Management and Orchestration of Autonomous Cyber Things

Bela Erdelyi, Metin B. Ahiskali
U.S. Army, Combat Capabilities Development Command (CCDC)
Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center
Aberdeen Proving Ground, Maryland, USA
usarmy.apg.ccdc-c5isr.mbx.i2wd-co2-public-contact@mail.mil

Abstract

This paper explores the concept of Management and Orchestration (M&O) for autonomous agent things. The battlefield of tomorrow will consist of a multitude of things communicating, acting, and collaborating with each other. Battle things may be defensively or offensively purposed consisting of heterogeneous controllers, sensors, and actuators requiring coordinated integration. Such things may act under human control, and at times under full or partial autonomy establishing the need for robust, persistent, reliable, and secure M&O.

Towards that end, a proposed framework is herein presented based on a notional M&O infrastructure concept.

Introduction

The motivation is to formulate a conceptual but concrete case for the management, control, and integration of autonomous agents. This paper derives from various previous works including one of the earliest workshops at the University of Maryland sponsored by the US Army Research Office, in March 2015 and its resulting publication [1]. Further, this paper builds on a 2017 study [2] collaboratively conducted, on the subject of autonomous battle systems, by the U.S. Army C5ISR Center and the U.S. Army Research Lab (US ARL)[1].

On the battlefield of the future, intelligent things will communicate, act, and collaborate with one another. The phrase Internet of Battle Things (IoBT) introduced in [3] appropriately encapsulates such notion. Our definition of "IoBT" is however extended as per [2] to consist of commercial Internet of Things (IoT), Cyber battle purposed things, adversary things, and interacting human things. This definition involves things on any network, whether operating on private or public networks, on the Cloud, or within any type of military or civilian enclave. One or more interconnected nodes may be considered a set of IoBT assets within this context.

Millions of interconnected IoBT devices with diverse functionality, complexity, and purpose are expected to manifest in the battlefield [3] of the future. Some will be more capable than others. Devices may be assisted by Machine Learning (ML), or by advanced Artificial Intelligence (AI) algorithms to engage or defend against Cyber enemies [4]. Human operators, being also battle things, may be assisted by or collaborate with IoBT devices; alternatively, humans may act to control the IoBT environment.

A concept and architecture for Autonomous Intelligent Cyber [defense] Agent (AICA) and a rationale of the AICA concept is described in [5], which is based on the NATO IST-152 Research and Technology Group[2] (RTG) work on the AICA Reference Architecture (AICARA). A more in-depth analysis is presented in [6]. NATO IST-152-RTG address requirements, architecture and composition of defense-purposed autonomous agents. An overarching agent management strategy to coordinate multi-agent activities is however not addressed by the report.

The complexity introduced by autonomous and distributed interacting things, myriads of agent cognitive capabilities, adversarial deceptive

[1] Both organizations are under the U.S. Army Combat Capabilities Development Command (CCDC)

[2] An activity initiated by the NATO Science and Technology Organization (STO).

actions, and heterogeneous communications protocols will be unsurmountable and difficult to control. Various abstractions will be needed to translate notifications, alerts, and commands in real-time. A properly architected system for IoBT control, their orchestration, mission management, infrastructure configuration, and the necessary superimposed security is essential.

To the best of our knowledge there are no studies, with the exception of [2] which have addressed autonomous things management. In [2] the concept for Autonomous Battle Things (ABT) management is explored within the offensive battle context. The herein objective is to extend that management infrastructure concept for Autonomous Cyber Things (ACT); i.e. a management infrastructure inclusive of defensive and offensive autonomous operations.

Defense or Offense

The IST-152-RTG report [6] provides a comprehensive coverage of autonomous agent properties involving their need for mobility, considerations for lethality, mission criticality, connectivity, power constraints, and their interaction with the environment. Towards such the report formulates an AICA Reference Architecture (AICARA).

A graphical representation of the proposed AICARA is reproduced here, as Figure 1 from [5].

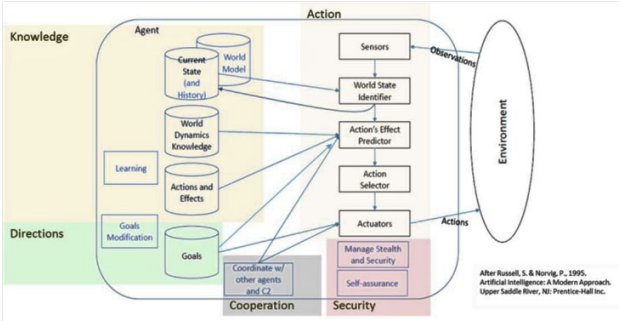

Figure 1. Preliminary AICA functional architecture.

Reference [5] further defines AICA's five high-level functions as sensing and identification; planning and action selection; collaboration and negotiation; action execution; and learning and knowledge improvement. Figure 2 reproduced from [5] provides a graphical representation of these five functions.

Figure 2. AICA high-level functions.

NATO's IST-152-RTG specifically set-out to define a "defense-purposed" agent architecture. It is however these author's contention that the traditional distinction between defense and offense in the context of military autonomous agents is blurred and not so easily distinguishable. To make the case lets explore two simple scenarios.

First, a defensive mission may consist of an intrusion-detection sensor (ID-S) agent in coordination with perhaps a Reinforcement Learning (RL) trained actuator (RL-A) agent. The ID-S agent detects a DoS attack against deployed resources and communicates relevant information to the RL-A agent. RL-A has various options (based on its learning process and policy base) to select from in order to affect an appropriate defense against the intruder. For instance, it may select to implement firewall rules to block the DoS, or alternatively it may solicit an attack (via other agent resources) against the intrusion source. The first option hence may be classified as a defensive action,

with the latter alternative considered to be an offensive action.

Similarly, an offensive mission may consist of an Intelligence and Reconnaissance sensor (IR-S) agent in coordination with a RL-A agent. Additionally, an ID-S agent may be deployed to provide mission protection. Upon identifying the intended target, the IR-S agent communicates the relevant information to the RL-A agent causing it to execute possible attacks. The ID-S agent subsequently discovers a counter attack against the RL-A agent induced activity and elicits defensive resources to eliminate the threat. The ID-S agent's defensive activity may result in a counter-counter attack against the threat, or it may cause the relocating of the offensive activity to a different actuator, or perhaps it may culminate on pausing the offensive action. This cascading of events could be initially classified as offensive which is followed by defensive actions, which in turn may culminate in further offensive actions.

The described scenarios, as well as any other possibly conceivable scenario, represent a potential for both defensive and offensive activities. Single agent actions could be either one regardless of mission type. All scenario deployed agents would exhibit the same five high-level functions illustrated by Figure 2.

While agent specific functional details may greatly differ from each other, their general architecture could conform to the construct of Figure 1. Intuitively, sensor type agents would tend to be agnostic to either defensive or offensive mission intent. Actuator agent types may exhibit passive defensive actions, or alternatively various degrees of aggressive actions. At times, an actuator such as an RL-based agent may optionally select from a set of passive and aggressive actions making an a priori defensive or offensive designation inappropriate.

Hence, mission profiles may be designated as either defensive or offensive. The composition however may consist of a selection from various agent profile types capable of either defensive or offensive actions. The herein proposed ACT infrastructure for autonomous agent Management and Orchestration (M&O) hence is intended to be inclusive of either defensive or offensive missions.

An ACT M&O Infrastructure

The 2017 preliminary study conducted by I2WD and ARL [2] conceived the ABT infrastructure M&O construct. The proposed concept heavily borrowed from the ETSI[3] Network Function Virtualization (NFV) Management and Orchestration (MANO) reference architecture, published in 2014. Since then, NFV MANO specifications have matured into a series of volumes addressing the various aspects of the architecture. Nonetheless, the original NFV MANO reference model still stands, as well as the adaptation in [2] which formulated the original ABT infrastructure framework reference model.

Reference [2] describes a management and orchestration framework for the provisioning of ABT under an offensive scenario. Figure 3 represents the same architectural concept being relabeled here as ACT instead, to accommodate not just battle things but all Cyber things, whether defensive or offensive.

[3] European Telecommunications Standards Institute.

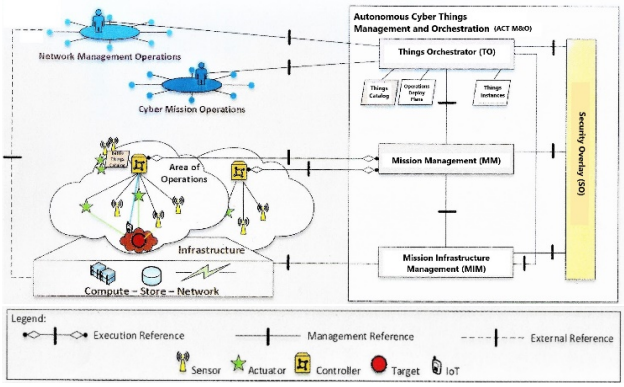

Figure 3. Cyber operations assisted by ACT M&O.

The left side of Figure 3, illustrated below as Figure 4 for clarity, shows an operational deployment of a notional Cyber operations center with corresponding deployment of controllers, sensors, and actuators in an Area of Responsibility (AOR).

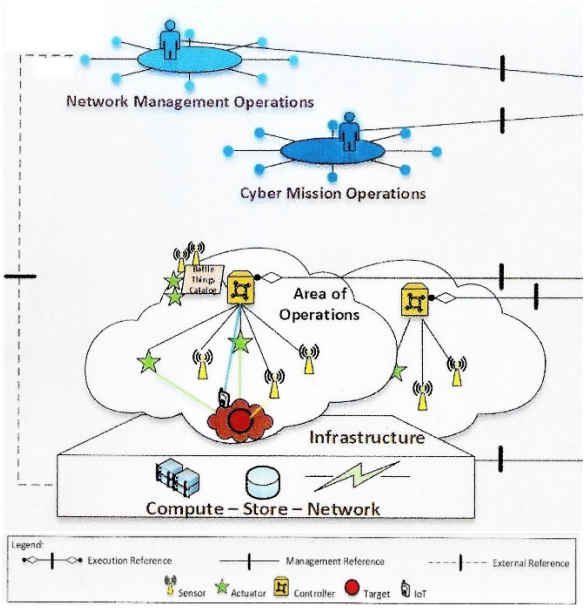

Figure 4. Notional Cyber operations.

The top of the figure may be interpreted as an Offensive Cyber Operations (OCO) Center manned by network management and Cyber mission operations personnel. It could also be interpreted as an enterprise Network Operations Center (NOC) manned by network administrators. Network management responsibilities associated to personnel in these operational centers consist of network planning, preparation of environment, and the allocation and deployment of resources. In an enterprise NOC the expectation is that of a greater control over the environment and for the full ownership of resources, contrary to similar expectations with OCO environments where control over the environment and resources could be elusive.

Regardless of operational environment types, the network management function is to be equally assisted by the Things Orchestrator (TO) component of M&O (Figure 3) for the allocation of resources as needed for agent deployment. It is however recognized that some resource allocations may not be entirely feasible thru M&O automation. The dashed external reference line on the left side of Figure 3 and Figure 4 illustrates such interaction to occur outside of an ACT M&O framework; i.e. depicted external reference point connection.

On the other hand, the conduct of Cyber mission operations is expected to be fully supported by TO interacting with Mission Management (MM), and the Mission Infrastructure Management (MIM) components of M&O. The Cyber operational role performs the deployment, activation, monitoring, and management of controller, sensor, and actuator agents on previously allocated resources.

Controllers are ACT devices in the infrastructure intended to provide the technology glue between M&O and operational sensors and actuators. Controller attributes and roles consist of the following:

a. Deployed as virtual or physical devices.
b. Maintain control over an enclave of agents providing connectivity and the communications pipeline.
c. Implement a lexicon to translate and abstract the various heterogeneous agent protocols.

d. Receive commands from and send responses to M&O.
e. Perform recon to identify existing IoT devices and other deployed agent resources which conform to an operational plan.
f. As needed, initiate requests for additional agent and capability resources (e.g. ancillary comm. modules, or software implants).
g. Direct the activation of witting and unwitting agents.
h. Collect and transmit information back to operational centers.
i. Interact and collaborate with other controllers.
j. Cognitively process collected information to inform and act according to the environment and the current situation.

In the current technology context, the ACT M&O may be viewed as a Cloud based management resource while controllers may be analogous to smart edge devices in proximity to the action. However, controllers may be deployed locally or remotely from the AOR, and not always immediate within an AOR. Further, a single virtual or physical controller device may not need to host all necessary functionality. Controller activity may reside on several distributed devices acting in harmony to provide the entire functionality.

An essential function of controllers is to abstract the heterogeneous nature of sensors and actuators. Sensors and actuators come in various forms and capabilities, adopt different communication protocols, and possess a multitude of wireless interfaces. The aim could be to construct controller family classes which each family class adapts and abstracts a set of capabilities for M&O (ultimately for human) interactions.

Mission and network management roles are to be assisted by an M&O infrastructure supporting the deployment of autonomous things. The right side of Figure 3, shown as Figure 5 below, illustrates the M&O automation building blocks.

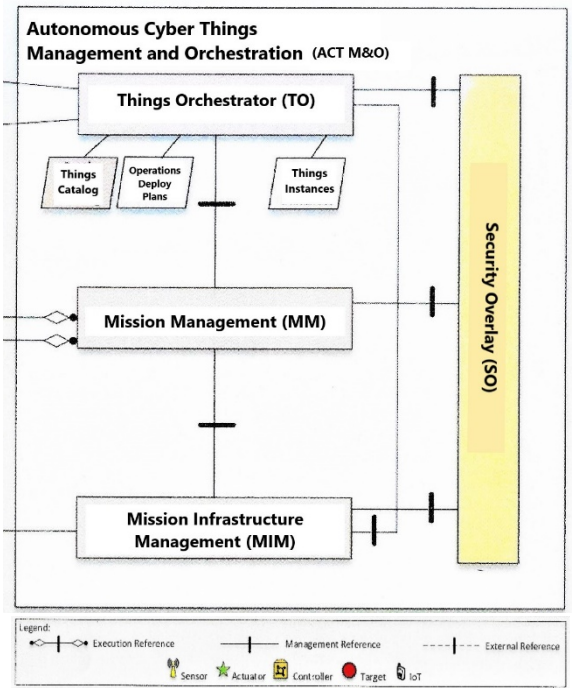

Figure 5. M&O building blocks

The ACT M&O framework is intended to be disruptive to existing network deployments with transformations predicated on changes in mind-sets, skills and tools. Autonomous agents will become ubiquitous with almost all network components evolving into agent-like entities in the future. It can be almost predicted that current network software virtualization once equipped with intelligent and cognitive algorithms may evolve into autonomous agent entities.

Building Blocks

M&O building blocks consist of TO, MM, MIM, and the Security Overlay (SO), as illustrated by Figure 5.

TO is positioned to provide for orchestration of things within the ACT M&O infrastructure. As

such, TO is expected to implement the following functionality:

a. Supports an interface for human operators for the deployment and operation of things. Effectively provides the autonomous agent human-machine interface.
b. Facilitates access to digitized network plans and layouts.
c. Facilitates access to digitized mission plans, Operating Orders (OPORDs), Tactics, Techniques, and Procedures (TTPs), and Standing Operating Procedures (SOPs).
d. Provides a catalog of available Cyber things and corresponding attributes and properties.
e. Facilitates operator interactions with controller agents via a management reference point connection with MM.
f. Dynamically, and on-demand, delivers deployable Cyber thing instances and modules in the form of executable applications, containers, or virtualized images. The dynamic process is conducted in support of either operator or autonomous controller requests.
g. Provisions access to compute, store, and network resources via a management reference connection point with MIM. Resources may be hosted on the Cloud, Cyber physical systems, or logical and virtual facilities.

MM is the management component of ACT M&O which interfaces with controller things over an execution reference point. MM is responsible for implementing the following:

a. Provides for the interaction and command and control of controllers by humans via a management reference connection point with TO, and an execution reference point connection with controllers.
b. Maintains awareness of multi-control configurations, and of distributed deployments in order to provide integrated situational views.

MIM is responsible for allocation and deallocation of infrastructure resources in the form of compute, store, and network facilities needed for the deployment of things. MIM supports mission planning, execution, and its termination by allocating and deallocating mission infrastructure resources. As such, MIM implements the following:

a. Supports network management tasks over a dedicated execution reference point connection with TO.
b. Allocates and maintains necessary resources to support autonomous agent deployment.
c. Deallocates resources upon mission termination.
d. Supports dynamic resource allocation and deallocation during mission conduct over a management reference point connection with MM. The dynamic process is conducted in support of either operator or autonomous controller requests.

SO is integrated over internal management reference point connections with TO, MM, and MIM functional blocks. SO is responsible to provide security protections across all aspects of the ACT M&O infrastructure. A few responsibilities are listed as examples, with a comprehensive specification to be defined during a future design and development phase:

a. Provides role-based authentication.
b. Maintains authentication and integrity of TO repository entities, catalogs, and resources.
c. Supports MM secure deployment of agent assets.

d. Supports the validation of MIM resource allocations.
e. Conveys security primitives (e.g. cryptographic keys, certificates, and hashes) to all ACT components, as well as to deployed assets and operator-initiated processes.

An overarching consideration consists of the security of autonomous agent manifestations. For instance, controllers are an extension of the infrastructure, hence adversarial attacks against controllers could adversely impact or compromise the entire infrastructure's M&O.

Conclusions and Future Work

An autonomous Cyber agent ecosystem consists of diverse components to include human operators, controller agents, sensors, actuators, and adversaries. Interactions between these entities requires the formulation of a framework which implements real-time cohesive management and orchestration with minimal or no human intervention. This paper presented the building blocks for a conceptual M&O infrastructure.

Delays introduced by network latencies and humans-in-the-loop would not support the speed of action required in the upcoming future. The building blocks for an infrastructure to support speedy autonomous actions, human-machine and machine-to-machine (M2M) interactions was outlined. Many topics were however left uncovered to include the following:

a. A Multi Domain Operations (MDO) and Multi-service things ontology with common semantics for proper data interpretation and fusion.
b. Formulation of sensor data collection, processing, and its distribution strategy. Transmission of raw data to central processing centers by millions of things deployed per square kilometer is not sustainable or realistic.
c. Efficient M2M communication protocols with low overhead in support of operations under dynamic environment changes.
d. Exploration of agent embedded ML techniques that best suit autonomous mission profiles in highly dynamic and unpredictable environments. Would also require the investigation of imposed adversarial effects.
e. Evaluation of distributed autonomous agent collaboration, including possible adoption of Federated Learning (FL).
f. Strategies for long-term and short-term data attribution/provenance in order to establish collective trust and meaning.
g. Conducting Autonomy Requirements Engineering (ARE) to formally define agent self-managed objectives.

The need for standing-up an experimental ACT M&O environment is a necessary endeavor. Various research is currently being conducted for the development of autonomous agents. No research for the cohesive integration and management of these agents is known to exist. Dedicate Science and Technology (S&T) research in support of the development of autonomous agent management strategies is critically needed.

References

1. "War of 2050: A Battle for Information, Communications, and Computer Security", Alexander Kott, Davis S. Alberts, Cliff Wang, US Army Research Office Workshop Report, 2015.
2. "Autonomous Battlefield Systems – Concept Paper", Paul Robb, Michael De Lucia, Bela Erdelyi, US Army I2WD and US ARL, 25 October 2017.
3. "The Internet of Battle Things", Alexander Kott, Davis S. Alberts, Cliff Wang, IEEE Computer Society, Computer, pp. 98-101, December 2015.
4. "Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments", Alexander Kott, US ARL, April 2018.

5. “Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture”, Paul Theron, et al, Proceedings of the 2018 International Conference on Military Communications and Information Systems, April 2018.
6. “Toward Intelligent Autonomous Agents for Cyber Defense: Report of the 2017 Workshop by the North Atlantic Treaty Organization (NATO) Research Group IST-152-RTG”, Alexander Kott, et al, US ARL, ARL-SR-0395, April 2018.
7. “Network Functions Virtualization (NFV); Management and Orchestration”, ETSI GS NFV-MAN 001 V1.1.1 (2014-12).