Towards Software-Defined Battlefield Networking

Jéferson Nobre*,¹, Denis Rosário*, Cristiano Both†, Eduardo Cerqueira*§, and Mario Gerla*†

* Federal University of Pará, Belém – Brazil
† University of Vale do Rio dos Sinos, São Leopoldo – Brazil
§ Computer Science Department, University of California Los Angeles, Los Angeles – USA
Email: jcnobre@unisinos.br, {denis, cerqueira}@ufpa.br, cbboth@ufcspa.edu.br, gerla@cs.ucla.edu

Abstract—Battlefield Networks (BN) consider that each network entity is a network in itself composed of several communication technologies usually interconnected by multiple satellites. In this context, we must consider the intrinsic properties of military contexts to apply in network-centric Software Defined Network (SDN) in BN to get more flexibility and programmability. For instance, BN considers several communication technologies, as well as the distinct application requirement on the traffic transmitted over BN in terms of Quality of Service (QoS) and security features in a dynamic environments, where flexible network-centric operations are mandatory. In article, we define an SDBN architecture that adapts SDN technology to BN, enabling SDN-based applications, methods, and policies. To the best of our knowledge, the proposed architecture in this article is the first one aimed at integrating BN and SDN into dynamic and heterogeneous network-centric environments.

Index Terms—BN, SDBN, Heterogeneous network

I. INTRODUCTION

Battlefield Networking (BN) enables the integration and synchronization of military forces capabilities to improve the effectiveness of deployed missions [1]. BN boosts information sharing concerning different types of traffic, ranging from real-time (e.g., situation awareness dissemination) to elastic traffic (e.g., file transfers). Typically, BN applications consider client-server paradigm with bidirectional data transfers among mobile entities (i.e., tank, battleship, and others) and fixed stations (i.e., ground station) [2]. In battlefield scenarios, several communication technologies are employed to support such applications.

BN is a network of networks (usually interconnected by satellite communications [3]), where each end node can be a network in itself. These nodes can be hosted by different units of military forces, such as tanks, ships, and aircrafts [4]. In this way, BN communication is subject to multiple complex and dynamic policies. For example, some network flows might have different Quality of Service (QoS) requirements, as well as traffic isolation needs, due to some nodes belonging to various national military forces [5]. These policies may be supported in BNs ranging from satellite links to long-range radio links.

BN requires flexibility, programmability, and management for integrated network-centric BN operations, where Software-Defined Networking (SDN) paradigm addresses such capabilities [6]. SDN has been successful applied different networking environments besides wired ones, such as satellite networks [7] and wireless networks [8]. More specifically, SDN consists of four pillars: i) separation of the control and data planes, ii) centralized control plane, iii) programmability of the control and data plane, and iv) standardization of application programming interfaces (APIs) [9]. A SDN-based tactical environment can incorporate benefits from networks softwarization since BN is a composition of wired and wireless networks. However, today SDN has been applied in a restricted way to BN.

Despite SDN benefits, some key challenges must be overcome to apply SDN paradigm on BN. First, several wired and wireless networks compose BN infrastructures [10]. In this way, it is essential to incorporate legacy networks that are not softwarized, and the integration of these legacy networks can be a challenging task. Second, the BN heterogeneity requires specializations on the control plane for particular networks, where different network-specific controllers may be orchestrated to apply network-wide policies. However, there is no standardized signaling for the interactions among such controllers. Third, safety features in BN have strict requirements. Hence, few existing works investigated the relationship between SDN paradigm and these features.

In this article, we describe the operational benefits and impacts of considering the SDN paradigm on BN (SDBN). The SDBN advantage provides flexibility in the BN setup, and also to apply policies on network-centric operations. Also, it enables different SDN features, such as topology and flow optimization, as well as monitoring and adaptation mechanisms. The main contribution of this article is to define an SDBN architecture that adapts SDN technology to BN, enabling SDBN-based applications, methods, and policies. This architecture supports police management, controllers orchestration, and integration of legacy networks. To the best of our knowledge, the proposed architecture is the first one aimed at integrating BN and SDN.

The remainder of this article is organized as follows. In Section II, we present a concise background on SDN. In Section III, the proposed architecture for SDBN is depicted. In Section IV, SDBN use cases are discussed. Finally, the concluding remarks are presented in Section V.
II. SDN in a Nutshell

SDN emerged as a networking paradigm for wired networks and it has been extended for environments such as satellite networks [7], wireless networks [8], among others. SDN architecture consists of four planes (Application, Control, Forwarding, and Management planes) and 3 APIs (Northbound, Southbound, and Management interfaces) [11]. Also, SDN separates the control and the data forwarding planes, allowing quicker provisioning and configuration of network connections [7]. Moreover, its network-centric paradigm defines a centralized entity (called SDN controller) that coordinates the forwarding decisions of network elements. Finally, SDN considers standardized APIs for the communication between the planes.

One of the main characteristics of SDN is the clear separation of the control and the data planes, where network elements become simple forwarding devices and the control logic is implemented in a controller. In fact, SDN decouples the system that makes decisions about where traffic is sent (i.e., control plane) from the underlying system that forwards traffic (i.e., data plane) [8]. This separation simplifies policy enforcement and network configuration, evolution, scalability, as well as the control and data planes can be developed separately from each other.

The SDN controller coordinates the forwarding decisions of network elements. For instance, it enables to adapt network policies on-the-fly much better and faster than traditional routers [6]. In this way, SDN has the benefits of a centralized approach for network configuration, where network administrator do not need to configure all network elements individually to (re)configure the network, allowing easy management functions [12].

SDN enables the programmability of the control plane. It refers to the ability of control, change, and manage network policies on-the-fly employing software via open interfaces in contrast to relying on closed boxes and proprietary defined interfaces. It also represents the ability to treat the network elements as a single programmable entity instead of a set of devices that have to be configured individually [6].

It is fundamental to consider open interfaces to reach its full potential regarding flexibility and adaptability required in the tactical environment on BN [6]. In this context, SDN architecture has well-defined three APIs: Northbound, Southbound, and Management interfaces. The southbound API allows the forwarding plane to communicate with the control plane; the northbound API abstracts control plane functions to network applications at the top level; the management API allows information to flow between the management plane and other planes [11]. Hence, we argue that a BN architecture comprising heterogeneous wired and wireless legacy networks must be SDN-based enabling the benefits from softwarization to be applied in the complex tactical environment.

III. Proposed SDBN

The employment of SDN in BN must consider the intrinsic properties of military contexts. For instance, BN regards several communication technologies, such as, satellite, line of sight and long range radio, and others wireless technologies, applied in different battlefield scenarios (e.g., tactical edge networks). Besides that, there are distinct application requirements on the traffic transmitted over BN in terms of QoS and security features. In this section, we introduce the proposed SDBN elements, architecture, policies, and security issues that considers both BN features.

A. SDBN Elements and Architecture

The proposed SDBN architecture follows the key ideas of the SDN paradigm. For instance, the SDBN architecture also considers 4 planes: forwarding, control, application, and management. However, BNs are composed of several wired and wireless communication technologies applied in different battlefield scenarios, and these BNs are usually interconnected by satellites. Hence, multiple SDBN controllers must be (co)located with network entities, such as, satellite stations. As illustrated in Figure 1, several controllers may be in charge of the SDBN control plane (left side of Figure 1). Each cloud in this figure can be depicted in more detail, showing the specific controller and the forwarding elements (switches). Such controllers may employ different southbound protocols, e.g., OpenFlow and Interface to the Routing System (I2RS). These protocols can involve either in-band or out-of-band communication.

The SDBN application plane supports applications to perform different tasks. However, these applications have different requirements in terms of QoS and security levels, which might be considered. For instance, BN traffic with strict requirements in terms of delay (e.g., defined via Differentiated Services Code Point (DSCP) values) or security (e.g., in terms of cryptographic key sizes) may be separated from non-interactive application traffic (e.g., file transfer and email) via policies.

The SDBN control plane is responsible to address traffic decisions and specific needs concerning the BN data communication elements. In this context, the availability and performability of end-to-end paths is intrinsic to successful applications operation. With SDN, efficient path deployment can be deployed using individual links from (possible) heterogeneous networks. Despite being logically centralized, the SDBN control plane can be executed by multiple controllers. Such controllers, in turn, can be embedded in different kinds of network entities.

The relationship among SDBN controllers can be addressed in different ways. We consider multiple SDBN controllers with 2 distribution approaches since the granted SDBN architecture has to consider which network technologies are to be supported via specific capabilities. We highlight 2 distribution approaches for the SDBN controllers: Hierarchic SDNB and Federated SDBN, such as illustrated side-by-side in Figure 2. Besides that, all hardware and software elements have to take into account the different military security levels.

A multi-level hierarchy SDBN controller helps the consistency of the SDBN as a whole. In this context, a 2-level hierarchy approach that considers global and local controllers connected via an event service achieves reachability, while avoiding excessive complexity. This is because each local
(low-level) controller abstracts the specificities of its communication technologies from the SDBN (high-level) controller. Besides that, a hierarchy SDBN controller improves the data consistency maintenance, due to consolidation functions from the SDBN controller.

In an SDBN federation approach, controllers interact directly with each other using the event service to support the SDBN operation. The use of a federation approach promotes the autonomy of individual controllers. This avoids dependability issues (i.e., there is no Single Point of Failure - SPoF), and also enables the organic growth of the SDBN control plane (i.e., the capacity of the control plane is increased with the addition of new controllers). In Table I, we summarize the Pros and Cons of the adopted controller distribution approaches, as well as include the centralized approach as a baseline.

In the present architecture, we introduce an event service to connect the signaling channels of the SDBN controllers. Based on the distribution approaches for the SDBN controllers, the event service use is twofold: it enables the communication of a global controller with local controllers in a hierarchical approach; or it supports the message exchange among federated controllers in a federation approach. In either way, the event service promotes an integrated SDBN operation.

The SDBN forwarding plane is composed of (re)configurable entities connected to a controller. The forwarding plane can be responsible for information maintenance, network information, and others. These entities can be hosted by Low Earth Orbit (LEO) and GEOstationary orbit (GEO) satellites, terrestrial and aerial vehicles, watercrafts, ground stations, and other heterogeneous communication elements (e.g., WiFi and E-UTRA base stations). The service area (i.e., radius ranges) of these entities depends on the network technology, where some entities provide more extended service area.

The SDBN management plane enables to perform the SDBN administrations and operations. It also allows informa-
### TABLE I
**Distribution Approaches for the SDBN Control Plane**

<table>
<thead>
<tr>
<th>Distribution Approach</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| Centralized           | • Greatest simplicity  
                        | • Current controllers can be supported without modifications | • Lack of flexibility  
                        | • SPoF for all operations  
                        | • Poor abstraction of communication technologies |
| Hierarchical          | • Adequate simplicity  
                        | • Data Consistency | • Possible SPoF for some operations  
                        | • Need to define the hierarchical relationships |
| Federated             | • Dependability  
                        | • Organic growth  
                        | • Controller autonomy | • Complex interactions  
                        | • Significantly rewrite of current controllers |

BN communication is subject to multiple complex and dynamic policies. In this context, policies are defined as high-level forms of guidance, information, and command to meet specific application or user requirements. For instance, tactical information in BN may be separated from non-tactical information traffic via network policies, due to QoS and security requirements. In this way, the network administrator can manage the SDBN as a whole via policies, including the BN infrastructure, and also the network services that are running over such infrastructure. Besides that, policies can be used to address different features of heterogeneous networks in a BN towards specific goals.

The detailed policies content should be defined for specific applications, where the SDBN controller should be able to unscramble and implement such policies consistently and act accordingly. In this context, detailed (re)configurations for every node are not needed, since the SDN enables the programmability of the control plane on-the-fly. Policy-based methods help SDBN elements to configure the different communication technologies that compose the BN scenario, as well as the nodes themselves.

Policy enforcement in SDBN depends on accurate network knowledge. Such information is composed of information about network elements such as links, traffic, routing table, as well as their updated state. Despite the fact that the accuracy of network knowledge is a generic network problem, this is particularly important regarding heterogeneous networks (e.g., including satellite, wireless and wired communications), such as those which build SDBN. Since the SDBN control plane is logically centralized, it helps an efficient policy enforcement in respect to the collection of network information. In this context, when considering multiple SDBN controllers, it is also necessary a mechanism to maintain the consistency of network state among such controllers.

The SDBN Controller is in charge of optimizing the BN performance through the use of policies. In this context, graceful near real-time BN adaptation by forwarding nodes in the heterogeneous BN scenario is required by the SDBN Controller. This (re)configuration helps medium allocation and flow table prioritization. Policies provide the necessary flexibility and programmability for integrated BN operation.

### C. Security

The application of SDN features in a BN must be followed by the employment of security mechanisms to meet military requirements. Some of such mechanisms are added natively regarding the available southbound APIs. For example, the OpenFlow protocol can use Transport Layer Security (TLS), which must be mandatory when this protocol is used as a SDBN southbound API. Besides that, additional mechanisms must be employed to increase the security level of the SDBN.

The definition of security mechanisms is performed through the specification of security policies. In this context, authorization policies, such as those related to bandwidth consumption and response time, are used to define what services or resources a given subject can access. In SDBN, these subjects can have diverse roles and belong to different national armed forces. Besides that, policies can be also used to define the actions to be taken when security violations occur. These actions include either passive measures, such as security violation logging, or active ones, such as disabling entries in flow tables.

Heterogeneous networks forming a BN, and thus there are also heterogeneity in the security mechanisms. In this context, applications can be implied in the support of SDBN security...
features. Such application may be used to transform input or output parameters need in security mechanisms. Besides that, proxies can be implemented to adapt current applications to use the SDBN infrastructure and leverage native security mechanisms. This can avoid changes in legacy networks.

IV. USE CASES

The proposed SDBN architecture supports several types of wired and wireless networks controlled by the proposed SDBN controller distribution. The forwarding nodes are clustered around specific controllers, which in turn can be steered by a higher-level controller. In this section, we introduce two SDBN use case scenarios that can be deployed in the tactical environment as Figure 3 illustrates. In each use case, we first describe the operation scenarios, and then we depicted how our proposed SDBN architecture improves these BN use cases. These features include SDBN applications, virtual overlays created across the BN, the policy behaviour, and security mechanisms.

A. Use Case #1: Bi-directional Video Streaming

Let us consider an heterogeneous BN able to operate seamlessly in order to compose the coverage area. In the first use case scenario, we describe a bi-directional video streaming task (e.g., real-time video conference or battlefield mission video transmission) among several BN end-nodes. For instance, this task is useful for tactical edge network in disaster recovery situations, where in military operations tanks might need to send real-time videos from a given operation to others military forces (i.e., others BNs). In this scenario, a user cannot tolerate receiving videos with large delays and poor video quality level based on the user perspective. Despite different supported policies levels (due to specific communication technologies and user mobility), it is expected near real-time adaptation by distributed network elements, according to the availability of communication channels.

In this way, considering the network-centric hierarchical SDBN controller approach, the streaming request is routed from forwarding elements to the SDBN controller via southbound API connections that are multiplexed on the event service. A flow optimization application (in the Management Plane) helps this controller to select the proper communication medium technology to disseminate the video streaming with low delay and high video quality level. The flow tables in the other local controllers are set up to filter the predefined packet headers corresponding to such streaming.

Policies are used for information filtering and access control regarding video streaming. For example, military subjects (e.g., users or roles) can have different rights to available video channels which compose the streaming. Besides that, location information can be employed as a condition to only permit video streaming access to a certain location, such as a soldier in a specific battlefield coverage area.

B. Use Case #2: Execution of Coordinated Tasks

In this second BN operation scenario, we consider an execution of a coordinated task by a BN unit. For example, the command for a given military task may be originated in a different network regarding the node which will execution such task, i.e., a given ship wants to send a “fire” command to a tank. At least, local SDBN controllers from both networks need to communicate to establish the flow considering service level requirements. Potentially, the operational information is transmitted via heterogeneous networks, as well as their mechanisms to prioritize flows.

In this context, considering the federated SDBN controller approach, the SDBN architecture uses the event service to connect different controllers that participate in a BN. Periodically, the SDBN may optimize the BN for specific service levels using a topology optimization application. Such application must provide support for the execution in a federation, e.g., easing the introduction of new controllers. Besides that, a police application is used to define which flows may have a delay minimization, despite the use of more costly communication technology.

The execution of coordinated tasks requires security properties, such as integrity and non-repudiation. Integrity is provided by the SDBN architecture through channel security and a data hash application provided in the management plane. Non-repudiation is provided with digital certificates to trust the subject which issues the execution. In this context, the subject uses its private key to sign such certificate, thus building a proof of the origin.

V. TRENDS AND FINAL REMARKS

SDN features can provide significant benefits over traditional BN. Depending on the military tasks and the heterogeneity of networks which compose the BN, several SDBN applications can perform networking control tasks, such as the definition of resource allocation and flow priorities. The SDBN controller can be viewed as a military SDN exchange which integrates different SDN controllers, considering specific communication technologies.

Several legacy (i.e., non-SDN) networks are expected to be part of SDBN. In fact, it is difficult to completely replace all current communication technologies with SDN-enabled ones. Thus, it is necessary to decide to implement a proxy that performs the required conversions from the SDBN controller to the networking equipment of legacy networks (and vice-versa). This proxy needs to translate SDBN southbound API to network management protocols (e.g., NETCONF) or, eventually, to Command-Line Interfaces (CLIs).

We envision that several organizations, besides the military ones, may be interested in the feature supported by SDBN. An example of these organizations is police forces. As we expect to see an increase in the equipment which are SDN-enabled, other improvements that have been proposed in general SDN can be also studied in SDBN. An example of such improvements is the use of Network Function Virtualization (NFV).

As future work, we intend to enhance the SDBN architecture and the operational scenarios in which the architecture could be deployed. For example, the utilization of high-level policies to operate the SDBN as a whole could be addressed by intent-based management (i.e., Autonomic Management) or
service abstractions for policies (i.e., Simplified Use of Policy Abstractions - SUPA). Furthermore, we are also looking at additional settings that could lead to important effects, such as network partitions.

REFERENCES


