Argumentation-based Policy Analysis for Drone Systems

Erisa Karafili
Imperial College London
e.karafili@imperial.ac.uk

Emil C. Lupu
Imperial College London
e.c.lupu@imperial.ac.uk

Saritha Arunkumar
IBM UK
saritha.arun@uk.ibm.com

Elisa Bertino
Purdue University
bertino@purdue.edu

***Abstract*—The use of drone systems is increasing especially in dangerous environments where manned operations are too risky. Different entities are involved in drone systems' missions and they come along with their vast varieties of specifications. The behaviour of the system is described by its set of policies that should satisfy the requirements and specifications of the different entities and the system itself. Deciding the policies that describe the actions to be taken is not trivial, as the different requirements and specifications can lead to conflicting actions. We introduce an argumentation-based policy analysis that captures conflicts for which properties have been specified. Our solution allows different rules to take priority in different contexts. We propose a decision making process that solves the detected conflicts by using a dynamic conflict resolution based on the priorities between rules. We apply our solution to two case studies where drone systems are used for military and disaster rescue operations.**

***Keywords*-Drone systems, policy analysis, argumentation reasoning, policy conflict resolution, policy efficiency.**

I. Introduction

Drone systems operations are taking hold, especially in hazardous environments where manned operations are too risky and for invigilation and exploration operations. The level of autonomy of drones is increasing as often it is impossible to have ground bases, connectivity, or interactions, without compromising the security and the accomplishment of the mission. The drone system behaviour is described by a set of rules that we call *behavioural policies*, and are composed of the various security requirements, the legislation and normative rules, and the actions to be executed.

Usually different parties, coalitions and alliances are involved in various missions. The mission requires a large scale of planning and coordination, and has to take into account the rules and agreements between the different parties. The agreements take into consideration the relations between the parties, their respective coalitions, and the mission's goals. Therefore, deciding the rules that represent the actions to be taken in particular cases is not trivial. Due to the heterogeneity of the rules and the entities involved, various conflicts, redundancies and gaps may arise.

We introduce an argumentation-based policy analysis that captures the different conflicting policies and solves them by introducing preferences between policies in drone systems scenarios. The used rules are of different types, e.g., legal, security, data access, and are sensitive to the applied context. Our policy analysis identifies and solves conflicts between rules. The proposed solution allows different rules to take priority in different contexts. Thus, it solves the detected conflicts by using a dynamic conflict resolution based on the rules' priorities. The result of the conflict resolution is used by the decision process which decides the policies to apply for particular contexts, and also provides an explanation for the taken decisions.

We show the use of our argumentation-based policy analysis with two scenarios of drone systems: military operations and natural disaster rescue operations. In both cases, different entities with their specific requirements are involved, and the drones need to take efficient and prompt actions. In the military operations the main actors are the military organisations and the coalitions between different countries, e.g., UK and U.S., but sometimes also non-military organisations are involved, e.g., humanitarian ones. On the other hand, natural disaster rescue operations involve both military and non-military organisations, where the latter (e.g., civil protection) play an important role, and military organisations mainly provide the tools and the arrangements for the mission accomplishment. Deciding the policies to apply for every case is not easy, as the entities have different requirements. These organisations have various regulations between each other and the actions depend on the mission, the context, and the environment, e.g., the legal and normative rules depend by the type of use is made to the drones: military or humanitarian mission.

During military operations different parties and coalitions are involved. Usually the squad of involved drones communicate with each other. If the squad of drones is composed of drones from different countries, their communication should respect the conform regulations between countries. Different parties can be part of a joint mission, thus, the drones should send the information also to them. Deciding the policies that apply in this case is not easy, as the relations of the involved parties need to be taken into consideration.

In natural disaster rescue operations, the policies about sharing information are less restrictive because non-military organisations do not have strict security requirements. In this case, from the military organisations' point of view, sensitive information about the type of capabilities should not be revealed. The goal of the mission in this case is gathering information from rescue areas. Deciding the type

of data to be shared and the policies to be applied is not easy as different drones and entities are involved.

Lately, research focused on unmanned aircrafts (e.g., drone systems) is increasing, especially with the expansion of their usage, e.g., drones packages delivery like *Amazon's Prime Air* [1] or *Google's Project Wing* [2]. Different studies have been made by Amazon [3], [4], Google [5] and NASA [6] concerning the safety and efficiency of design, management, operations of unmanned aircraft systems (UAS), their safe airspace access, and their communications and collaborations. The authors in [7] present a model of architecture for coordinating the access of UAS to controlled airspace and for providing navigation services between interested locations. The increasing autonomy on the airborne drones in joint collaborative operations between different parties and their impact is analysed in [8].

An important challenge that arrises during the coordination and planning phases of drone systems, especially in collaborative scenarios, is the decision process of applicable actions for particular cases. The decision process is not a trivial task, due to the conflicting and redundant rules. We introduce a policy analysis that is able to capture and solve conflicting rules, and improve the efficiency of the used set of rules. The proposed analysis is based on argumentation based reasoning [9], [10] and abductive reasoning [11]. Argumentation reasoning is a suitable technique for implementing decision making mechanisms [12], [13] under conflicting and incomplete knowledge. The conflict resolution is made by introducing preferences between conflicting rules that is supported by our preference based argumentation reasoning. For implementing part of our analysis and conflict resolution we use the *GorgiasB*[1] [14] tool. This tool combines argumentation reasoning with preference-based rules and abductive logic programming. It is based on Gorgias [12] that is an argumentation framework that uses abduction with preference reasoning.

The introduced analysis is an extension of the one proposed in [15], [16] where argumentation based analysis together with abductive reasoning are used for enabling data sharing in different contexts by enforcing the correct data sharing agreements, and during forensics investigations for attributing cyber attacks to attackers. Another interesting technique that uses an argumentation based analysis is introduced in [17], where the authors present a method for goal conflict resolution by analysing competing hypotheses and beliefs of stakeholders. Argumentation reasoning is part of the non-monotonic reasoning, which permits to deal and solve conflicting rules. An interesting decision process for preference-based systems based on a non-monotonic reasoning is presented in [18], [19], where the authors present a defeasible decision process for energy saving techniques.

In this work, we show how to model and analyse the policies in drone systems scenarios with our argumentation-based policy analysis. We solve the conflicts between policies and decide the policies to be applied by using our dynamic conflict resolution.

We introduce our policy analysis and conflict resolution based on argumentation in Section II. We show with two scenarios how various conflicts are captured and solved in Section III. In Section IV, we conclude and discuss some of the future challenges of drone systems.

II. Argumentation-based Policy Analysis

For capturing the policies conflicts and redundancies, we introduce a policy analysis based on argumentation and abductive reasoning [15], [16]. This analysis is applied to drone systems behavioural policies and detects the conflicting policies, the redundant ones, and the cases that were not covered by the given set of policies. Identifying conflicting policies is not trivial, due to the different types of policies and to their context dependability, e.g., the security requirements state that the drone should share information with their ground bases, whenever it is possible, but in case the country that owns the drones is not a direct participant of the mission where its drones are involved, then the drones are forbidden to send any information to their country ground bases.

Our policy analysis captures context dependent conflicts and solves them thanks to the use of argumentation reasoning. Argumentation and abductive reasoning expressive power permits us to work with conflicting policies that have exceptions and preferences between them. For performing the redundancy analysis and finding gaps between policies we use abductive reasoning, in particular, an abductive constraints system called A-system[2] [20]. To identify and solve the policies conflicts and to apply the above reasonings to the drone systems policies we use the preference-based argumentation tool *GorgiasB* and its useful graphical user interface.

We first run the abductive reasoning analysis, that detects all the explicit conflicts, the redundancies and gaps in the given set of rules for the given pieces of information which might be incomplete. If any conflict, redundancy or gap is identified, then the drone systems administrator is notified for solving the inconsistencies or improving the efficiency of the set of rules. This analysis provides also explanations and the conflicting, redundant or missing cases, thanks to the use of abduction. The explanations are used by the systems administrator to solve the inconsistencies and improve the efficiency of the set of policies. Once the redundancies, gaps, and conflicts due to errors or misrepresentations are solved by the system administrator, the argumentation reasoning analysis is executed. This analysis detects all the conflicting rules, especially the context dependent ones. Argumentation

[1]GorgiasB http://gorgiasb.tuc.gr/

[2]A-system http://dtai.cs.kuleuven.be/krr/Asystem/

reasoning permits the resolution of conflicts, by introducing preferences/priorities between conflicting rules and by explicitly specifying the context when a particular rule has to be considered stronger than another one.

A preference relation denoted by $>$ is used to indicates the preferences between two policies. Given two conflicting policies p_1 and p_2, where for the context and the information we have, p_1 should be applied instead of p_2, we denote it with $p_1 > p_2$. The introduced priorities between rules, that for the sake of simplicity we will call *priority rules*, together with the existing rules are checked again, and if any conflict is found, the process is re-iterated, and other priority rules are introduced.

III. Use Cases: Policy Analysis for Drone Systems

In this section, we introduce two applications of the proposed policy analysis for drone systems. The scenarios are related between each other, as we assume that the same squad of drones can be used for different types of missions. In the below scenarios, we introduce the drone systems behavioural policies. We show how the conflicts and redundancies are captured using our argumentation-based analysis. As described in the previous section, our analysis tasks and the conflict resolution are performed using the A-system and GorgiasB tools.

A. A Military Scenario for Drone Systems

Let's assume, we are dealing with squad of drones that are property of a military organisation of a particular country. The behavioural rules of the squad of drones depend on its owner, i.e., the country/entity that owns the drones and their policies and legislations. These rules describe how the drones should behave, act, interact, and exchange information between drones of the same squad, and other entities like other squads, drones, countries. The main actors of the behavioural rules are the drones $\mathcal{D} = \{D_1, D_2, \cdots\}$, the squad of drones $\mathcal{S} = \{S_{C_1}, S_{C_2} \cdots\}$ where the drones are part, in this case C_1, C_2 represent the countries that owns the squad of drones, the ground bases $\mathcal{B} = \{B_1, B_2, \cdots\}$ that communicate with the squad of drones, the ground bases are part of the country ground base denoted by $\{\mathcal{G}_{C_1}, \mathcal{G}_{C_2}, \cdots\}$, where C_1, C_2 are the countries that own the ground bases. We deal also with the notion of resources of a country, which include all the drones, squad of drones and bases of that country, denoted with $\mathcal{R} = \{R_{C_1}, R_{C_2}, \cdots\}$, where C_1, C_2 are the countries that own these resources. We denote with O a particular object, when we do not want to specify its type (or it is not known).

Let's assume we are in a military scenario and we are dealing with an UK squad of drones. The drones' behavioural policies are as below:

1) The drones of the same squad can exchange encrypted information between each other.
2) The drones can send encrypted information to their ground base.
3) They do not send information to anybody else.

The above policies can be written in a semi-natural language as below[3], where on the right hand side we state the conditions that should hold for the left hand side action to be true or occur.

$$Send(D_1, D_2, data, permit) \leftarrow \{D_1, D_2\} \in S_{UK} \quad (1)$$

$$Send(D, B, data, permit) \leftarrow D \in S_{UK}, B \in \mathcal{G}_{UK} \quad (2)$$

$$Send(D, O, data, deny) \leftarrow D \in \mathcal{S}_{UK}, O \in R_C, C \neq UK \quad (3)$$

More specifically, the first rule says that if drones D_1 and D_2 are from the same squad owned by UK, then they are permitted to send data to each other. The second rule says that a given UK drone D can send data to a ground base B, if the latter is an UK ground base. The third rule says that a given UK drone D is not permitted (*deny*) to send data to non UK resources (bases or drones).

The squad of drones can be involved in military missions, we denote the missions with $\{\mathcal{M}_1, \mathcal{M}_2, \cdots\}$. Different countries can take part of the same mission, where some of them provide the needed equipment for the mission accomplishment. The involved countries can also be in alliance between each other, e.g., the NATO alliance, or create a coalition between countries, e.g., when the mission is located in a non ally country, but special relations are created with it for permitting the performance of the mission in that territory. We denote by $\{\mathcal{A}_X, \mathcal{A}_Y, \cdots\}$ the different alliances, and by $\{\mathcal{C}_X, \mathcal{C}_Y, \cdots\}$ the different coalitions.

When in the mission are involved different countries, the drones should alter their data, denoted by alt, before sending them, in a way to avoid the disclosure of sensible information. The data are classified in three types, depending on their security level and how much they can compromise the mission, the country and the alliance security: *low*, *medium*, *high*. The type of disclosed data depends on the relation of the countries that are part of the mission.

Returning to the above example, let's assume that UK is taking part of mission $\mathcal{M}$ with other allies countries, e.g., U.S., from the NATO alliance $\mathcal{A}_N$, and the mission is taking place in a non ally country C, that is in a coalition with the NATO countries, $\mathcal{C}_N$. The previous rules for UK drones were to send all the information to UK resources and do not send any information to other entities. In this case, as UK is in a joint mission with U.S. and C, for the accomplishment of the mission, UK drones need to share some information with these countries ground bases (the data are going to by altered). Suppose now, that in the middle of the mission, U.S. drones join the UK squad of drones. The UK drones should exchange information with the U.S. ones to coordinate the

[3]For the sake of simplicity, we assume that the data are always encrypted.

trajectory and divide the mission tasks. UK drones cannot share all types of information with U.S. drones and the information should be altered. The behavioural policies are described below.

4) In case the drones are part of a multi-country mission, then they send low and medium security type data to alliance bases, and the data are altered and encrypted.
5) In case the drones are part of a multi-country mission, then they send low security type of data to other coalition bases, and the data are altered and encrypted.
6) In case the drones are part of a multi-country mission and drones of other alliance countries are involved, then the drones can share low and medium type of data with their partner[4] allies drones, but by altering and encrypting the data.
7) In case the drones are part of a multi-country mission and drones of other coalition countries are involved with it, then the drones can share low type of information with their partner coalition drones, but by altering and encrypting the data.

The above rules can be represented as described below.

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{G}_C, \mathcal{G}_C \in \mathcal{M}, \{UK, C\} \in \mathcal{A}_N, \mathcal{A}_N \in \mathcal{M}, Data = alt(data), type(data) = \{low, medium\} \quad (4)$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{G}_C, \mathcal{G}_C \in \mathcal{M}, UK \in \mathcal{A}_N, \{C, \mathcal{A}_N\} \in \mathcal{C}_N, \mathcal{C}_N \in \mathcal{M} \quad Data = alt(data),\ type(data) = \{low\} \quad (5)$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{S}_C, \mathcal{S}_C \in \mathcal{M}, \{UK, C\} \in \mathcal{A}_N, \mathcal{A}_N \in \mathcal{M}, Data = alt(data), type(data) = \{low, medium\} \quad (6)$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{S}_C, \mathcal{S}_C \in \mathcal{M}, UK \in \mathcal{A}_N, \{C, \mathcal{A}_N\} \in \mathcal{C}_N, \mathcal{C}_N \in \mathcal{M} \quad Data = alt(data),\ type(data) = \{low\} \quad (7)$$

In this case, our analysis finds that rules (4), (5), (6) and (7) are in contradiction with rule (3), as rule (3) is denying the access to all the entities that are not UK resources. Being on a multi-country mission is more specific than doing a mission alone and not sharing information can bring the non accomplishment of the mission. Hence, being in a multi-country mission brings the four last rules to take hold over rule (3). When the squad of drones is on a mission with other countries, they can share altered information with their partner bases and drones. Thus, we introduce the following priority rules: (4) $>$ (3), (5) $>$ (3), (6) $>$ (3) and (7) $>$ (3).

Sometimes, a country is not part of a joint mission, but provides the necessary instruments, e.g., squad of drones, ground bases. In this case, for not revealing sensitive information to countries that are not directly involved with the mission and do not have clearance for accessing that information, the drones send information just to the mission participants, and not to their own bases. The decision of the policies to apply in this case is context dependent, as it depends on the type of regulations between the countries, the coalitions, and the regulations of the drones' owner country.

8) In case the squad of drones is involved in a mission where their owner is not directly involved but provides technical support, the drones can send encrypted data to each other.
9) The above drones send encrypted and altered data of all security types (low, medium, high) to the ground allies bases that are part of the mission.
10) The above drones send encrypted and altered data of low security type to the coalition ground bases that are part of the mission.
11) They send encrypted and altered data to the partners alliance drones.
12) They send encrypted, altered and low security type data to the partners coalition drones.
13) They cannot send any data to their own bases, as they are not part of the mission.
14) They cannot send any data to any other subject.

Suppose that UK is providing a squad of drones to NATO for using them in an invigilating mission, $\mathcal{M}$, around a given area, where also a coalition country C is involved in it with coalition C_N. The UK drones should continue to send data between each other, as shown in rule (8).

$$Send(D_1, D_2, data, permit) \leftarrow D_1, D_2 \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, UK \notin \mathcal{M} \quad (8)$$

Our policy analysis is able to identify a redundancy between rule (8) and rule (1), as rule (8) is included in rule (1), because it is a specific case of it. Thus, we can remove rule (8) for avoiding redundancies and improving the efficiency of the decision process.

As U.S. is part of the mission $\mathcal{M}$, the UK drones should send all their data to U.S. ground bases, as described in rule (9). This policy is an extension of rule (4) and is in conflict with rule (3). In case the country is providing technical support to the mission but is not participating in it, then rule (9) has higher priority than rules (4) and (3), denoted as (9) $>$ (4) and (9) $>$ (3). The same reasoning applies to rule (11) that describes the type of data that UK drones can share with other alliances drones, that is an extension of rule (6) and contradicts rule (3). Thus, rule (11) is stronger than rules (6) and (3), denoted as (11) $>$ (6) and (11) $>$ (3).

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{G}_C, \mathcal{G}_C \in \mathcal{M}, \{UK, C\} \in \mathcal{A}_N, \mathcal{A}_N \in \mathcal{M}, UK \notin \mathcal{M}, Data = alt(data) \quad (9)$$

[4]We call partner drone/base when a drone/base is involved in the same mission and it is owned by an ally or a coalition country.

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{G}_C, \mathcal{G}_C \in \mathcal{M}, UK \in \mathcal{A}_N, \{C, \mathcal{A}_N\} \in \mathcal{C}_N, \mathcal{C}_N \in \mathcal{M} \; UK \notin \mathcal{M}, Data = alt(data), type(data) = \{low\} \tag{10}$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{S}_C, \mathcal{S}_C \in \mathcal{M}, \{UK, C\} \in \mathcal{A}_N, \mathcal{A}_N \in \mathcal{M}, UK \notin \mathcal{M}, Data = alt(data) \tag{11}$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{S}_C, \mathcal{S}_C \in \mathcal{M}, UK \in \mathcal{A}_N, \{C, \mathcal{A}_N\} \in \mathcal{C}_N, \mathcal{C}_N \in \mathcal{M} \; UK \notin \mathcal{M}, Data = alt(data), type(data) = \{low\} \tag{12}$$

Rules (10) and (12) are contained correspondingly in rules (5) and (7), that describe how UK drones can share data with resources of coalition countries. The same holds for rule (14) that is contained in rule (3). Our policy analysis is able to capture these redundancies, and in this case, rules (10), (12) and (14) can be removed.

The most interesting rule is the one saying that UK drones should not send information to UK ground bases, rule (13). This rule is in contradiction with rule (2) that describes drones behaviour, and states that the drones should send their data to their ground bases. In this case rule (13) is stronger than rule (2), denoted with (13) $>$ (2), as UK is not part of the mission.

$$Send(D, O, data, deny) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{G}_{UK}, \mathcal{G}_{UK} \notin \mathcal{M}, UK \notin \mathcal{M} \tag{13}$$

An interesting case for the described scenario is when the drones that are part of the mission have sensitive information related to the drones safety and operation (this information can be of all types of security level). In this case, the drones should send the sensitive information to their bases when one of the involved countries in the mission grant this permission.

15) In case the drones of a squad are involved in a mission where their owner is not directly involved, then the drones are permitted to send sensitive data, related to their operation and safety, to their ground bases, when they have the permission, $grant\_perm$, from one of the countries or the alliance involved in the mission.

$$Send(D, O, data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{G}_{UK}, \mathcal{G}_{UK} \notin \mathcal{M}, UK \notin \mathcal{M}, type(data) = sensitive, grant\_perm(C', D), C' \in \mathcal{M} \tag{15}$$

The above rule is in contradiction and stronger than rule (13), as we are dealing with sensitive data. Thus, rule (15) $>$ rule (13).

All the above conflicts are detected and solved using GorgiasB. Once the analysis and conflict resolution are made, the set of policies is ready to be tested.

B. A Disaster Rescue Operation Scenario for Drone Systems

In case of a disaster rescue operation different types of entities are involved, e.g., military organisations, humanitarian entities, civilian volunteers. The main goal is to help and rescue life in an efficient and swift way. Coordinating the different entities is not trivial, as they have their behavioural rules, and some of them have not collaborated before.

During a disaster rescue operation, especially in natural disasters, military entities and their equipments are involved. Therefore, as the mission does not have any security (national or military concern) the division of data in security types is not needed any more. The alteration of the data is still needed, as the data can be used or stolen by malicious users that can extract information about the drone systems capabilities. Thus, the squad of drones, used for gathering data about a certain area, share all security type of data with other drones or ground bases involved in the mission.

16) The drones of the same squad exchange encrypted information between each other.
17) The drones can send encrypted information to their ground base.
18) In case the drones are part of a rescue operation mission[5], RO, and drones of other entities are involved with it, then the drones can share all type of data with their partner drones, by altering and encrypting them.
19) In case the drones are part of a RO mission, then they can send all type of data to other bases, by altering and encrypted them.

$$Send(D_1, D_2, data, permit) \leftarrow \{D_1, D_2\} \in \mathcal{S}_{UK} \tag{16}$$

$$Send(D, B, data, permit) \leftarrow D \in \mathcal{S}_{UK}, B \in \mathcal{G}_C, C = UK \tag{17}$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{S}_C, \mathcal{S}_C \in \mathcal{M}, Data = alt(data), type(\mathcal{M}) = RO \tag{18}$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{G}_C, \mathcal{G}_C \in \mathcal{M}, Data = alt(data), type(\mathcal{M}) = RO \tag{19}$$

Our policy analysis identifies redundancies between rules (16), (17) and (1), (2). Therefore, the knew rules are not needed and can be removed. Rules (18) and (19) are in contradiction with rule (3) and correspondingly with rules (6), (7) and (4), (5). In case of a disaster rescue operation, rules (18) and (19) have higher priority than the others, (18) $>$ {(3), (6), (7)} and (19) $>$ {(3), (4), (5)}.

IV. Conclusion and Future Work

The increasing use of drone systems, in particular in military scenarios, comes along with the need of extending the level of autonomy of these systems. Various entities can be involved in drone systems' missions, increasing the heterogeneity of the involved rules. Drone systems given the various rules of behaviour and actions, depending on the environment and the type of mission, should decide the rules to apply. Making this decision is not trivial, as the

[5]We introduce the type of mission, denoted by $type$, where rescue operation mission $\mathcal{M}$ has type $type(\mathcal{M}) = RO$.

involved rules can be in conflict between each other, redundant, incomplete or not applicable. For solving this problem we propose an argumentation-based analysis that given the drone systems' rules analyzes them and solves their conflicts by putting priorities between rules. The decision making process uses these priorities to decide the rules to apply for particular contexts. We show how our argumentation-based analysis works in two scenarios: military operations and disaster rescue operations.

The introduced technique performs a dynamic conflict resolution, where depending on the contexts different priorities apply. In the future, we will combine our analysis with the behavioural analysis [21], which will bring a great benefit to the efficiency of the set of behavioural policies of drone systems. We plan to increase the level of autonomy of drone systems decision making by using generative policies [22], [23]. An interesting work is to construct policy analysis and analytics for drones systems that use generative policies.

ACKNOWLEDGMENTS

Supported by EPSRC Project CIPART grant no. EP/L022729/1. 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 copyright notation hereon.

REFERENCES

[1] Amazon.com Inc, "Amazon prime air." [Online]. Available: https://www.amazon.com/b?node=8037720011

[2] Google X, "Project wing." [Online]. Available: https://x.company/wing/

[3] Amazon.com Inc, "Determining safe access with a best-equipped, best-served model for small unmanned aircraft systems," 2015. [Online]. Available: https://images-na.ssl-images-amazon.com/images/G/01/112715/download/Amazon_Determining_Safe_Access_with_a_Best-Equipped_Best-Served_Model_for_sUAS.pdf

[4] ——, "Revising the airspace model for the safe integration of small unmanned aircraft systems," 2015. [Online]. Available: https://images-na.ssl-images-amazon.com/images/G/01/112715/download/Amazon_Revising_the_Airspace_Model_for_the_Safe_Integration_of_sUAS.pdf

[5] Google Inc, "Google UAS Airspace System Overview," 2015. [Online]. Available: https://utm.arc.nasa.gov/docs/GoogleUASAirspaceSystemOverview5pager[1].pdf

[6] NASA, "NASA UTM 2015: The next era of aviation," 2015. [Online]. Available: https://utm.arc.nasa.gov/utm2015.shtml

[7] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[8] A. Cullen, B. Williams, E. Bertino, S. Arunkumar, E. Karafili, and E. Lupu, "Mission support for drones: A policy based approach," in *DroNet*, 2017.

[9] A. Bondarenko, P. M. Dung, R. A. Kowalski, and F. Toni, "An abstract, argumentation-theoretic approach to default reasoning," *Artif. Intell.*, vol. 93, pp. 63–101, 1997.

[10] P. M. Dung, "On the acceptability of arguments and its fundamental role in nonmonotonic reasoning, logic programming and n-person games," *Artif. Intell.*, vol. 77, no. 2, pp. 321–358, 1995.

[11] A. C. Kakas, R. A. Kowalski, and F. Toni, "Abductive logic programming," *J. Log. Comput.*, vol. 2, no. 6, pp. 719–770, 1992.

[12] A. Kakas and P. Moraitis, "Argumentation based decision making for autonomous agents," in *AAMAS*. ACM, 2003, pp. 883–890.

[13] A. K. Bandara, A. C. Kakas, E. C. Lupu, and A. Russo, "Using argumentation logic for firewall configuration management," in *IM*, 2009, pp. 180–187.

[14] N. I. Spanoudakis, A. C. Kakas, and P. Moraitis, "Gorgias-B: Argumentation in practice," in *COMMA*, 2016, pp. 477–478.

[15] E. Karafili and E. C. Lupu, "Enabling data sharing in contextual environments: Policy representation and analysis," in *SACMAT '17*. ACM, 2017, pp. 231–238.

[16] E. Karafili, A. C. Kakas, N. I. Spanoudakis, and E. C. Lupu, "Argumentation-based security for social good," 2017. [Online]. Available: http://arxiv.org/abs/1705.00732

[17] P. K. Murukannaiah, A. K. Kalia, P. R. Telangy, and M. P. Singh, "Resolving goal conflicts via argumentation-based analysis of competing hypotheses," in *RE*, 2015, pp. 156–165.

[18] M. Cristani, C. Tomazzoli, E. Karafili, and F. Olivieri, "Defeasible reasoning about electric consumptions," in *AINA*, 2016, pp. 885–892.

[19] C. Tomazzoli, M. Cristani, E. Karafili, and F. Olivieri, "Non-monotonic reasoning rules for energy efficiency," *JAISE*, vol. 9, no. 3, pp. 345–360, 2017.

[20] B. V. Nuffelen and A. C. Kakas, "A-system: Declarative programming with abduction," in *LPNMR*, 2001, pp. 393–396.

[21] M. Touma, E. Bertino, B. Rivera, D. Verma, and S. Calo, "Framework for behavioral analytics in anomaly identification," in *SPIE*, 2017.

[22] E. Bertino, S. Calo, M. Touma, D. Verma, C. Williams, and B. Rivera, "A cognitive policy framework for next- generation distributed federated systems," in *ICDCS*, 2017.

[23] D. Verma, S. Calo, S. Chakraborty, E. Bertino, C. Williams, J. Tucker, and B. Rivera, "Generative policy model for autonomic management," in *DAIS*, 2017.