Policy Analysis for Drone Systems: An Argumentation-Based Approach

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 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 conflictual policies. 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 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. 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. Usually different parties, coalitions and alliances are involved in various missions. 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 a policy analysis argumentation and abductive reasoning [1]–[3] 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.

II. Policy Analysis for Drone Systems

We show the use of our argumentation-based policy analysis with two scenarios of drone systems: military operations and natural disaster rescue operations.

A. A Military Scenario for Drone Systems

During military operations different parties are involved. 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. Deciding the policies that apply in this case is not easy, as the relations of the involved parties need to be taken into consideration.

Let's assume, we have a squad of drones, S, property of a particular country, e.g. UK, in this case, denoted by S_{UK}. The behavioural rules of the squad of drones depend on its owner and the owners policies and legislations, that describe how the drones should behave, act, and exchange information between drones of the same squad, and other entities. 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, $\mathcal{G}_{UK}$.
3) They do not send information to anybody else.

The above policies can be written in a semi-natural language as below, where D_1, D_2, D denote the drones, B the ground base, O an object.

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

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

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

UK is 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, $\mathcal{C}_N$. In this case, as UK is in a joint mission with U.S. and C, then UK drones need to share some information with these countries ground bases (the data are going to by altered). In the middle of the mission, U.S. drones join the UK squad of drones. The UK drones should exchange part of their information (by altering it) with the U.S. ones to coordinate the trajectory and divide the mission tasks. Below are given the policies rules for this case, where the drones are part of a multi-country mission.

4) The drones send low and medium security type data (encrypted and altered) to alliance bases.

5) The drones send low security type of data (encrypted and altered) to other coalition bases.
6) The drones share low and medium type of data (encrypted and altered) with their partner allies drones.

The above rules can be represented as described below.

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

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

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

In this case, our analysis finds that rules (4), (5), and (6) 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, as not sharing data can bring the non accomplishment of the mission. Hence, the three last rules to take hold over rule (3), the following priority rules are introduced: (4) $>$ (3), (5) $>$ (3), (6) $>$ (3).

B. A Disaster Rescue Operation Scenario for Drone Systems

Natural disaster rescue operations involve both military and non-military organisations, where the formers provide the tools and the arrangements for the mission accomplishment. In this case, the policies for sharing information are less restrictive because no strict security requirements are needed. From the military organisations' point of view, sensitive information about the type of capabilities should not be revealed. The main goal is to help and rescue lifes, by gathering information from rescue areas.

The squad of drones, used for gathering data for a certain area, share all security type of data with other involved drones or ground bases. The alteration of the data is still needed, as the data can be used or stolen by malicious users to reveal systems capabilities.

7) The drones of the same squad exchange encrypted information between each other.
8) When the drones are part of a rescue operation mission, $type(\mathcal{M}) = RO$, then they send all type of data (altered and encrypted) to the involved drones.
9) When the drones are part of a RO mission, then they send all type of data (altered and encrypted) to the involved ground bases.

$$Send(D_1, D_2, data, permit) \leftarrow \{D_1, D_2\} \in \mathcal{S}_{UK} \quad (7)$$

$$Send(D, O, Data, permit) \leftarrow D \in \mathcal{S}_{UK}, \mathcal{S}_{UK} \in \mathcal{M}, O \in \mathcal{S}_C, \mathcal{S}_C \in \mathcal{M}, Data = alt(data), type(\mathcal{M}) = RO \quad (8)$$

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

Our policy analysis identifies redundancies between rules (7) and (1), where rule (7) is removed. Rules (8) and (9) are in contradiction with rule (3) and correspondingly with rules (6) and (4), (5). In case of a rescue operation, rules (8) and (9) have higher priority than the others, $(8) > \{(3), (6)\}$ and $(9) > \{(3), (4), (5)\}$.

III. Conclusion

We propose an argumentation-based analysis that given the drone systems' rules analyzes them and solves their conflicts by putting priorities between rules. 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 [4], which will bring 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 [5]. An interesting work is to construct policy analysis and analytics for drones systems that use generative policies.

Acknowledgments

Partially 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] E. Karafili, E. C. Lupu, S. Arunkumar, and E. Bertino, "Argumentation-based plicy abalysis for drone systems," in *IEEE Smart World Congress, DAIS Workshop*, 2017.

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

[3] 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

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

[5] 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.