Leveraging SDN for Cyber Situational Awareness in Coalition Tactical Networks

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

Dinesh Verma
IBM T J Watson Research Center, Yorktown Heights, NY 10598, USA
dverma@us.ibm.com

Christopher Williams
Defence Science and Technology Laboratories, Porton Down, Salisbury, Wiltshire SP4 0JQ, UK

CWILLIAMS@mail.dstl.gov.uk

ABSTRACT

Coalition tactical networks are composed of different networks of two or more nations coming together for securing a mission in the tactical arena. Cyber security is an important consideration in coalition operations, and is a complex challenge due to the need for operational effectiveness, as well as for limited trust relationships that exist among coalition partners. New emerging paradigms in networking, such as Software Defined Networks (SDN), provide a mechanism to deal more effectively with their security challenges. In this paper, we discuss how to utilize the principles of SDN to improve the cyber situational awareness in coalition environments as well in various military networks. We propose the concept of SDN oriented OODA (Observe, Orient, Decide and Act) loop for improving the cyber security awareness, and then demonstrate how this paradigm can be used in coalition networks.

1.0 INTRODUCTION

Coalition operations refer to an environment in which networks and systems belonging to different countries or organizations are brought together to perform a task, often at short notice and potentially for short time periods. Differences in the pedigree of disparate systems necessitate the development of approaches that can work with partial visibility, partial trust, and cultural differences, while simultaneously dealing with the challenges of a dynamically changing situation on the ground.

While there are many different definitions of situational awareness, it can be simply defined as knowing what is happening around us. In the context of security of computing systems, we can use a working definition that situationally aware computing system has the relevant knowledge to make a reasonably accurate assessment of the friendly and inimical operations in a combat theatre. Such a situationally aware computing system maintains awareness of the security threats in the environment, and provides an input about the current state of the security to enable the best possible decision making for mission success.

In the context of coalition operations, situational awareness is extremely important for effective security management. At the same time, it is extremely difficult due to the fact that coalition operations bring together resources and people from different organizations and countries. Each of them has its own set of networking and computing assets, its own security procedures, and its own culture resulting in a many different approaches towards threat assessment and reaction to perceived threats.

In this paper, we assert that a combination of two paradigms of SDN [1] and OODA [2], can be used to create an architecture for effective situational security awareness in coalition operations. SDN is an emerging paradigm in communication networks that promotes the principle that control ought to be separated from data. OODA loop is an established paradigm used in military decision making. By treating the cyber security situational awareness as a software implementation of the OODA loop, and using a SDN like architecture to control it, we can create an architecture that is automated and addresses the various challenges of coalition operations. This architecture brings together paradigms from many different fields, namely (i) SDN from Communications Networks, (ii) OODA from military strategy, and (iii) cyber-security concerns from the field of network security, and applies them to the coalition systems.

Since the readers are not likely to be familiar with all of these paradigms, the Section 2 provides a brief background of coalition systems, SDN and OODA loop. Section 3 describes the application and benefits of SDN to coalition networks, and is followed by Section 4 discussing the use of OODA loop for implementation of cyber-security functions in a single organization in a non-coalition context. The two approaches are then combined into a SDN-oriented cyber security operations for coalition networks in Section 5. Finally, we show how this architecture can be used to improve situational awareness for a potential security threat in the environment as an example.

2.0 BACKGROUND

The architecture combines existing ideas from SDN and OODA loop in the context of cyber security situational awareness. In this section, we briefly review the background of coalition environments, SDN and OODA loop. This section provides a highly simplified view of all three of the above areas, with the intent of establishing common taxonomy and approach for use in the future sections of the paper, as opposed to covering all the nuances of these areas.

2.1 Coalition Environments

A coalition environment refers to a setting in which assets from two or more participating countries are brought together for a common strategic purpose [3]. It may have different formats depending on the working arrangement between the participating nations. Nevertheless, we can assume a simplified model of a coalition environment, in which each individual country's environment consists of the four segments as shown in Figure 1.

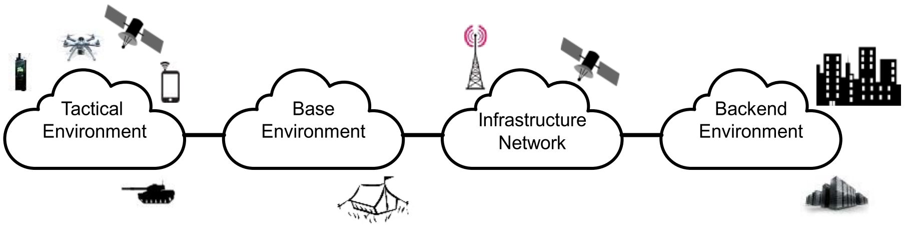

Figure 1: Simplified model of a single country military network.

The tactical environment is the first segment consisting of the devices and the network used by war-fighters in the theatre of operation. This will contain many different handhelds, UAVs, ISR devices, mobile networking and computing environments to be carried onto various platforms such as tanks, ships or vehicles. These devices may establish an ad-hoc network among themselves, or use satellite communications to interconnect themselves.

Tactical environments are connected to the 2nd segment of base environments found in bases and buildings used for military operations. They may use portable laptops, desktop computers, storage devices, and networking equipment that are usually create a temporary network infrastructure. It may also reflect the computing environment in a military base that has been setup for a temporary period, ranging from a few days to a few months.

Such base environments usually connect via the 3rd segment of the infrastructure network. It may involve satellite communications or may leverage installed civilian infrastructure such as cellular communications networks. Depending on base's life-time, it may also leverage fixed network infrastructure, such as a wired cable of fibre network to connect to the 4th segment of the backend environment. It may consist of the computing infrastructure found in buildings and military headquarters. In general, computing and communication resources in these environments are plentiful, and tend to be static in nature.

Coalition operations require military networks from two or more nations to work together. The current state of the art is to have such collaboration mostly in the backend or base environments. Using SDN and the new architecture we propose, we can enable collaboration among coalition partners in the tactical environments as well. In general, coalition operations would setup their environments independently, and have some level of network connectivity among them. They may have one or more tactical environments within each nation's network. In a typical coalition operation, a community of interest (CoI) is dynamically formed to conduct joint coalition operations. The CoI can be an ad-hoc team consisting of several coalition partners executing many concurrent missions including border/perimeter reconnaissance and surveillance, camp site surveillance, and detection/classification of human activities in concealed/confined spaces or locations of human infrastructures.

A CoI brings together a set of assets, specific missions, and sets of policies that govern information security and sharing of information. The CoI environment would be built by combining assets from the tactical environments of multiple coalition partners, i.e. the dynamic CoI would take some assets from all of its partners in order to conduct its mission. One such sharing arrangement is shown in Figure 2 where a dynamic CoI is formed between a U.S. and UK coalition, e.g. when a joint patrol is formed to conduct surveillance in a specific area. In other cases, the CoI may also share assets from the base and other environments, including access to the backend.

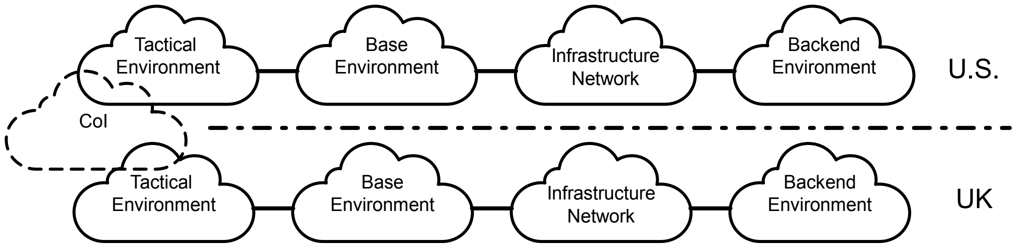

Figure 2: Simplified model of a coalition network between U.S. and UK

When such a dynamic CoI is formed, assets from different partners may be shared. Each of the two nations may have policies limiting how the assets are shared, as well as how information from an asset may be shared with coalition partners.

2.2 SDN

The function of a computer communication network is to accept the data packets or protocol data units, from one computer and deliver it to another computer. The network consists of several elements working together to provide the connectivity required for such delivery. Each of these elements performs some operations on receiving the packet, e.g. deciding which of several possible outbound interfaces to choose for forwarding the packet, or whether to drop the packet due to a security reason. The operations are usually referred to as Data Plane (DP) functions which necessitate defining the information needs at each of the network elements, e.g. calculation of data forwarding tables, setting up of virtual connections, or defining the filtering rules. The types of operations that establishes how to build such tables or other required information, are called Control Plane (CP) operations. In a traditional network, they are carried out using a distributed algorithm, e.g. in an Ethernet, a forwarding table which follows the links of a spanning tree among all participating switches is established as part of the CP using a distributed protocol implemented within them.

Software-defined Networking (SDN) is a new approach that replaces CP operations of individual devices with a CP run from a centralized SDN Controller or SDNC [4]. The SDNC implements the CP operations as software running on standard IT servers. This moves the CP functions from each device in the network to a logically centralized controller, and enables more flexibility. The high-speed DP that is responsible for actually forwarding packets remains in the network devices. As an example, in an Ethernet, the logically centralized controller can be configured to implement algorithms that compute not just a spanning tree, but a more complex graph for forwarding packets which use links not on the spanning tree. One need not implement a distributed protocol, which is more complex, and may require standardization among different devices manufacturers to work properly. In addition another key component of SDN is a set of programming interfaces that allow applications and control programs to automate network operations through well-defined, open APIs enabling much more agile interaction with the network than traditional methods, such as scripted CLIs and proprietary interfaces.

Figure 3 shows the picture of the network before and after SDN enablement. A network of three nodes is a function implemented without SDN. With SDN, a common API is put on the nodes, and the network device operation is controlled through the APIs by means of software on the controller node. The controller provides more flexibility in the network operation. SDN use cases have been developed in a variety of network types, including wired and wireless carrier networks, data centre networks, and enterprise or campus networks. Some common examples are SDN-based interfaces to automate network service provisioning across the WAN, dynamic fine-grained access control in wireless networks, and creation of virtual networks in multi-tenant cloud data centres.

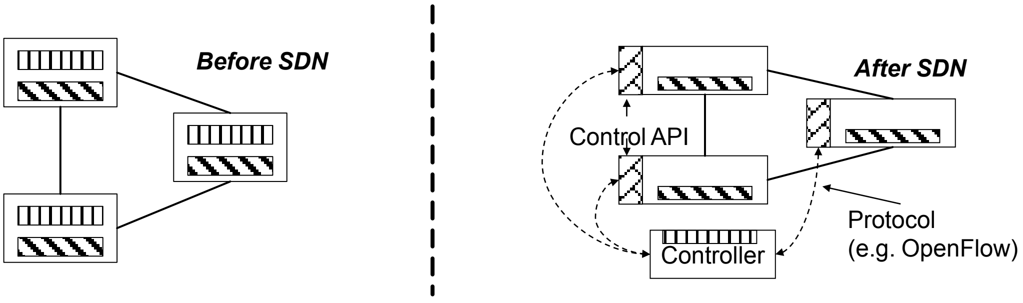

Figure 3: A network before and after SDN. The boxes with vertical stripes implement control plane function, while the boxes with slanted stripes implement data plane functions. SDN moves control plane functions to a central controller.

The concept of separating control from data results in a significant simplification of the network infrastructure, and is one of the reasons for the popularity of SDN.

2.3 OODA

The OODA loop is one of the established approaches for describing how humans make decision [5]. It explains that activity as consisting of the four stages of Observe, Orient, Decide and Act.

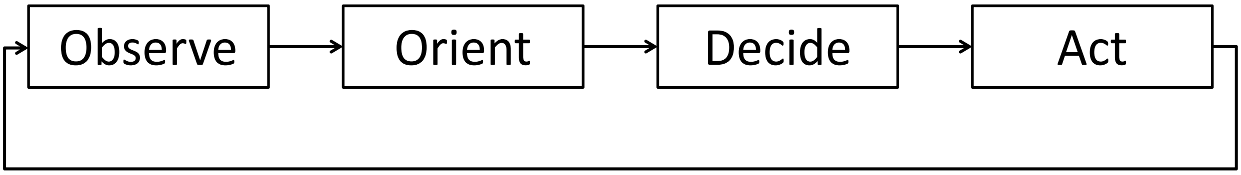

Figure 4: The OODA loop for Decision Making.

The four phases are the following: (i) Observe Phase: All relevant information available from the environment is collected, (ii) Orient Phase: The observed is analysed further to get a deeper understanding of its implications, e.g. one may try to determine a root cause from the various observations, (iii) Decide Phase: The trade-offs involved in different courses of action are considered, and the right course of action is determined, and finally (iv) Act Phase: The action is actually undertaken, which results in a change to the environment, again leading to an observation of the environment. This completes the loop.

As an example, suppose one hears the sound of a gunshot. During the observation phase, the sound of the gunshot is heard. In the orient phase, additional determination, e.g. the location of the gunshot is determined, or other information sources, e.g. a camera video input is used to get more information. In the decide phase, the possible options to deal with the gunshot is determined, and the resulting action is then taken. Although developed for the human behaviour, the OODA loop can also be applied to tasks performed by a computer, and in particular to the task of security in military networks. The application of SDN to cyber security situational awareness deals with using the OODA loop for cyber-security to get human like situational awareness implemented within a computer software.

3.0 SDN FOR CYBERSECURITY IN SINGLE COUNTRY ENVIRONMENT

Let us examine how the concept of SDN would be applicable to cyber-security and situational awareness. In order to apply SDN principles, we need to differentiate between the control part and the data part of the cyber-security situational awareness, as well as define what the implementation of the OODA loop means in this context. The architecture that we envision for cyber-security situational awareness implements the OODA loop in software in the one or more elements of environment which is described in Figure 1. That software is responsible for performing the tasks required in the OODA loop as follows:

(i) The (O) observe part of the OODA loop consist of capturing portions of the network traffic that an element is seeing. Such data observations can be achieved by activating a variety of data collection elements. A data collection element may be collecting a subset of network packets, or looking at performance metrics within a computing system, or keeping track of the number of processes that are active within a computing device.

(ii) The O (orient) part of the OODA loop needs to determine if anything abnormal is taking place in the network environment. The orient part of the system tries to map the observed data into higher level phenomenon [6], implementing algorithms for root cause analysis to determine why specific observations might be happening.

(iii) The D (decide) part of the OODA loop needs to process the collected information and assess the ongoing threat situation. On the basis of this assessment a course of action (COA), which may comprise multiple parts, is then chosen as the response. Several approaches for making decisions, e.g. using policies or rules, utility maximization and game theory can be used at this stage.

(iv) The A (act) part of the OODA loop then implements the COA activities. For cyber-security purposes, the action may consist of installing new network access control rules, information filtering policies, reconfiguration of security parameters, or switching to a different mode of encryption for secure communication.

In each of the above implementations, the CP and the DP functions of the OODA loop can be defined: (i) In the Observe phase, the DP function is the actual collection of the data. Determining which type of information to collect, and how to balance off the power and energy needs of an element against that of the normal computation would be the CP functions. (ii) In the Orient phase, the DP function invokes the algorithms that map observations into phenomenon, while the CP function is the definition of the parameters in the algorithms that can enable such a mapping. (iii) In the Decide Phase the policy rules are implemented in the CP which leads to decision. (iv) In the Act Phase the DP functions actuate the desired action of the data flow or sensors.

As an example, if a set of rules are being used to map observations into phenomenon, the rules are determined by the CP, while the rules are enforced by the DP. Similarly, the utility functions, policies or defining the parameters of the game are CP functions, while the actual decision making is a DP function. The actual invocation of the action is a DP function.

In the SDN architecture for cyber-security, we can define a cyber-security software agent on various devices that implement the DP functions. These use a simple protocol to get their configuration, rules and policies from a controller, which is responsible for providing them with the right information needed for the DP operation. The structure is as shown in Figure 5 below.

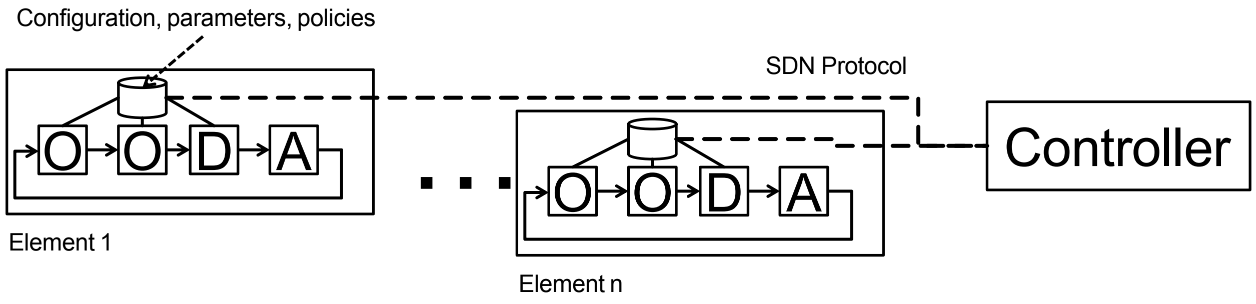

Figure 5: OODA loop based Cyber Security Architecture using SDN .

The SDN protocol ensures that the controller determined rules and configuration are provided to the different elements. In tactical environments, where bandwidth is limited, disruption tolerant approaches would be needed to keep the configuration, parameters and policies of different elements in synchronization with the values determined by the controller.

4.0 SDN BASED SITUATION AWARENESS FOR COALITION

ENVIRONMENTS

When we extend the SDN based situational awareness architecture to a coalition environment from a single network environment, the architecture needs to be augmented to provide for the presence of multiple SDNCs. Each country network is likely to have their own SDNC which need to be federated together to create a completely functional system for the overall network. In order to do that, we need to augment the SDNC with not just a North-South interface between the elements and the SDNC in individual country networks, but with a East-West interface that is used to exchange information between the individual controllers. In this respect, the architecture we propose is similar in principles to relation coalition operations for ISR assets [7] and general networking [8].

The architecture of a system with controllers from both the U.S. and UK is shown in Figure 6. In the figure, the oval and circular boxes represent assets belonging to the U.S., while the square and rectangular boxes represent assets belonging to the UK. The controllers in each of the individual networks are responsible for providing the policies, configurations and parameters that drive the operation of each of their elements. The OODA loop implemented within the U.S. elements and the UK elements could be quite different, with the use of different approaches in each of the individual country elements.

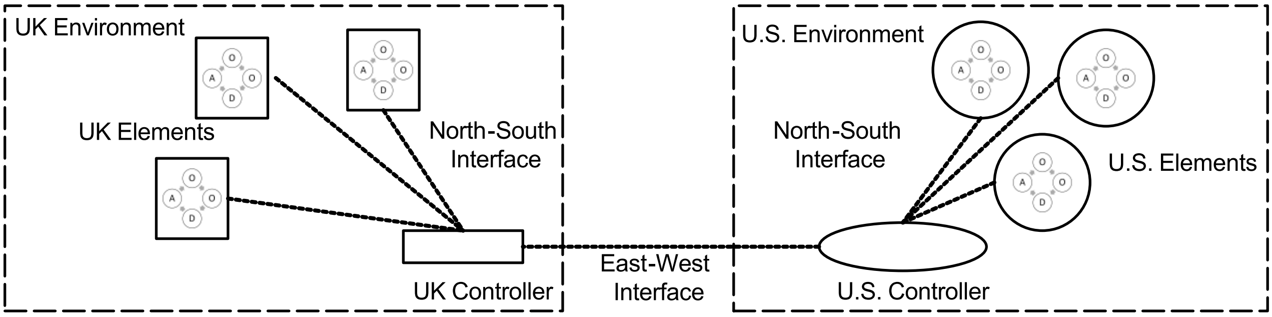

Figure 6: ODDA loop based Cyber Security Architecture using SDN for Coalition Networks .

The SDN protocol shown in Figure 5 translates to the North-South interface in both the U.S. and UK. While the U.S. and UK are not obligated to use the same protocol, a common protocol such as one based on a REST interface to harmonize policies and parameters of different elements is likely to be used in each nation. Nevertheless, the choice of specific names of variables and parameters, as well as policy format and specifications, are likely to be different in each nation. The East-West interface provides a mechanism for the controllers to work and interoperate with each other. This interface can be used to share policies, or negotiate dynamic policies when Communities of Interest are formed dynamically.

This architecture can be used to coordinate the security threat assessment and share information among different coalition partners. As a very simple example, let us consider the case where a rogue terrorist is trying to launch an attack on the UAVs that are operated by coalition partners in a theatre of operation. Let us also assume that the terrorist has been able to determine the frequency at which commands are issued to the UAV, and is trying to launch a scanning attack to determine if any communication port in the UAV is vulnerable. The U.S. may have detected the terrorist probes and the U.S. controller has installed a rule for orientation that maps more than 3 probes on illegal ports from an device to mark that device as unauthorized entity to be added to a black list. The UK detection module, however, may have ended up with a policy that locates the spatial region of the terrorist, and in those regions disable all external communication and operate using a disconnected operation mode.

When a dynamic CoI is formed in which the U.S. and UK both contribute UAVs for the operations, the controllers for both nations can share the policies they have formed with one another. This enables the UAVs for the CoI, which may have come from either country, to install the security policies which enable the joint insights from both nations to be used. The U.S. UAVs can get insights about the vulnerability region in the theatre, while the UK UAVs get additional rules to learn the address of the device, and block them dynamically even when exposed outside that region.

5.0 SUMMARY AND FUTURE WORK

In this paper, we have proposed an architecture that leverages SDN and OODA loop to propose a new architecture for cyber-security situational awareness in the context of a coalition operation. We have also shown how the architecture can help in improving situational awareness and security using a simple example.

While the architecture appears promising, this paper is just an initial exercise in an attempt to use SDN and OODA to improve coalition network security. A significant amount of research exploration is needed for SDN expansion in coalition contexts, as well as implementation of OODA principles in security situational awareness. The areas for further exploration include, but are not limited to (i) identifying the correct abstractions which can be exposed to the partner respecting all the policies of coalition members; (ii) creating the right interfaces for OODA based control of individual elements; (iii) developing the right routing, security information sharing and asset sharing arrangements for coalition operations; and (iv) optimizing the policy constructs for coalition missions.

7.0 ACKNOWLEDGEMENTS

This research was partially 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.

7.0 REFERENCES

[1] Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." IEEE Communications Magazine 51.2 (2013): 114-119.

[2] Brehmer, Berndt. "The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control." Proceedings of the 10th international command and control research technology symposium. 2005.

[3] Verma, Dinesh, ed. Network Science for Military Coalition Operations: Information Exchange and Interaction. IGI Global, 2010.

[4] 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.

[5] Grant, Tim, and Bas Kooter. "Comparing OODA & other models as operational view C2 architecture." Proceedings of the 10th International Command and Control Research Technology Symposium. 2005.

[6] Ye, Fan, et al. "MECA: Mobile Edge Capture and Analysis middleware for social sensing applications." Proceedings of the 21st International Conference on World Wide Web. ACM, 2012.

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

[8] Sørensen, Erik. "SDN used for policy enforcement in a federated military network." (2014).