Resilient and Robust Human-Agent Collectives: A Network Perspective

Willy Picard

Resilient and Robust Human-Agent Collectives: A Network Perspective

Willy Picard

Department of Information Technology,
Poznań University of Economics and Business
al. Niepodległości 10,
61-875 Poznań, Poland
picard@kti.ue.poznan.pl

Abstract. Human and software agents are more and more often interacting in groups in which directives are originated as well as addressed by humans or software agents. Among challenges raised by the rise of such heterogeneous groups, referred to as Human-Agent Collectives (HACs), resilience and robustness remain an open question. In this paper, the factors that influence the resilience and robustness of HACs are identified based on former research concerning interdependent and complex networks. The two main factors identified in the paper are 1) interactions between HACs with their open-networked environment, 2) the structure of the interactions among members of the HACs.

Keywords: Human-Agent Collectives; HAC; resilience, robustness, interdependent networks, small-world networks

1 Introduction

With the rise of the internet of think and the ubiquity of ICT, humans are interacting more and more with various electronic devices and information systems. These devices and systems provide not only means to sense and act on the surrounding world, they also allow for distant, often complex, interactions between humans. As such, humans and devices often collaborate within limited temporal frames to achieve a common goal. An example of such interactions is the process of online booking at airport during which many actions are performed by humans with the help of various systems, depending if the booking process is taken from the perspective of the traveler, of the airline company officer that checks the travelers, or the immigration officer.

The collaboration with devices and information systems may take different forms: in some cases, the human being is controlling the device, by asking the device to perform in a given manner. However, in more and more frequent cases, the device is asking the human to behave in a given manner: in the case of online booking at the airport, the information system instructs the traveler about the information to be provided to the system. Another example of a system that instruct human being are

most hotlines, especially in the e-banking sector: the system directly asks the customer to press some keys to perform certain tasks.

Therefore collaboration may take place within groups whose members can be humans or agents. In the remaining of this paper, the word "agents" refers to electronic devices and information systems. Importantly, the social relations between humans and agents are not based on a fixed hierarchy: humans may instruct other humans or agents as well as agents may instruct other humans or agents.

Human-Agent Collectives (HACs) have been proposed by Jennings et al. [1] as a new concept to capture these type of collaborative systems. Jennings et al. define HAC as "a new class of socio-technical systems in which humans and smart software (agents) engage in flexible relationships in order to achieve both their individual and collective goals. Sometimes the humans take the lead, sometimes the computer does and this relationship can vary dynamically" [1]. Among key research challenges related to HACs, they have identified, among others, "achieving flexible autonomy between humans and the software, and constructing agile teams that conform and coordinate their activities".

Underpinning the question of flexible autonomy, the question of resilience and robustness for HACs is not mentioned in [1] although it has to be addressed, especially in the concept of open environments. There is a need to identify factors that influence the resilience and robustness of human-agent collectives. Although other aspects of HACs, such as flexibility, agility, efficiency, effectiveness, responsiveness, and stability, still need to be addressed, we choose to focus in this paper on the aspects of resilience and robustness.

In this paper, we will present an analysis of the problem of resilience and robustness of HACs from the perspective of networks and based on the results of former works on complex and interdependent networks. The basic concepts underlying this paper are presented in Section 2, starting from robustness and resilience, followed by human-agent collectives. In Section 3, the interactions between HACs with their open-networked environment are presented as an important factor influencing the resilience and robustness of HACs. In Section 4, the structure of the interactions among members of the HACs, especially when structured as small-world networks, are discussed as a second important factor influencing the resilience and robustness of HACs. Finally, Section 5 concludes this paper.

2 Basic Concepts

2.1 Robustness and Resilience

The concepts of robustness and resilience have been studied in various scientific fields such as ecology [2], transportation [3], digital forensics [4], or supply chains [5]. Currently, there is no consensus on a broadly accepted definition of these concepts.

Although these concepts are related, they are different and refer to two distinct characteristics of systems that should not be considered as synonyms. The concept of robustness refers to "the ability to withstand or survive external shocks" [6]. As an

illustration, most nuclear plants are robust, as they may continue to operate even in the case of external shocks.

In this paper, we adopt the definition of resilience given by Haimes as "the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks" [7]. The concept of resilience is related with the idea that a resilient system may absorb shocks and adapt to the damages caused by these shocks. While a robust system withstands shocks *by construction*, thanks to its internal constitution, a resilient system withstands shocks *by behavior*, thanks to its adaptation capabilities. As an example, urban road transportation systems are resilient as, although some traffic jam may congest a large part of a city, the traffic will be redirected to other streets and arterial roads to keep the transportation system working.

2.2 Human-Agent Collectives

The concept of Human-Agent Collectives (HACs) has been forged by Jennings et al. in [1]. The term HAC aims at reflecting "the close partnership and the flexible social interactions between the humans and the computers. As well as exhibiting increased autonomy, such systems are inherently open and social. This openness means participants need to continually and flexibly establish and manage a range of social relationships".

One may recognize in HACs characteristics of Collaborative Networks defined as "a network consisting of a variety of entities—organizations and individuals—that are largely autonomous, geographically distributed, and heterogeneous in terms of their operating environment, culture, social capital and goals, which collaborate to better achieve common or compatible goals, and whose interactions are supported by computer networks" [8]. Therefore HACs are CNs in which entities may be either humans or agents and the interactions are not only supported by computer networks, but they can also be initiated by entities existing only on computer networks (i.e., agents). In HACs, the control usually shifts between humans and agents in a flexible manner.

HACs exhibit the following characteristics as collaborative networks:

- *Socially heterogeneous* – humans and agents are related by very different social bounds. Power is exerted in a different manner between humans, between humans and agents, and between agents;
- *Embedded in an open environment* – when both humans and agents are always connected to the Internet, HACs have to face the possibility of a broad variety of competitive entities (humans or agents) that may potentially perform the tasks of some entities of the HAC in a competitive manner;
- *Adaptive* – Not only humans have to react to changes in the HAC and its environment, but agents should also be able to adapt to highly adaptive human decision making processes. As a consequence, the whole HAC itself often has to adapt by changing its structure, shifting control from members to members.

These characteristics of HACs lead to a set of major research challenges, among which Jennings et al. pointed out:

1. *Flexible autonomy* – "flexible autonomy […] allows agents to sometimes take actions in a completely autonomous way without reference to humans, while at other times being guided by much closer human involvement".
2. *Agile teaming* – agile teams should be able to "come together on an ad hoc basis to achieve joint goals and then disband once the cooperative action has been successful".
3. *Incentive engineering* – as a result of incentive engineering, "the actors' rewards are designed so the actions the participants are encouraged to take generate socially desirable outcomes"
4. *Accountable information infrastructure* – an "accountable information infrastructure […] allows the veracity and accuracy of seamlessly blended human and agent decisions, sensor data, and crowd-generated content to be confirmed and audited".

One may notice that the second and third points are objects of research for the community focusing on CNs, and that HACs could probably benefit from the results concerning CNs in these areas.

3 Robustness of HACs in Interdependent Networked Environments

3.1 Interdependent Networks

HACs operate in open, networked environments. In these networks, it is frequent to observe various networks, interacting one with another. A well-known example of this fact is the structure of IT networks according to the Open Systems Interconnection model, known as the OSI model [9]. In this model, 7 layers, corresponding to various networks, are defined and their potential interactions are defined. In HACs, agents are usually related to various networks, such as telecommunication networks, application networks, social networks, corporate networks…

Interdependent networks are defined as a set of networks whose nodes and links are connected by *epilinks.* We define an epilink as a link connecting two nodes, or two links, or a link and a node from two networks. The concept of an interdependent network captures the idea that various networks may influence each other. For, example, in metropolises, the exchange of ideas and information via social media relies on infrastructural networks, such as the wired and wireless Internet or cable television. Similarly, attendance of a child at a given school is often related with the existence of appropriate transportation means, which illustrates the interdependence between social networks and infrastructure networks. Interdependence between

networks is usually reciprocal, i.e., if a network A influences a network B, then the network B often influences the network A as well. As an example, not only is the school attendance of children correlated with available transportation means, but also transportation means, especially the capacity and timetable of public transportation, are usually evolving to appropriately support the population of children attending schools.

3.2 Failure Propagation in HACs and Surrounding Interdependent Networks

Buldyrev et al. [10] have shown that the dynamics of interdependent networks is a novel surprising field of study. They have studied the robustness of a set of interdependent networks, i.e., the vulnerability of interdependent networks to the removal of nodes and links. The results of this study are that interdependent networks are less robust than each network is isolation due to cascades of failure from one network to another. And "surprisingly, analysing complex systems as a set of interdependent networks may destabilize the most basic assumptions that network theory has relied on for single networks" [10].

An exhaustive list of studies of interdependent networks is provided in [11] and [12].

As HACs are embedded in interdependent open networks, they are also exposed to the weaknesses pointed out by Buldyrev et al.: as an HAC is connected to an interdependent network, the robustness of the HAC may be deeply affected by potential *cascades* and *propagations* in the surrounding interdependent network. The case studied by Buldyrev et al. was related with a failure in the Italian electric grid, which has propagated to the Italian Internet (Internet routers needed energy to work), which has propagated back to the electric grid (as power stations are controlled remotely via the Web). Other examples of cascades and propagations in interdependent networks may be found in the area of infrastructure networks, transportation networks, and the financial sector and its recent crisis.

In the scenario of a failure in the HAC, a similar scenario may happen: not only the other members of the HAC may be directly affected by the failure, but they may also be affected in an indirect manner: the member that fails may by connected by one network to the surrounding interdependent open environment. In the surrounding environment, the failure may propagate to another network via epilinks, which may further affect another member of the HAC. Figure 1 illustrates this scenario.

The risk that the surrounding open interdependent environment introduces for HACs may be mitigated:

1) by reducing the number of interactions with the environment, which reduces the probability of a failure directly cause by the surrounding network. An entity may play the role of a façade to the HAC with regards to the surrounding environment, hiding the remaining member of the HAC from the environment, and therefore protecting them;

2) by limiting the number of networks to which the various members of the HACs are connected to in the surrounding environment. As a result, failures propagated via epilinks will less probably cause failures to HAC members connected to the surrounding interdependent network.

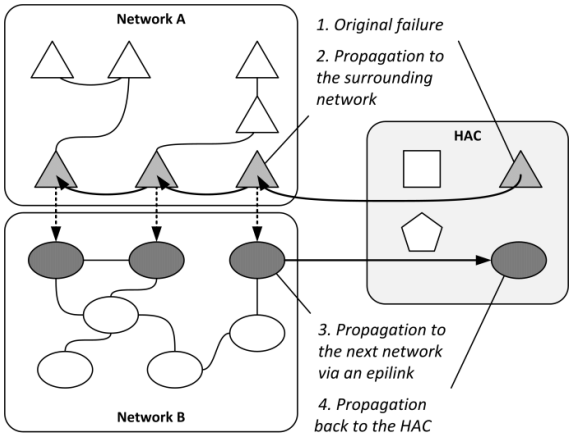

Fig. 1. Failure propagation in HACs and surrounding interdependent open networks

4 Internal Structure of HACs as a Key Factor of Resilience

While the interdependent structure of the surrounding environment has an influence on the robustness of HACs, the key factor of resilience for HACs is related to their internal structure, which is defined, to a large extent, by its network structure.

4.1 Popular Network Structures

Networks have been the object of intense research works since the late 1990's. Among key characteristics of networks, the clustering coefficient, the scale-free and the small-world properties of some networks have been intensively scrutinized. The *clustering coefficient* is a measure of the tendency of nodes to connect to other nodes within groups of nodes. The highest the clustering coefficient, the highest the number of connected triplets of nodes. *Scale-free networks* are networks in which the probability that a randomly selected node has k links, i.e., degree k follows $P(k) \sim k^{-\gamma}$, where γ is the degree exponent. In *scale-free networks*, a limited number of nodes have a large number of links (a large degree), while a large number of nodes have a small number of links (a small degree). Small-world networks are graphs in which the clustering coefficient is high and the average path length is small. In small-world networks, a relatively small number of nodes separate any two of them, even if most nodes are not connected to each other.

Popular models of structure of networks are:

- *the Erdős–Rényi model* – this model is a random model in which the links between nodes are added in a random manner. Clustering of Erdős–Rényi networks is low;
- *the Barabàsi-Albert model* – in this model, a newly added node is connected to other nodes of the network, such that the probability to connect to a given node is proportional to the degree of this node. Barabàsi-Albert networks are scale-free and their clustering coefficient is usually higher than in Erdős–Rényi networks;
- *the Watts-Strogatz model*: – in this model, a regular network, in which each node is connected to its neighbors, is modified by replacing with a given probability β the end destination node of each link by a randomly chosen different node. The Watts-Strogatz model may generate random networks, similar to Erdős–Rényi networks, as well as regular networks, depending on the value of β. Even small values of β lead the generation of small-world networks, although not scale-free ones;
- *the hierarchical model*– in this model, a network pattern is iteratively replicated, leading to a hierarchical organization. Hierarchical networks may be both small-world networks and have a high clustering coefficient.

4.2 Resilience of Networks

The resilience of networks has been largely studied in the literature, mostly from a topological perspective. It has been shown that the resilience of a networks depends not only of its structure but also depends on the type of attack. Albert et al. have demonstrated that scale-free networks are highly resistant to attacks focused on random nodes, but they are very vulnerable to attacks targeting the hubs, i.e., highly interconnected nodes.

In [14], Watts provides an analysis of the 1997 Toyota-Aisin crisis with regards to resilience and network topology. On February 1, 1997, a fire started in the Toyota Aisin factory. This factory was producing almost all p-valves, a valve used to control the fluid pressure in brakes. Without almost any stock, the destruction of the Aisin factory may cause the interruption of the whole Toyota production. However, within 4 days, Toyota was producing its first p-valves with the help of its other factories and business partners.

According to Watts, the resilience of Toyota in the Aisin incident was due to the structure of the social and organizational network. On the one hand, the Japanese culture has imposed a strongly hierarchical organization within Toyota. On the second hand, due to internal policies providing strong incentives for employee mobility, many horizontal relations between various factories have been created by employees visiting other factories for a few months.

This particular network structure, consisting of a highly regular structure and many shortcuts, allows to control the exchange of information (on the regular structure) but

also to speed up and to *recover* from failure (with shortcuts) if the regular structure is partially destroyed. One may notice that the idea of a regular structure rewired with shortcuts is at the heart of small-world networks [15]. Figure 2 illustrates this type of network structure.

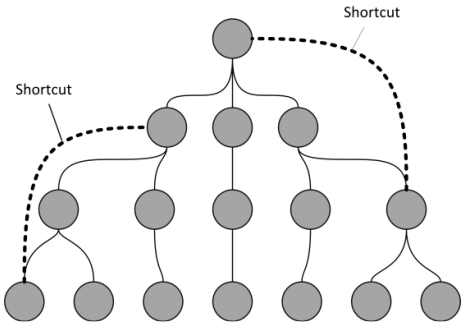

Fig. 2. A resilient network with a regular hierarchical network and shortcuts.

Following the Aisin-Toyota case, HACs could rely on their internal structure, especially shortcuts between their members to increase resilience. In case of a failure of an HAC member, shortcuts can be used to recover efficiently by increasing the speed of information exchange among HAC members.

5 Conclusions

HACs are a novel type of collaborative networks in which both humans and agents can ask their counterparts to take some actions. HACs requires additional works in many areas, including technical and business ones.

As far as resilience and robustness are concerned, HACs are facing various important challenges. For the robustness of HACs, the open interdependent networked environment in which they exist is an important challenge as the interdependency of the networks in the surrounding environment is potentially strongly degrading the robustness of HACs.

From a broader perspective, although interdependent networks have been studied in various contexts, e.g., critical infrastructure or population mobility, there is still a need for a unifying theory of interdependent networks that would encompass and largely extend former studies in a structured and organized manner.

For the resilience of HACs, their internal structure plays an important role: an appropriate structure, with shortcuts, may allow an HAC to rapidly recover from a failure by rapidly exchanging information among the remaining HAC members, which speed up the decision making process related with recovery.

The case of Toyota is a very interesting example of resilience within networks of networks. Or to be precise, Toyota may be considered as an organization consisting of various organizational entities. These organizational entities are collaborating in a

similar way to collaborative networks. The case of the fire in the break factory of Toyota illustrates the idea that collaborative networks, if appropriately structured can be resilient.

Finally, this paper is in not proposing an exhaustive treatment of the hard question of robustness and resilience of HAC, leaving many questions not only unanswered but even unformulated: what is the role of trust for the resilience and robustness of HACs and how to measure/improve it? Is it possible to adopt preventive measures to improve the robustness and resilience of HACs? These questions remain open and are waiting for further attention.

References

1. Jennings, N.R., Moreau, L., Nicholson, D., Ramchurn, S., Roberts, S., Rodden, T., Rogers, A.: Human-Agent Collectives. Communications of the ACM, 57-12, 80--88 (December 2014), http://dx.doi.org/10.1145/2629559.
2. Meerow, S., Newell, J.P.: Resilience and Complexity: A Bibliometric Review and Prospects for Industrial Ecology. Journal of Industrial Ecology, Special Issue: Advances in Complex Adaptive Systems and Industrial Ecology, 19/2, 236--251 (April 2015) http://dx.doi.org/ 10.1111/jiec.12252
3. Gluchshenko, O.: Definitions of Disturbance, Resilience and Robustness in ATM Context, DLR Report IB 112-2012/28, release 0.07 (2012) http://elib.dlr.de/79571/1/IB-112-2012-28_web_Gluchshenko_0.07.pdf
4. Kim, Y., Chen, Y.-S., Linderman, K.: Supply network disruption and resilience: A network structural perspective. Journal of Operations Management, 33–34, 43--59 (January 2015) http://dx.doi.org/10.1016/j.jom.2014.10.006.
5. Amann, P., James, J.I.: Designing robustness and resilience in digital investigation laboratories, Digital Investigation. 12/1, S111--S120 (March 2015) ISSN 1742-2876, http://dx.doi.org/10.1016/j.diin.2015.01.015.
6. Bankes, S.: Robustness, Adaptivity, and Resiliency Analysis. In AAAI Fall Symposium: Complex Adaptive Systems. (2010) https://www.aaai.org/ocs/index.php/FSS/FSS10/paper/viewFile/2242/2643
7. Haimes, Y.Y.: On the Definition of Resilience in Systems. Risk Analysis 29(4), 49--501 (April 2009). http://dx.doi.org/10.1111/j.1539-6924.2009.01216.x
8. Camarinha-Matos, L.M., Afsarmanesh, H., Ollus, M.: Ecolead And CNO Base Concepts. In: Methods and Tools for Collaborative Networked Organizations, 3--32. Springer US (2008)
9. Zimmermann, H.: OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection. IEEE Transactions on Communications, 28/4, 425—432 (1980). http://dx.doi.org/10.1109/TCOM.1980.1094702
10. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H. E., Havlin, S.:Catastrophic cascade of failures in interdependent networks. Nature. 464/7291, 1025—1028 (2010) http://dx.doi.org/10.1038/nature08932
11. Zio, E., Sansavini, G.: Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins. IEEE Transactions on Reliability. 60/1, 94--101 (2011), http://dx.doi.org/10.1109/TR.2010.2104211
12. Gao, J., Buldyrev, S. V., Stanley, H. E., Havlin, S.: Networks formed from interdependent networks. Nature Physics. 8, 40--48 (2012) http://dx.doi.org/10.1038/nphys2180

13. Albert, R., Jeong, H., Barabási, A.L.: Error and attack tolerance of complex networks. Nature, 406, 378—382 (2000)
14. Watts, D.J.: Six Degrees: The Science of a Connected Age. W. W. Norton & Company, New York – London (2004)
15. Watts, D.J., Strogatz, S.H.: Collective dynamics of 'small-world' networks. Nature, 393, 440--442 (4 June 1998)
http://dx.doi.org/10.1038/30918
16. Kakihara, M., Sørensen, C.: Exploring Knowledge Emergence: From Chaos to Organizational Knowledge. Journal of Global Information Technology Management. 5/3, 48--66 (2002)
http://www.kakihara.org/papers/Kakihara&Sorensen_JGITM.pdf