Comparing Software Defined Architectures for Coalition Operations

Vinod Mishra
U.S. Army Research Labs
APG, MD 21005, USA
vinod.k.mishra.civ@mail.mil

Dinesh Verma
IBM Watson Research
Yorktown Hts,NY,USA
dverma@us.ibm.com

Chris Williams
UK Dstl, Porton Down,
Wiltshire SP4 0JQ, UK
cwilliams@dstl.gov.uk

Kelvin Marcus
U.S. Army Research Labs
Adelphi, MD 20783, USA
kelvin.m.marcus.civ@mail.mil

***Abstract*—Software Defined Networking (SDN) and analogous approaches to different domains like storage, compute and security have emerged as promising paradigms for controlling and managing many different types of distributed systems. In this paper, we examine the application of software defined concepts to coalition operations. Specifically, we propose the concept of Software Defined Coalitions (SDC), a mechanism by which IT infrastructure required by dynamic Communities of Interest (CoI) among coalitions can be enabled rapidly. We examine many different coalition interoperability architectures as SDC candidates, and evaluate their key performance metrics.**

Keywords—SDN; Coalition Networks; Coalition Operations, Software Defined Architectures

I. INTRODUCTION

Software Defined Networking (SDN) [1] is a new and promising approach for creating flexible networks, whose functions can be programmed, defined, and controlled by means of software. The concept of SDN can also be extended to create aggregate systems whose software, communication, and computational resources can be modified and controlled by extensible software. This paradigm has been shown to be useful in many different contexts. As a result, it is natural to explore whether it can also be used in the context of coalition operations, and adapted to improve their agility and effectiveness.

This is the problem which we study in this paper. As a first step, we draw upon the principles of SDN to define a construct called Software Defined Coalition (SDC). An SDC provides the mechanism to support the IT needs for a dynamic community of interest that is used to conduct a coalition operation. We consider different alternative approaches that can be used to enable SDCs, and evaluate their performance by means of computer simulations.

Our results indicate that a traditional model for sharing assets in coalition operations by using compatible model provides operational simplicity, but has a relatively low chance of successfully establishing a community. A brokered approach has a higher chance of establishing the community, but requires a higher level of trust. A federated approach has more complexity, but eliminates the challenges associated with trust among coalition partners, and has the same chance of community establishment as the brokered approach.

In the next section of the paper, we provide an overview of SDN paradigm, with a brief discussion of how the paradigm can be extended to many other domains. The following section introduces the concept of dynamic communities of interests, and how they can be formed in the ad-hoc environment, which is followed by a section introducing the concept of SDCs. Then, we discuss the approaches that can be used to achieve SDCs, focusing on the fact that resources for SDCs need to be drawn from several coalition partners. We discuss the performance metrics that need to be used to compare alternative architectures for SDCs, and present simulation results on the performance characteristics of different alternative approaches.

II. SOFTWARE DEFINED NETWORKING (SDN)

At its essence, the communication networking deals with the task of moving bundles of data between different computing devices, using intermediary nodes as needed. A large number of protocols and mechanisms have been developed to deal with the different characteristics of networks in many different environments. However, the design of any networking infrastructure can be divided into three fundamental areas (or planes) as shown in Fig. 1. These three planes are the data plane, the control plane and the management plane. Each plane describes a set of functions to be executed in each of the devices that make up the traditional communication network.

(i) The Data Plane (DP) functions are required for the actual transport of bits between different devices. Some examples are encapsulating upper layer protocol packets into lower layer protocols packets (e.g. encapsulating TCP segments into IP packets), encrypting packets, computing checksums, or forwarding packets on appropriate links.

(ii) The Control Plane (CP) functions are required to control the DP functions, e.g. maintenance of tables for forwarding packets. The CP information can be abstracted into either configuration parameters or DP policies, where the former is the specification of some value needed by the DP functions (e.g. size of packet buffers) and the latter is a set of conditions and actions to be taken when they are satisfied.

(iii) The Management Plane (MP) functions needed to configure the DP or CP, monitor and report on the overall networking, and any trouble-shooting or fault-diagnosis that may need to be done for the other two planes. In other contexts, MP is replaced by an Applications Plane (AP). For this paper MP will be considered more important.

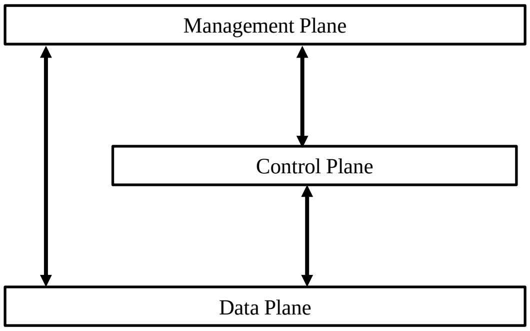

Fig. 1. Different Planes in a Computer Network

Each of the planes may be implemented in a distributed or centralized manner. In the former, each node in the network performs the same function in the network, while in the latter, each node in the network has an agent, which essentially contacts a central server to perform all the functions. The server has all the algorithms and intelligence required to perform the required functions in the plane.

The DP is usually implemented in a completely distributed manner, while the MP is usually centralized. For the CP, one can use either a distributed or a centralized implementation. The driving principle of SDN is to have a complete separation of DP and CP, which itself is centralized. This leads to a programmable and flexible network in which it becomes easier to add new functions through new software modules in the CP.

The separation of various functions into data, control and management plane is a paradigm that can be copied into distributed systems beyond the field of computer networking. The DP in those cases would contain the actual function being performed, and so function plane may be a better description. However, in order to stick with the convention, we will continue to call it DP even when we are applying the same paradigm to different domains of networking.

III. Dynamic Communities of Interest (CoI)

Although coalition forces tend to separate themselves geographically in order to simplify their operations, they often need to conduct joint missions. Some examples are, a joint patrol, a joint surveillance operation providing disaster relief, or airlifting an injured colleague. These joint operations need coalition members to pool their people and resources together in some manner. The extent of pooling and sharing is limited by the national policies of each member of the coalition.

For illustration, let us consider a scenario in which a dynamic Community of Interest (CoI) [2] needs to be formed between the U.S. and UK coalition forces whose objective is to distribute blankets in a local village since they expect an unusually harsh winter. Based on the size of the village, a platoon is sufficient for the task which will last four hours, but each country allocates people to the mission at the level of a platoon, so a platoon is assigned from each country for this mission. The two platoon contingent from both countries collects the blankets, meet at a different point, travel to the village together and distribute the blankets. They may choose to conduct the entire operation as consisting of two disjoint activities with very loose coordination, e..g the U.S. platoon can distribute blankets on the east side of the village while the UK platoon can distribute blankets on the west side of the village. However, one of the platoons may run out of blankets sooner than the other. Both platoons can conduct their missions more effectively and faster if they tried to pool together their resources in a more coordinated manner.

One such approach would be to treat the group of soldiers as an integrated unit. All the soldiers from both countries are put together under the command of a single non-commissioned officer from one of the two nations, who coordinates their operations as a single integrated unit. The officer is in control only for the duration of the operation, and the community ceases to exist once the operation is over. The officer can decide to conduct the distribution of blankets in any manner deemed suitable. Such coordination has several operational benefits, e.g.

(i) Only one platoon consisting of soldiers drawn from each country can be sent saving resources,

(ii) Better cohesion develops among the participants, and

(iii) Any prior experience of a member from one nation to deal with the sensitivities of the villagers can be shared dynamically with members from both countries.

Such a group formation is a dynamic community of interest (CoI).

Several types of coordination and support operations need to happen in order to achieve the objective of a dynamic CoI. A command and control infrastructure for the CoI needs to be determined, mutually acceptable operational practices need to be agreed upon, logistics for provisions (e.g. blankets) have to be managed in a coordinated manner, etc. One of the critical support functions needed for dynamic CoI is the enablement of their Information Technology (IT) requirements. The members of the dynamic CoI need to be equipped with personal communication devices to communicate and coordinate with one another during the mission, even if they come from different countries. Different types of joint operations would require different types of IT assets, but the required capabilities must be enabled rapidly.

IV. Software Defined Coalition (SDC)

The SDC is the mechanism required to enable the IT infrastructure needed for the operation of a dynamic CoI. Depending on the specific CoI objectives, they may need different types of IT equipment and services available at different locations. For example. a CoI may need devices carried on a soldier's person, equipment carried in a vehicle, IT services available at the base-camp, or IT services that are provided via satellite communications from backend centers located in the U.S. or UK. At each of these locations, equipment may come from any of the coalition partners. IT equipment includes Intelligence, Surveillance, and Reconnaissance (ISR) assets such as sensors, surveillance cameras and UAVs, which generate information and need to be connected together. Dynamic CoI may also require resources from other coalition partners outside U.S. and UK depending on the availability and accessibility of the needed resources.

From the view of the members of the dynamic CoI, the most expedient approach would be to come to a single individual within their country, who will provide them with the right personal equipment, or configure them to enable their participation in the dynamic CoI. That single individual would also decide all the IT needs for the CoI, and would provision all the resources, including setting up the right permissions for the members of the CoI to work with each other. Logically, the process for enabling the IT infrastructure for the CoI would look like the steps shown in Figure 2.

The equipment and services that each country is willing to provide for the dynamic CoI are put into a common pool. The IT individual selects the set of equipment and services that can interoperate at some level to support the CoI. The IT individual then configures the equipment and services to enable CoI members to communicate with each other to meet their objective.

When the CoI is dissolved after the completion of the objectives, the services and equipment will once again be reconfigured so their previous states, when individuals do not have access to other coalition partner's information or services.

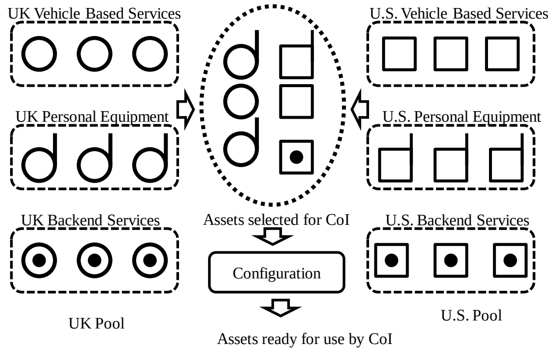

Fig. 2. Selection and Configuration of CoI Assets. Assets are chosen from a pool of both countries, and then configured for the CoI.

Depending on standardization, technology maturity, trust and cooperation among different members of the coalition, assets may be interoperable at different levels of granularity. We can identify the following three levels of interoperability among different partners.

- *Network Level*: To enable the CoI, only network level reconfiguration is needed. Reconfiguration includes setting up the right configuration parameters, the right security protections against unwarranted intrusions, and appropriate access control and authorizations.
- *Network and Storage Level*: The needs of the CoI require configuring some storage needs in addition to the network enablement. The storage needs include access to the right database, file system or appropriate storage mechanism needed for the mission of the CoI.
- *Network, Storage and Compute Level*: The needs of the CoI require access to some significant computation capability, in addition to the networking and storage. The computational needs include access to any applications or services needed for the mission of the CoI.

The network and storage level mechanism combines ideas from SDN [1] and Software Defined Storage (SDS) [4], while the network, storage and compute levels build upon the concept of Software Defined Environments (SDE) [3].

As to the different types of interoperability, let us revisit the example of the humanitarian distribution of blankets. The U.S. and UK troops may only need to be able to communicate with each other during the mission. If the communication can be enabled using an ad-hoc peer to peer infrastructure, the only reconfiguration needed is the ability for the U.S. and UK devices to talk to each other. If such communication requires access to a backend service, e.g. a messaging service running at the U.S. base-camp, the devices just need authorization to access that messaging service for the life-time of the CoI.

On the other hand, if another objective of the CoI is to collect images and video of the countryside and the villagers, and these pictures and video footage require significant storage, appropriate storage must be provisioned at the base-camp or another appropriate location for such storage. The storage equipment may come from any of the coalition partners.

Similarly, if the CoI wants to further have analytics run on the images and video collected, or run analytics on any other ISR input that was collected, it needs access to applications that are able to perform such analytics. This requires that the CoI IT infrastructure include enablement of the right servers and applications that can run the logic associated with their needs.

The SDC is the IT infrastructure enabling the CoI to work in a seamless manner. It consists of the mechanisms which allow the appropriate IT needs of the CoI to be satisfied. SDC is focused on the control plane of the CoI IT infrastructure, and enables the transfer of the configuration and control of the data plane components that will be used by the CoI. An SDC can be viewed as an instantiation of the general concept of SDE [3], which has been customized and adapted to support dynamic CoI in tactical environment.

The DP of a SDC consists of the different applications that may be running on the hand-held personal devices or different services that may be running at the base, on-vehicle equipment, or other locations including those in the fixed infrastructure. This will include logistics applications like those that may keep track of blankets, a video analytics application, and network forwarding functions or the task of encrypting packets, among other similar tasks. The nature of the DP functionality will depend on the specific goal of the CoI.

The CP consists of an agent, one per device, and a single controller. In accordance with SDN principles, there is a single controller and many control agents. The control agent configures and provides policies for the various data plane functions. The controller will disseminate the right information needed by the agents.

Additionally, the MP consists of the management system which is usually centralized. Like the control agent, the MP may also contain a management agent per device. In most cases, we would expect the management agent to be an instance of an implementation of industry management standards, e.g. it may be an SNMP agent. The MP implements its own set of protocols for agent-manager communication.

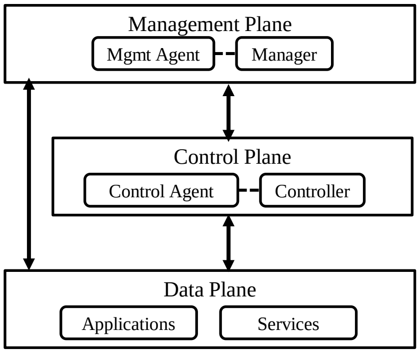

Fig. 3. SDC Control, Data & Mgmt Plane functions

The number of controllers in the CP depends on the size and complexity of the network. At the minimum, each coalition partner would have at least one controller, and some coalition partners with larger networks may have multiple controllers, e.g. one controller for each segment of the network. Even assuming that each partner has just one controller, we have a variety of options for arranging a controller for the dynamic CoI where the assets may come from any coalition partner.

V. Alternative SDC Architectures

In a coalition environment, the CP for supporting SDC implies that we have to have a controller asset which can work with the control agents that are present on any of the devices in the CoI, regardless of the national origin of the device. Each partner in a coalition is likely to have a controller that it operates and controls. In this section, we look at the various options that can be used to coordinate different controllers belonging to different partners.

Approach 1: Single SDNC for Coalition

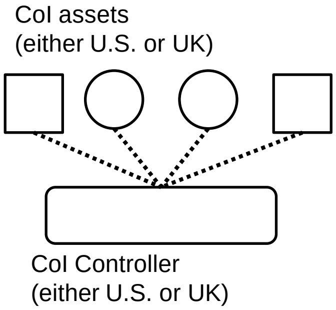

Fig. 4. Simplifying Coalition CoI to a single Organization CoI

Figure 4 shows one possible approach. When the U.S. and UK need to form a dynamic CoI with their assets, they designate one of their controllers as the one to be used for the CoI. The different assets belonging to the coalition partners get configured and enabled by the CoI controller as if they were part of the tactical environment for the coalition partner who owns the selected controller.

The advantage of this approach is that the operational logic and mechanics of the CoI is no different than that of a single organization environment. The disadvantage of the approach is that it requires all CoI devices to interoperate with the selected controller. If the devices from all countries use the same protocol, it is a non-issue. However, if the devices from different countries do not have the same protocol for communicating with their controllers, the only viable solution is to use assets from only one country. Thus, the main decision in forming a CoI becomes which country/organization should be the one providing the assets. As a result, this approach does not enable efficient sharing of resources.

Approach 2: Broker Layer over coalition SDNCs

An alternative approach uses multi-domain multi-broker (MDMB) architecture in which the controllers of each country retain their autonomy and communicate via a Broker Layer [5]. In such an architecture, an additional broker acts as the mechanism for enabling the decision making across controllers from different countries, as shown in Figure 5 In addition to the standard SDN controllers, a broker is introduced which acts as another layer providing the top level hierarchy for coordinating SDN brokers. The layout of the broker and its relation to the SDNC of different coalition partners is illustrated in Figure 5.

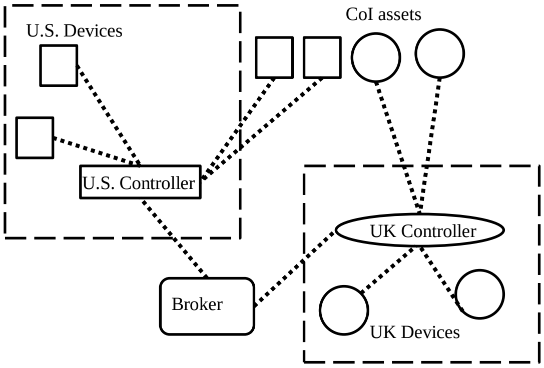

Fig. 5. Broker Architecture for Coalition SDN Controllers

The advantage of this architecture is that each asset talks to the controller of their own organization, eliminating the challenges associated with interoperability. The broker provides the ability for the SDNC of each organization to work with each other, in effect becoming a super controller. The main challenge with this approach is the issue associated with the operation of the broker. The coalition member operating the broker has a significant advantage in controlling the CoI compared to other partners. The issue of deciding which partner ought to run the broker can easily become very contentious.

Approach 3: Distributed SDNC Architecture for Coalitions

Another approach, which is inspired by federation of ISR assets [6] and SDN based policy enforcement [7], creates a distributed environment in which the broker is eliminated, while the equivalent functionality is provided by the collection of each country's SDNC. This approach, illustrated in Figure 6, avoids the tricky issue of control over the broker. The distributed approach requires a East-West Interface connecting different controllers, and is operationally more secure since no additional elements are introduced which can act as a point of vulnerability.

These three solutions present alternative approaches for handling the issue of federation across different coalition controllers. The choice of the right solution depends on the level of trust among different partners, and the degree of standardization between the nodes and controller. When the controller and the devices use the same interface, reducing the problem to a single organization system for the CoI would work. In other cases, the choice depends on the level of trust among coalition partners. When one partner is trusted to operate a broker, the broker based approach will be most appropriate. When partners only trust each other partially, the distributed East-West approach is more suitable.

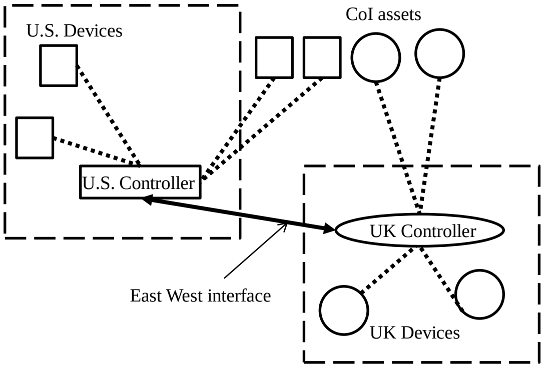

Fig. 6. Federated Architecture for Coalition SDN Controllers

VI. Performance Evaluation

The performance of different SDN interoperability mechanisms can be gauged by two complementary measures:

(i) How likely is a dynamic CoI able to get its desired resources using one architecture versus another?

For this metric, the probability of a successful CoI formation, the federated architecture, and the broker based architecture have similar characteristics.

(ii) What is the overhead of control operations that need to happen in each architecture?

During the operational phase, all three approaches are likely to have very different overhead for each CP exchange.

To evaluate the first measure, we ran a Monte-Carlo simulation of a coalition environment with the following assumptions.

(i) The dynamic CoI consists of people and assets from 2 to 5 coalition partners. In the current context of coalition operations, a dynamic CoI with more than 5 partners appears to be very unlikely.

(ii) Each partner brings different amount of assets to offer to the CoI for use in the dynamic CoI.

(iii) Each partner contributes at least one asset to the CoI

(iv) For the simplified model shown in Figure 5, the partner requesting the establishment of CoI would provide a controller for the same.

We refer to the coalition partner that is bringing the most assets to the table as called the Primary Partner. The other partners are characterized by a number called ***skew***, a number between 0 and 1, equal to the ratio of the resources provided by the partner to that of the primary coalition partner. Thus, if the primary coalition partner provided 100 assets to the pool, then a partner with a skew of 0.8 would only provide 80 assets. For the simulation with 2 partners, the skew was computed as defined. For simulation with 3 or more coalition partners, each partner's skew was determined randomly with a mean value around the skew.

Another measure impacting the performance of different architectures is the probability of compatibility between different coalition partners. If an asset from a partner has to be used with a controller from another partner, it is not always guaranteed that the assets will interoperate, or whether the asset can be reconfigured to support the controller belonging to another partner. This challenge is circumvented in the federated architecture and the broker approach. The compatibility probability would have a significant impact on the relative performance of the two approaches. In practice, the probability of compatibility is likely to range from very low for some partners to very high for others.

The simulations we ran compared the results of allocations of assets to form new dynamic CoIs using either the simplifying approach shown in Fig 5, or the broker/federated approach shown in Fig 6 and 7. For the allocation itself, there was no difference between the federated and broker approach. The system simulated the handling of 10,000 dynamic CoI creations, each of them lasting for a duration which was, on the average, 10 times longer than the interval between two consecutive CoI creations. The duration for each CoI was generated as a random value drawn from a uniform distribution between 0 and twice the average value. For each simulation run, a number of assets and a corresponding compatibility matrix was generated for each coalition partner. The compatibility matrix was a Boolean value indicating whether a given asset belonging to one partner would interoperate with the controller belonging to another partner, and was generated randomly at the beginning of the simulation using the compatibility probability value. We assumed that each CoI required an asset from each of the coalition partners. For CoIs that need more assets, the situation will be akin to reducing the resources available to each of the partner.

Each run of the simulation measured the fraction of generated CoIs that could be successfully established. A CoI would only be successfully established if it could find adequate number of assets from all of the coalition partners. In the simplified model, this could be done as long as enough assets were available that were compatible with the controller provided by the partner establishing the CoI. In the federated and brokered model, this could be done as long as enough assets are available across all partners, and compatibility was not an issue since an asset and a controller belonging to the same partner should be compatible with each other.

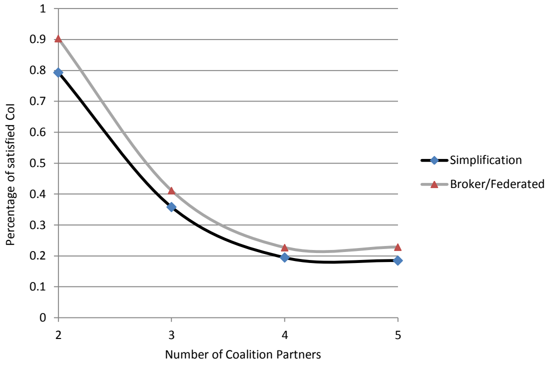

Fig. 7. Percentage of satisfied CoI when primary partner has 20 assets in the pool, with a 50% compatibility probability and 50% skew.

Figure 7 shows the percentage of satisfied CoI which can be realized when the primary partner has 20 assets in the pool, assets have a 50% chance of compatibility, and the resource skew is 50%. Since the size of CoI increases as the number of partners increase, the percentage decreases as more coalition partners become part of the CoI, explaining the declining shape of the curve. As shown in the figure, federation among controllers can increase the percentage of satisfied CoIs significantly, with almost 10% increase in the number of CoIs that can be satisfied. This increase happens because the compatibility constraint between assets of one country and a controller from another country is no longer present in the federated or brokered approach.

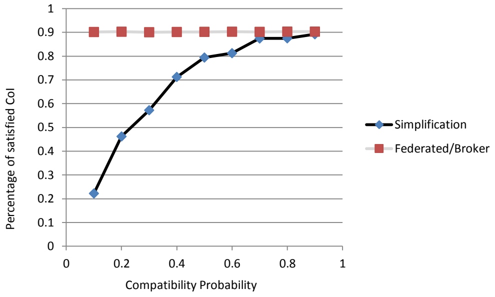

Fig. 8. Percentage of satisfied CoI requests with 2 partners

Figure 8 shows the percentage of satisfied CoI requests as the probability of asset compatibility varies among partners. 2 coalition partners are considered. As expected, the federated or broker based approach, which relies on its own controller, has a very high probability of forming a CoI, while the simplification approach can not satisfy the requests when it runs out of compatible assets. In the Simplification approach, an asset from UK can only be used in a CoI with a controller provided by U.S. if the UK asset is compatible with the U.S. controller. In the federated or brokered approach, each asset talks to their own country's controllers, and thus any available asset can be used in the CoI. This increases the probability of establishment of the CoI, albeit at the cost of increased communication overhead during the operational phase.

On the operational side, the different architectures need to be compared on the basis of the exchanges each control interaction needs. In this case, the control operation exchange would depend heavily on factors such as the mobility characteristics of the assets involved in the CoI and their ability to reach their controller. These depend on factors such as the routing algorithm used, reliability of the links, and other factors independent of the controller architecture. To compare the controller architecture, we need to compare the latency involved in obtaining any of the control operations that may be requested from the controller in these operations.

In order to model the complexity of control plane coordination, we compute the latency involved in the successful exchange of a control plane operation in different CoIs using one of the three different control plane coordination architectures. The successful exchange depends on three factors, how long it takes for an asset to communicate with the controller, how long it takes for controllers to communicate with each other or to the broker, and the number of message that is required to be exchanged in each of the architectures.

A Simplified Mathematical Model

In the simplified model of CoI formation, the asset always talks to the compatible controller, which we can assume is always the closest one, since in principle, the dedicated controller can be in a vehicle close to the CoI assets as they perform their mission. We define

α = latency of the simplified model in Approach 1

f = scaling factor for additional latency in reaching the controller in Approaches 2 and 3.

αf = latency of an asset in reaching the controller in Approaches 2 and 3.

g = scaling factor for the latency between two partner controllers, or between a controller and the broker.

αg = latency on the links between two partner controllers, or between a controller and the broker

n = The number of coalition partners

With the help of these definitions, we can estimate the latency in a control exchange that happens in the federated and brokered model or Approaches 2 and 3 for different number of partners.

It is clear that the latency in a control message for the simplified architecture is α, the latency in control messages for brokered architecture is $(f+g)\alpha$, while the latency for the federated architecture is $(f+ng)\alpha$. The federated architecture is the most complex of all three approaches because an n-way communication and negotiation is needed for each request.. However, this complexity provides the value that it can allow interoperability, when the level of trust between partners is not high enough to enable the creation of a broker.

VII. Conclusions

In this paper, we have examined the problem of creating software defined coalitions or SDCs, which enable sharing of assets between different coalition partners. We introduced the task of SDCs, looking at the simplest form of the concept where assets are shared by enabling them to work with a common controller. We have proposed three different mechanisms for interoperability of the SDN controllers, and compared their ability to establish a dynamic CoI as well as their complexity of control operation.

In future work, we want to explore SDCs which share assets at increasing granularity, allowing a better sharing of the network, storage and application level services available in each of the partners. We also want to gain better insights into the operational aspects of SDC by examining their performance in an emulated test-bed.

VIII. ACKNOWELDGEMENTS

This research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence under Agreement Number W911NF-16-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copy-right notation hereon.

References

[1] Nunes, Bruno Astuto A., et al. "A survey of software-defined networking: Past, present, and future of programmable networks." IEEE Communications Surveys & Tutorials 16.3 (2014): 1617-1634.

[2] E. Asmare et. al., “Secure Dynamic Community Establishment in Coalitions," IEEE Military Communications Conference, IEEE MILCOM 2007, Orlando FL, Oct 2007.

[3] Li, C-S., et al. "Software defined environments: An introduction." IBM Journal of Research and Development 58.2/3 (2014): 1-1.

[4] Carlson, Mark, et al. "Software defined storage." Storage Networking Industry Assoc. working draft, Apr (2014). Available from URL http://datastorageasean.com/sites/default/files/snia_software_defined_storage_white_paper_v1.pdf.

[5] A. Castro et al., "Brokered Orchestration for End-to-End Service Provisioning Across Heterogeneous Multi-Operator (Multi-AS) Optical Networks", Journal of Lightwave Technology, VOL. 34, NO. 23, DECEMBER 01, 2016.

[6] Calo, Seraphin, et al. "Technologies for federation and interoperation of coalition networks." Information Fusion, 2009. FUSION'09. 12th International Conference on. IEEE, 2009.

[7] Sørensen, Erik. "SDN used for policy enforcement in a federated military network.", Ph.D. Thesis, Norwegian University of Science & Technology, June 2014, Available at URL http://brage.bibsys.no/xmlui/bitstream/handle/11250/263070/753752_FULLTEXT01.pdf