고 신뢰성 및 서비스 품질을 보장하는 경로를 통해 임무 중요 데이터를 전송하는 다중 경로 라우팅 기술을 제안한다. 전술 데이터는 각 속성에 따라 긴급성 및 신뢰성이 보장되어야 하기 때문에 신뢰성 및 서비스 품질을 보장하기 위한 연구가 필수적이다. 본 논문에서 제안한 기법은 신뢰성 및 서비스 품질의 요구조건에 부합하면서 신속하고 안전하게 데이터를 전송할 수 있는 기법으로 타 기법과 비교해 성능 우의를 보인다. 향후 연구로 신뢰성 및 서비스 품질을 보다 향상시키고 신뢰된 다중 경로를 통해 신속하고 안전하게 전송 할 수 있는 기술을 연구할 계획이다.

References

[1] George I. Seffers, *NATO Strudying Military IoT Applications*, 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*, Retrieved Apr. 12, 2018. from https://internetofbusiness.com/us-army-iot-warfare/.

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

[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] 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.

[7] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," *Wireless Commun. and Mob. Comput.*, vol. 6, pp. 969-988, Oct. 2006.

[8] D. H. Keum, D. Kim, and Y.-B. Ko, "A trust guaranteed multi-path routing protocol by considering mission-critical IoT data," *J. KICS*, vol. 43, no. 06, pp. 994-1004, Jun. 2018.

[9] 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.

[10] 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.

[11] B. G. Jeffrey and W. Foley, "WIN-T increasing the power of battlefield communications," *Army Communicator*, vol. 33, no. 3, 2008.

금 두 호 (DooHo Keum)

2015년 8월 : 아주대학교 정보통신공학과 석사
2015년 9월~현재 : 아주대학교 컴퓨터공학과 박사과정
<관심분야> 신뢰성 보장 네트워킹, 애드혹 네트워크, 사물인터넷(IoT), 전술네트워크
[ORCID:0000-0002-8267-2331]

임 지 훈 (Jihun Lim)

2018년 2월 : 아주대학교 소프트웨어학과 학사
2018년 3월~현재 : 아주대학교 컴퓨터공학과 석사과정
<관심분야> 신뢰 보장 네트워킹, 센서 네트워크, 사물인터넷(IoT), 전술 네트워크
[ORCID:0000-0001-6342-9267]

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)
[ORCID:0000-0002-8799-1761]