On the Potential of SDN Enabled Network Deployment in Tactical Environments

George Lazaridis, Kostas Papachristou, Anastasios Drosou, Dimosthenis Ioannidis, Periklis Chatzimisios, Dimitrios Tzovaras

On the potential of SDN enabled network deployment in tactical environments*

George Lazaridis[1,2], Kostas Papachristou[1], Anastasios Drosou[1], Dimosthenis Ioannidis[1], Periklis Chatzimisios[2], and Dimitrios Tzovaras[1]

[1] Centre for Research & Technology Hellas, Thessaloniki, Greece
{glazaridis, kostas.papachristou, drosou, djoannid, dimitrios.tzovaras}@iti.gr
[2] International Hellenic University, Thessaloniki, Greece
{glazaridis, pchatzimisios}@ihu.gr

Abstract. Modern critical operations and defence applications require highly demanding information and communication systems, making ad hoc networks, which are mainly used nowadays in tactical zones, to be difficult to manage. The evolution of the Software Defined Networking (SDN) technology has brought new perspectives to security and defence applications, making them more reliable, more stable, more secure and more portable. This research paper proposes an SDN topology for secure communications in a tactical environment, overcoming several challenges that a conventional network faces. Moreover, an Artificial Intelligence (AI) methodology, exclusively used in SDN environments is presented, providing Quality of Service (QoS) features to the network, based on which rerouting paths can be calculated. Finally, our routing methodology is illustrated using representative evaluation scenarios.

Keywords: Software Defined Networking · Defense · Security · Artificial Intelligence · OpenFlow · Quality of Service.

1 Introduction

Even though the field of Artificial Intelligence (AI) research emerged in 1956 at a workshop at Dartmouth College, it has made significant progress over the years, both in industry and academia [6]. The rapid development of AI has also brought about great changes in the field of defense and security systems, which combine a large number of Internet of Things (IoT) devices being capable of accumulating quantities of data, regarding the environment they are operating in, as well as information related to their own operation. Furthermore, safe communications in a tactical assembly area or in a military camp, is an aspect that should be seriously considered. In order to circulate trusted information through defense and security systems, reliable communication networks should be established,

* This work has been partially supported by the European Commission through project SDN-microSENSE funded by the European Union Horizon 2020 programme under Grant Agreement no 833955. The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the European Commission.

taking advantage of AI techniques. These types of communication networks face several challenges, due to the outdoor environment they operate in, compared to conventional networks. They should be distinguished by portability in order to be easily deployed in any environment and operate with low power consumption. Moreover, they should be able to cover a large area of interest and be easily extendable, depending on the needs of the network deployment. Communication networks are facing the challenge of sustainability in environments with high vegetation, ground irregularities, where Quality of Service (QoS) and the data transmission rates are poor. Tactical networks, should be able to adapt transmission paths and overcome any malfunction or destruction of routing hardware. All these challenges are bypassed, and the survivability of the communication network is achieved thanks to topology of the SDN network and the rerouting techniques that the AI algorithms offer.

Over the past decade, SDN has majorly evolved, leading to a new era in the area of networks. Major technology conglomerates, such as Facebook, Google or Amazon have introduced the SDN technology to their complex data centers. The innovative approach behind SDN is the introduction of dynamic and programming methods to automate network management processes [2]. Traditional networks' architecture, consist of intermediary devices, such as a routers or switches, each of which has its own control plane and takes decisions independently regarding the forwarding policy of each packet. On the other hand, SDN virtualizes the control plane by moving it to a central place, commonly called SDN controller. The major advantages of introducing the SDN technology to defense and security domain applications include the centralized view of the entire network, the low overall operating and equipment costs, the granular security, the ability to shape and control data traffic by implementing AI-based QoS provisioning algorithms and the offer of enhanced flexibility, scalability and efficiency compared to traditional networks. Current routing algorithms in non-SDN networks, such as Open Shortest Path First (OSPF) [12], can only support best-effort services. In other words, the network makes no commitment that data will be transmitted or that it will be of acceptable quality, especially in the presence of high network traffic [1]. With the rising need for internet services, it is more critical than ever for Internet Service Providers (ISPs) to guarantee QoS provisioning.

The following are the key contributions of this paper: (i) We introduce an AI-based QoS algorithm for rerouting in SDN environments used in defense and security applications (ii) we describe a low cost SDN testbed deployed in our research center's premises, built in order to be able to adequately test the proposed AI algorithm and promote the capabilities of such SDN architectures in tactical ad-hoc networks, ensuring portability, survivability and sustainability.

The rest of our paper is organized as follows: Section 2 presents some background information on SDN technology together with the related work. Section 3 outlines the proposed defense SDN enabled network, presenting both the SDN enabled topology to be used in security and defense applications and the devel-

oped AI QoS algorithm. Section 4 demonstrates two evaluation scenarios and finally Section 5 concludes the work done and propose potential future work.

2 Background & Related work

Defence and security organizations implement advanced, integrated communication systems incorporating technologies that are cutting edge when used solely, but if these technologies are appropriately combined, they can achieve flexible and secure communications, capable of transmitting video, audio or data in tactical areas. OpenFlow is an SDN network protocol that enables the researchers to fully monitor the routing of packets in an SDN environment.

OpenFlow is an open protocol that can be used to program the data flows in SDN enabled switches and routers. Flow tables, secure channel and the OpenFlow protocol are the three elements, which make up OpenFlow. On the other hand, a SDN switch is a multi-port bridge, which allows any OpenFlow-compatible SDN controller to control its data plane. Multiple OpenFlow instances, known as datapaths, can run on a switch managed by OpenFlow. The key component of a SDN architecture and the brain of the system is the SDN controller, which is responsible for managing network flows and programming SDN enabled intermediary devices. An SDN controller uses a southbound interface, such as OpenFlow, in order to manage network elements (SDN enabled switches or routers), but it can also use a northbound interface, such as a REST API, in order to enable third-party applications to communicate with the SDN controller.

The area of SDN technology provides a wide range of research topics, therefore each of the following research papers covers a different aspect of SDN. Śliwa et al. [19] investigates how SDN techniques can promote survivability of military networks, on the strategic/operational and tactical levels. Furthermore, the SDN technology in combination with supporting techniques, will contribute in addressing the emerging complexities in military networks leading to challenging situations. Streit et al. [16] introduce in their work, a controller-equipped topology update process, which can be used in military communication applications using the SDN technology. This process was developed in order to provide a detailed and accurate description of the network topology and achieve QoS conform delivery rates, before the SDN controller begins the routing procedure. Gkioulos et al. [5] make available a comprehensive literature research of the application of the SDN technology in the wide fields of tactile networks, coalition networks, adhoc networks, tactical networks, and/or mission-critical infrastructures. Spencer et al. [14] conclude that even though SDN technology is still under research, and has been deployed only in high-bandwidth and highly secure data center ecosystems, it has a range of convincing advantages in tactical networks. However, a range of obstacles must be solved before the framework can be applied to tactical networks.

As already stated, SDN technology is evolving rapidly, leading to new kind of hybrid ad-hoc networks with SDN support, which can be used in a plethora of applications and fields. Yu et al. [18] presented in their work a practical im-

plementation of a Wireless SDN mobile ad-hoc network which takes advantage of all of the benefits of Device-to-Device (D2D) data transmissions, while still having the stability of a SDN network. Poularakis et al. [13] researched thoroughly the SDN technology in order to be used in mobile ad-hoc networks to support connectivity and service requirements, the feasibility and the reliability of such proposed networks. Moreover, in a SDN enabled tactical ad hoc network, Liu et al. [11] investigated the controller deployment issue and recommended a SDN enabled mobile ad hoc network architecture. In their work the authors also modeled and customized the controllers' implementation in order to ensure latency and reduce energy consumption. Finally, the Reliable and Dynamic Routing Technique (RaDRT) solution is analyzed in Streit et al. [15], which uses a SDN approach to control traffic flow routing in ad-hoc environments.

3 Defense SDN enabled network

3.1 Proposed SDN topology

This section describes the development and the implementation of an ad-hoc SDN enabled network, proposed for security and defense applications in tactical environments. This network is distinguished by reliability, portability, scalability, inter-connectivity, low deployment cost, easy network management, security, real-time information transfer with low latency and end-to-end encryption privacy. By its nature, a SDN network is capable of rerouting data paths programmatically, with the use of AI algorithms. The main components of SDN enabled networks are the SDN controller and a database, SDN enabled switches, a MQTT broker and different kinds of end devices, such as laptops, mobile phones, tablets, walkie-talkies, Global Positioning System (GPS) devices, which are capable of connecting to the SDN network through wireless Access Points (APs), Bluetooth gateways or direct Ethernet connections. All previously mentioned technologies are combined together in order to formulate a novel SDN topology, which can be used in a tactical environment. Figure 1 illustrates the topology of the proposed defense SDN enabled network.

SDN controller: The SDN controller is the brain of the SDN enabled network, being able to programmably compose the flow's route. For our environment, the Open Network Operating System (ONOS) was selected to be the SDN controller. ONOS is the leading open source SDN controller for building next-generation SDN solutions and it is written in the Java programming language [8]. The controller is installed on an Ubuntu-based computer running on the control plane.

Database: An InfluxDB database was installed and configured on a computer running the Ubuntu operating system, in order to collect network data regarding the performance of the SDN enabled network and more precisely the network statistics coming from each SDN enabled switch. The collected data is either used by our custom-built visualization tools in order to graphically represent

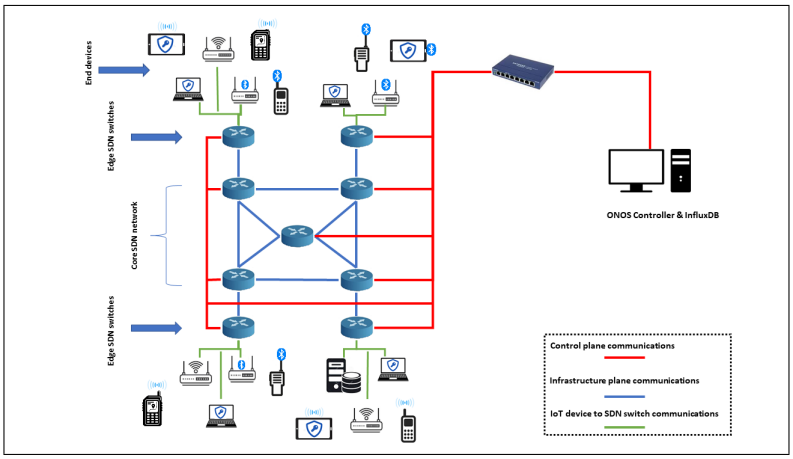


Fig. 1. Proposed defense SDN enabled network topology

network information to the administrator or forward this information to intrusion detection algorithms to further process it.

SDN enabled switches: Open vSwitch, also known as OVS, is a multilayer software switch that interconnects virtual devices in the same host or between different hosts, licensed under open-source Apache 2.0 license. OVS allows programmers to create forwarding functions in order to automate and control network traffic and supports standard management interfaces. The software-based Open vSwitch, which will be running on a Raspberry Pi 3B+ board, will form a SDN-Switch for the network. The SDN enabled switch includes a built-in Ethernet port and with the use of four USB-to-Ethernet adapters, it expands its network capabilities. The proposed SDN enabled network consists of nine SDN enabled switches. Five of them are part of the core network, where the system administrator is able to program different flow routes, while the remaining four are part of the edge network and allow different kind of devices to connect to the SDN network. The SDN switches are able to connect to each other either by taking advantage of their Ethernet interface or by using any wireless technology [7].

Wireless AP: An AP is a network device that establishes a Wireless Local Area Network (WLAN) in a desired environment. An AP uses an Ethernet cable to link to a wired router, switch, or hub and broadcasts a Wi-Fi signal to a specific location. In our case, a Raspberry Pi 3B+ board is configured to operate as AP, allowing devices to connect wirelessly to the SDN enabled network. The AP is connected via Ethernet cable to an edge SDN enabled switch, expanding the capabilities of a wired SDN network [4].

Bluetooth gateway: A Bluetooth gateway is a physical device, which allows Bluetooth-based products to connect to other devices or hardware. In our SDN enabled network, Raspberry Pi 3B+ boards are reconfigured accordingly, by adding software, in order to transform them into Bluetooth gateways and expand the connectivity of devices used in SDN networks by adding direct connection of Bluetooth devices. These types of gateways allow Bluetooth devices, used in tactical areas or military camps to firstly connect, in a secure mode, to the SDN enabled network and then translate the Bluetooth packets into MQTT packets in order to be sent over the SDN network to a desired recipient. Such tactical devices, which are capable of connecting via Bluetooth to the SDN network, could be a Bluetooth-enabled smartphone, a Bluetooth-enabled laptop or a portable GPS device [10].

MQTT broker: A Message Queuing Telemetry Transport (MQTT) broker is a server that accepts all messages from clients and forwards them to the correct destination clients. On the other hand, an MQTT client could be any system, which has installed an MQTT library and connects to an MQTT broker over a network. In the proposed SDN enabled topology, the MQTT broker is installed as an end device on a Raspberry Pi 3B+ board, using the Mosquitto MQTT Broker software. This MQTT broker is part of the Bluetooth gateway system, responsible for the transmission of Bluetooth packets translated into MQTT packets. The MQTT broker can be placed anywhere in the SDN enabled network [9].

End devices: Practically any device that contains a Bluetooth, a Wi-Fi or an Ethernet interface, could be an end device capable of connecting to the SDN enabled network. Many different kinds of devices can be used in security and defense applications, namely laptops, smartphones, portable GPS devices, walkie-talkies, tablets. Regarding their operating system, they will be able to run a custom-built application, which will allow them to securely send different types of data through the SDN enabled network, such as text messages, video, audio or any type of file. Furthermore, this application offers a lightweight end-to-end encryption mechanism, allowing sensitive information to pass through the network in a secure way and inaccessible to unauthorized users. Finally, even though the devices are able to connect to the SDN enabled network in a first stage, the SDN controller is responsible for granting access to them or rejecting them. This way, even if we try to embrace a Bring Your Own Device (BYOD) logic, only certified devices will be allowed to access and distribute sensitive information.

3.2 AI enabled SDN routing

In this section, we present the SDN rerouting methodology that is able to estimate and enforce flow rules of the defense SDN network ensuring energy, QoS provisioning and security efficiency. More specifically, we collect real-time metrics from the network in order to calculate a number of routing objectives that

concern energy, QoS and security information per SDN switch and link. By employing multi-objective optimization incorporating evolutionary algorithms, a set of the best solutions (i.e. flow rules) is identified. The set of new flow rules is then applied to the SDN system.

Network Monitoring: Our method collects various SDN traffic statistics and metrics in order to calculate security, QoS and energy consumption related objectives. First, QoS is a representative description of the overall performance of the network. Our approach utilizes the delays between switches and resource utilization statistics (i.e. CPU load and memory usage) to estimate a QoS metric for all the links and switches of the network. Since sensitive switches and links must be protected from attacks, each switch is characterized by a sensitivity level, which is estimated based on the amount of data serves each switch. Similarly, each link has a sensitivity level based on the amount of data being transmitted using this link. Every communication process between IoT devices consumes an amount of electrical energy, which could be translated into a financial cost. Therefore, the traffic in the network should be optimized in order to minimize the total energy consumption, and thus, have a lower operational cost. In our approach, the energy usage within a switch is estimated using the memory and disk metrics for each switch.

Concluding, the SDN topology of an IoT network is modeled as an undirected graph, $G = (N, E)$, where N indicates the set of the nodes (n) that represent the SDN switches and the E is the set of edges (e) that refer to the communication links between two switches. Each node n of the graph has the c_n, m_n and d_n attributes that correspond to the CPU, memory and disk metrics of the switch, while the total packets is represented by the p_n attribute. Finally, each edge e of the graph has the d_e and p_e attributes which are the delay of the communication and the total packets between two switches.

Routing Policies Formulation: A SDN flow rule (p) consists of a number of switches n and links e, while the set of all the alternative paths is devoted by P, where $p \in P$. The five flow routing objectives that must be followed and concern security, QoS and energy consumption information are listed below::

1. **Maximize the switch QoS**: The switch QoS is defined as
$$J_1(p) = \sum_{n \in p} c_n + m_n, \tag{1}$$
where c_n and m_n are the CPU load and memory usage metrics if the switch n belongs to the path p.
2. **Maximize the link QoS**: The link QoS is defined as
$$J_2(p) = \sum_{e \in p} d_e, \tag{2}$$
where d_e is the connection delay of the communication link e that belongs to the path p.

3. **Avoid sensitive switches**: The switch sensitivity is defined as

$$J_3(p) = \sum_{n \in p} p_n, \tag{3}$$

where p_n is the total number of packets served by the switch n that belongs to the path p.

4. **Avoid sensitive links**: The link sensitivity is defined as

$$J_4(p) = \sum_{e \in p} p_e, \tag{4}$$

where p_e is the total number of packets transmitted by using the link e belonging to the path p.

5. **Minimize energy consumption**: The energy objective is defined as

$$J_5(p) = \sum_{n \in p} d_n + m_n, \tag{5}$$

where d_n and m_n is the disk and memory metrics of the switch n that belongs to the path p.

Routing Optimization: The above presented objectives may be contradicting, i.e. optimizing the value of one objective may be negatively affecting the values of other objectives. In such cases, a multi-objective optimization approach is adopted that identifies a set of optimal solution, called Pareto optimal. In our case, the multi-objective optimization problem is formulated as follows:

$$\begin{aligned} &\arg\min_{p} && (J_1(p), J_2(p), J_3(p), J_4(p), J_5(p)) \\ &\text{subject to} && J_i^{min} \leq J_i(p) \leq J_i^{max}, \forall i \in [1,5], p \in P, \end{aligned} \tag{6}$$

where P is the possible set of solutions, $J_i, \forall i \in [1,5]$ are the objective functions (equations (1), (2), (3), (4) and (5), respectively) that must be minimized simultaneously and $J_i^{min} \leq J_i(p) \leq J_i^{max}$ are optional constraints that the objectives might have.

Since the number of all the available paths can be very large, i.e. $O(n!)$, in the complete graph of order n, the estimation of Pareto front by calculating all the available paths is not feasible for realistic SDN networks where the number of forwarders may be up to some hundreds. In order to quickly estimate the Pareto optimal solution set, a multi-objective routing optimization based on evolutionary algorithms is incorporated in our methodology. Evolutionary algorithms belong to Computational Intelligence field and efficiently produce solutions in computationally problems using robust approximation models. Evolutionary algorithms iteratively optimize a set of possible solutions. A set of possible solutions is called population that is evolved by applying a number of genetic operators to produce a new population based on objective functions [3].

In our approach a possible solution is represented by a sequence of nodes of the graph representing the forwarders of the SDN network. Each valid possible solution (i.e. there is a communication link for each pair of the sequence) is characterized by five objectives using the objective equations (1), (2), (3), (4) and (5). The population is evolved using the Multi Objective Evolutionary Algorithms by Decomposition (MOEA/D) [17]. MOEA/D finds optimal solutions for each objective and then evolves the initial population based on these solutions by applying operators. After the iteration is finished, the unique solutions of the final population comprise the Pareto optimal solution set.

Algorithm 1: Pseudo-code for multi-objective routing optimization using the Evolutionary approach

Input :
- a graph G where the nodes (n) and edges (e) indicate the forwarders and communication links of the SDN network
- the source node s and destination node d of a data flow
- the generation size ($gens$)

Output: the set of optimal routing paths (O)

```
Generate random population P = p_1, p_2, ... between s and d ;
for each p_i of P do
    check if p_i is valid;
    calculate the fitness based on the objectives (1), (2), (3), (4) and (5);
    evolve population using genetic operators;
    update population with update solution;
end
while iteration ≤ gens do
    repeat step 1;
end
find the unique solutions of the final population (Pareto optimal solution set Par);
if the weights of each objective are known then
    compute the unique optimal solution (p_opt) by minimizing the equation (7);
    let O = p_opt;
else
    let O = Par;
end
```

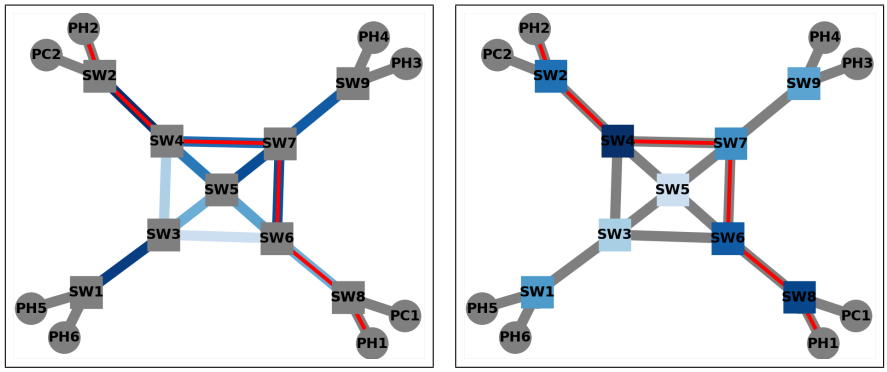
The unique optimal solution can by found by minimizing the following objective function when the importance of each objective is available (e.g. provided by the network operator)

$$\arg\min_{p} \alpha\, J_1(p) + \beta\, J_2(p) + \gamma\, J_3(p) + \delta\, J_4(p) + \epsilon\, J_5(p), \tag{7}$$

where $\alpha+\beta+\gamma+\delta+\epsilon = 1$. The values of $\alpha, \beta, \gamma, \delta, \epsilon$ define the user preference for each objective. The step-by-step outline of the proposed routing optimization is given in Algorithm 1.

4 Evaluation Scenarios

In this section, two evaluation scenarios are presented to illustrate the proposed SDN routing methodology and its effectiveness in tactical environment challenges. More specifically, we assume that there is a request for communication between two defense-related IoT devices, (i.e. between two mobile phones), while the data flow can be routed from a set of switches. In the first one, we assume that some links of the SDN network have significant transmission delays that would correspond to tactical environments with high vegetation and/or ground irregularities where the the data transmission rates are poor. The second scenario examines the case where some SDN switches have a large volume of data for processing, meaning that such network areas may have been overloaded.



(a) The darker blue a communication link between switches appears, the less connection delays are experienced.

(b) The darker blue a node is colored, the less data packets are travelled from this node.

Fig. 2. The estimated flow rule corresponding to optimal link QoS and switch sensitivity

Figure 2 depicts the path $SW8 \rightarrow SW6 \rightarrow SW7 \rightarrow SW4 \rightarrow SW2$, which is both QoS and sensitivity efficient, since it consists of links with low delays, while it avoids switches with a large data packet load, resulting in outdoor critical SDN network with high sustainability and survivability capabilities. In this example, PH, PC and SW nodes denote mobile phones, PCs and switches, respectively.

To demonstrate the two scenarios, we used a synthetic representative graph that represent a SDN network with IoT devices (e.g. mobile phones, PCs) that are inter-connected through SDN switches. For each switch and communication link, we randomly assigned values that correspond to network metrics, namely resource utilization (c_n, m_n, d_n) and traffic (p_n) metrics for each switch, connection delays (d_e) and total packets (p_e) between switches. Using these network metrics, our methodology computes the five objectives (i.e. equations (1), (2), (3), (4) and

(5)), respectively) for all the possible paths (i.e. flow rules) between PH_1 and PH_2 (representing two mobile phones) and, then, the Pareto optimal solution set is calculated by Algorithm (1). The estimated optimal flow rules regarding the QoS and sensitivity efficiency are shown in Figure 2. More specifically, the optimal flow rule is red highlighted (path $SW8 \rightarrow SW6 \rightarrow SW7 \rightarrow SW4 \rightarrow SW2$) in both cases, while the switch nodes and links are colored based on the packet load and link delay metrics, respectively. As already stated, the darker blue a communication link between switches appears, the less connection delays are experienced. On the other hand, the darker blue a node is colored, the less data packets have crossed this node.

Our methodology is able to estimate a QoS efficient routing path (i.e. $SW8 \rightarrow SW6 \rightarrow SW7 \rightarrow SW4 \rightarrow SW2$) consisting of links with low delays and avoiding some links (e.g. $SW3 \leftrightarrow SW4$, $SW3 \leftrightarrow SW6$) with significant transmission delays. In addition, the proposed path avoids switches (e.g., ($SW3$, $SW5$) with a large data packet load resulting in a optimal sensitivity routing path. In conclusion, the proposed SDN routing methodology is able to provide routing paths with high sustainability and survivability capabilities in outdoor critical environments.

5 Conclusions

In this paper we presented a SDN enabled network, which can be easily deployed in outdoor environments for critical operations. Our proposal provides a reliable, secure, portable, private and stable network with very low latency, because it consists of low cost hardware, together with highly effective SDN algorithms that offer QoS strategies, enabling rerouting techniques. In this scope, the proposed AI algorithm was presented and evaluated in our SDN enabled testing environment, promoting QoS techniques, which were used in order to reroute the packets in the SDN network. Finally, we intend to extend the capabilities of our proposed AI algorithm, not only taking advantage of the network and resources metrics, but also taking into account the application requirements of the end device. This will significantly improve the survivability of the communication network. On the other hand, the SDN enabled network will be further researched in order to extend the privacy and encryption features of the sensitive communications over the proposed network. Furthermore, the extensibility of the network will be ensured, by introducing new technologies, such as 5G, which will operate collaboratively with the SDN network and will increase connectivity.

References

1. Azzouni, A., Boutaba, R., Pujolle, G.: Neuroute: Predictive dynamic routing for software-defined networks (2017)
2. Dutra, D.L.C., Bagaa, M., Taleb, T., Samdanis, K.: Ensuring end-to-end qos based on multi-paths routing using sdn technology. In: GLOBECOM 2017 - 2017 IEEE Global Communications Conference. pp. 1–6 (2017)

3. Emmerich, M.T., Deutz, A.H.: A tutorial on multiobjective optimization: fundamentals and evolutionary methods. Natural computing **17**(3), 585–609 (2018)
4. Gilani, S.S.A., Qayyum, A., Rais, R.N.B., Bano, M.: Sdnmesh: An sdn based routing architecture for wireless mesh networks. IEEE Access **8**, 136769–136781 (2020)
5. Gkioulos, V., Gunleifsen, H., Weldehawaryat, G.K.: A systematic literature review on military software defined networks. Future Internet **10**(9) (2018)
6. Haenlein, M., Kaplan, A.: A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. California Management Review **61**, 000812561986492 (07 2019)
7. Hassan, M., Vien, Q.T., Aiash, M.: Software defined networking for wireless sensor networks: A survey. Advances in Wireless Communications and Networks **3**, 10–22 (01 2017)
8. Iurian, C.M., Ivanciu, I.A., Marian, B.M., Zinca, D., Dobrota, V.: An sdn architecture for iot networks using onos controller. In: 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet). pp. 1–6 (2020)
9. Jutadhamakorn, P., Pillavas, T., Visoottiviseth, V., Takano, R., Haga, J., Kobayashi, D.: A scalable and low-cost mqtt broker clustering system. In: 2017 2nd International Conference on Information Technology (INCIT). pp. 1–5 (2017)
10. Khanchuea, K., Siripokarpirom, R.: A multi-protocol iot gateway and wifi/ble sensor nodes for smart home and building automation: Design and implementation. In: 2019 10th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES). pp. 1–6 (2019)
11. Liu, W., Hu, X., Yan, X.: Controller deployments based on qos guarantees in sdn-enabled tactical ad hoc networks. In: 2020 12th International Conference on Communication Software and Networks (ICCSN). pp. 73–78 (2020)
12. Manzoor, A., Hussain, M., Mehrban, S.: Performance analysis and route optimization: Redistribution between eigrp, ospf & bgp routing protocols. Computer Standards & Interfaces **68**, 103391 (2020)
13. Poularakis, K., Qin, Q., Marcus, K.M., Chan, K.S., Leung, K.K., Tassiulas, L.: Hybrid sdn control in mobile ad hoc networks. In: 2019 IEEE International Conference on Smart Computing (SMARTCOMP). pp. 110–114 (2019)
14. Spencer, J., Willink, T.: Sdn in coalition tactical networks. In: MILCOM 2016 - 2016 IEEE Military Communications Conference. pp. 1053–1058 (2016)
15. Streit, K., Schmitt, C., Giannelli, C.: Sdn-based regulated flow routing in manets. In: 2020 IEEE International Conference on Smart Computing (SMARTCOMP). pp. 73–80 (2020)
16. Streit, K., Dreo Rodosek, G.: Cetup: Controller-equipped topology update process for tactical ad-hoc networks. In: Proceedings of the 17th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor & Ubiquitous Networks. p. 57–66. PE-WASUN '20, Association for Computing Machinery, New York, NY, USA (2020)
17. Trivedi, A., Srinivasan, D., Sanyal, K., Ghosh, A.: A survey of multiobjective evolutionary algorithms based on decomposition. IEEE Transactions on Evolutionary Computation **21**(3), 440–462 (2016)
18. Yu, H.C., Quer, G., Rao, R.R.: Wireless sdn mobile ad hoc network: From theory to practice. In: 2017 IEEE International Conference on Communications (ICC). pp. 1–7 (2017)
19. Śliwa, J.: Sdn and nvf in support for making military networks more survivable. In: 2019 International Conference on Military Communications and Information Systems (ICMCIS). pp. 1–6 (2019)