A Survival Performance Degradation Framework for Large-scale Networked Systems

Ricardo Macedo*, **Yacine Ghamri-Doudane**† **Michele Nogueira***
*NR2 - Federal University of Paraná, Curitiba, Brazil
†L3i - University of La Rochelle, La Rochelle CEDEX 1, France
Email: {rtmacedo, michele}@inf.ufpr.br, yacine.ghamri@univ-lr.fr

Abstract—**Large scale networked systems, such as Identity Management (IdM) systems and software defined networks (SDN), have contributed to technological evolution. They simplify user and network device management. However, they strengthen Distributed Denial- of-Services (DDoS) attacks. These attacks are able to compromise system availability and harm legitimate users. The main approaches against DDoS attacks apply external resources (replication) or try to detect DDoS attacks. The first approach increases solution cost. The second is prone to high false positives. In other contexts, research into resilient approaches has increased for addressing emergent threats. In this work, we advocate that networked systems can self-manage to provide resilience. We propose a framework to guide the system design to follow the ideas defended in this thesis. The framework comprises the survival, collaboration, and analysis modules. Following the framework, networked systems can preserve their lifetime without external computer resources. The DDoS attack mitigation process starts when the system capacity overcomes a pre-established threshold. A protocol and a scheme showcase the framework over IdM systems and SDN. We conducted performance evaluations by experiments and simulations. Results show an increase in throughput and a decrease in latency of essential services when we use the proposed framework.**

I. Introduction

Large scale networked systems, such as Identity Management (IdM) System and Software Defined Networks (SDN), have emerged to improve users account and network services management, promoting the technological evolution. SDN supports dynamic functions of future networks by employing controllers to decouple the control plane from the data plane, simplifying network management to support of the new demands of network traffic [1] [2]. IdM systems controls a large amount of users, separating resources provisioning (a role of **Service Providers - SP**) from the management of user's critical data by employing authentication authorities, named **Identity Providers (IdPs)**, as guardians of users' critical information [3]. SDN and IdM systems improve users account and network services management, contributing to the technological evolution.

Distributed Denial of Service (DDoS) attacks can downgrade or even shutdown IdM systems and SDN essential services [4]. In DDoS attacks, different sources send a huge volume of packets to a target [5]. On the IdM system context, IdPs are available over the Internet and they have limited resources in terms of memory and processing that can become exhausted under DDoS attacks, generating unavailabilities on identification, authentication, attribute provision operations, impacting indirectly in services provisioning [6]. In SDN, an attacker injects a large number of random fake packets into the SDN network forcing SDN switches to ask the SDN controller about how to handle each packet, overloading the controller to serve legitimate users [4], [7].

This work presents the **S**urvival **P**erformance degr**A**dation f**R**amework for ne**T**worked systems in l**A**rge-scale (SPARTA) [8]. SPARTA is the first framework that promotes large-scale networked systems survivability. Following the survivability concept [9], the large-scale networked system is capable to fulfill its mission, in timely manner in the presence of DDoS attacks. To provide this feature, SPARTA employs the collective intelligence principle to learn and incorporate lessons about performance degradation generated by DDoS attacks. The framework considers primary IdP operations, such as identification, authentication and attribute provision, and SDN controller decisions as essential services for addressed the large-scale networked systems, as suggested in the literature [7], [10]. The SPARTA framework comprises *survival*, *collaboration*, and *analysis* modules. The survival module comprises different techniques to attain resistance, recognition, recovery, and adaptation of essential services against performance degradation. The collaboration module promotes interaction among IdPs to share information about the status of the identity federation following the principles of collective intelligence [11]. The analysis module uses shared information to improve the adaptation of essential large-scale networked system services. This differs from solutions in the literature that, in general, ignore DDoS attacks [12] or tolerate a predetermined number of failures [10].

Experimental performance evaluations and simulations using the framework were conducted. A scheme and protocol show case the SPARTA framework. Employing the clustering reorganization concept, a **S**cheme for DDoS **A**ttacks **M**itigation with the re**O**rganization and optimization of the IdM **S**ystem (SAMOS), and a **P**rotocol for DDoS **A**ttack mi**T**igation in **M**ulti contr**O**llers SDN network**S** through controller's clustering (PATMOS) were designed. SAMOS and

978-3-901882-89-0 @2017 IFIP

PATMOS are evaluated over a real testbed and simulations, respectively. Results show SAMOS and PATMOS improving the latency, throughput and the CPU usage rate of IdM systems and SDN essential services.

This paper proceeds as follows. Section II describes the related work. Section III presents the SPARTA framework. Section IV showcases the framework in the scheme SAMOS and its performance evaluation results. Section V showcases the framework in the PATMOS protocol and its performance evaluation results. Finally, Section VI concludes the paper.

II. Related Work

In the last decade, the interest in scalable networked systems has increased. Over time, the advent of the Web and the increasing number of mobile devices has resulted in high demand to provide services and assist users at a large scale. The new context impacted on user account and network management, requiring more complex management and the need to execute these operations as quickly as possible.

In this context, many studies have presented failure-tolerance-based solutions to mitigate the effects of DDoS attacks on IdPs and SDN controllers. These studies employed replicas, *i.e*, many instances of the same service, to respond to requests in case of failures or overload by using external computational resources. *Barreto et al.* presented an intrusion-tolerant IdM infrastructure that uses replication and shared memory [3]. Aiming to mitigate attack effects, Fonseca *et al.* presented a component based on the primary-backup mechanism which offers resilience in case of DDoS attacks against controllers [13]. However, these approaches are designed to tolerate only a predetermined number of failures.

In other contexts, research interests in survivability have increased though the design of adaptable systems and networks to respond to new attacks, failures or accidents. These approaches manage emerging threats, thereby allowing the system or network to learn and to incorporate lessons about the improvement of the resistance, recognition, and recovery of essential services through the adaptation. In [14], *Nogueira et. al* presented an architecture to provide essential ad hoc and mesh networks services survivability during attacks, intrusions and failures by automatically adapting reactive and tolerant mechanisms. In [15], *Deshpande et. al* presented an architecture that provides survivability for systems that comprise *vetronics*, particularly in the military domain, in case of threats and attacks. In [16], *Mehresh et. al* proposed a survival architecture against the manipulation of exchanged data among distributed systems components. However, such approaches are designed following specific requirement contexts that differ from IdM and SDN.

Recently, the collective intelligence concept has emerged as a new perspective to represent an universal kind of intelligence. This has motivated innovative designs for complex and self-organized systems. Pierre Lévy defined collective intelligence as a form of universally-distributed intelligence that can be constantly improved and coordinated in real time and results in effective mobilization skills [11]. By this definition, collective intelligence comprises four main principles, *i.e*, intelligence distribution, improvement, coordination, and mobilization skills. Following this concept, a bio-inspired stochastic scheme for modeling multi-species prey-predator behavior has been proposed [17]. This concept also motivated new research into self-organization in communicating groups [18] and crowdsourcing [19].

Differing from previous solutions, SPARTA improves the performance of IdM operations by considering DDoS attacks. In addition, the SPARTA framework promotes the large-scale networked systems survivability according to the collective intelligence concept to create the interactions among system all components to adapt automatically resistance, recognition, recovery mechanisms in performance degradation situations.

III. A Survival Performance Degradation Framework for Networked Systems in Large scale

SPARTA provides the survivability of essential large-scale networked systems services. SPARTA is a PhD work result [8]. The framework considers as essential services the main IdP operations as: identification, authentication and attribute provisioning, and SDN controllers flow packets decision. Any interruption in such operations negatively impacts services provided to users of networked systems. SPARTA associates techniques and mechanisms with the survival properties of resistance, recognition, and recovery in order to ensure essential services availability against performance degradation.

For providing survivability, SPARTA explores performance degradation effects over associations among entities that compose the large-scale networked system. For example, in identity federations these entities are IdPs, SPs, and EDS. In SDN networks the entities are controllers and switches. Performance degradations over one of these entities impacts the others. For example, when an IdP is exhausted it affects SPs, resulting in delay of user's management operations. A SP exhausted also affects EDSs, occasioning delay to discover SP services. Moreover, performance degradations against an EDS affect SPs, delaying the redirection of users authentications to IdPs. The same effects occur in SDN networks. When a controller is exhausted it affects SDN switches and vice-versa.

SPARTA promotes the collective intelligence, exploring associations among large-scale networked system entities. The collective intelligence consists in a form of universally-distributed intelligence that can be constantly improved and coordinated in real time and results in effective mobilization skills [11]. In order to employ this principle, we define assumptions and requirements. We assume that the collective intelligence of the networked system is distributed among its entities, *i.e*, the IdPs, SPs and EDSs in identity federations and controllers and switches in SDN networks. We define three requirements. First, performance degradation events against these entities must be used to improve the collective intelligence of the large-scale networked system. Second, the communication among entities must be coordinated and preferably in real time. Third, the collective intelligence must promote survivability of the large-scale networked system.

In order to address these requirements, the SPARTA framework comprises three modules: **survival**, **collaboration**, and **analysis**. Figure 1 illustrates the modules and their associations. The survival module comprises different techniques to support the survivability properties of resistance, recognition, recovery and adaptation of essential services against performance degradation. The collaboration module promotes interaction among entities to share information about the status of the large-scale networked system. It follows the principles of cooperation and collective efforts used for decision-making defined by the collective intelligence [11]. The analysis module uses shared information to make decisions in order to improve the adaptation of the essential services.

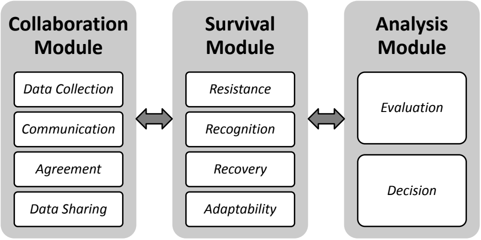

Fig. 1. A Framework for Survivability of Large Scale Networked Systems

Through the coordination among these three modules, the survival module receives updates to promote the large-scale networked system adaptability under the imminence of a performance degradation. By the collaboration module, the survival module receives the networked system status in terms of used resources. The survival module sends this information to the analysis module and receives configuration messages describing an adequate technique to promote the networked system adaptability. Thus, the framework combines the collective intelligence principle and the survivability concepts in order to improve the availability of essential large-scale networked system services.

A. Survival Module

The survival module considers four independent components to express the survival properties of *resistance*, *recognition*, *recovery*, and *adaptability*. These properties support the networked system to repel, detect, evaluate damage, recover features, and incorporate lessons learned by events that result in performance degradation. Each component aggregates particular strategies to achieve its own survival property.

The *resistance* component aggregates preventive mechanisms, such as the firewall employment [20], and graphical puzzles [21], e.g *captcha* mechanisms. This component self-protects and self-adjusts the configuration of mechanisms that protect the large-scale networked system. For example, partial rank correlation techniques [22] and entropy based approaches [23] can detect DDoS attacks through network traffic analysis. By detecting the attack, the component automatically uses the malicious traffic characteristics to insert new rules into the firewall, blocking new attempts.

The *recognition* component uses reactive mechanisms to identify a performance degradation when it is not repelled by the *resistance* component. This component employs, for example, Intrusion Detection Systems (IDS) [24], failure detector services [25] and strategies for monitoring events of memory and processing usage [26]. This component reconfigures such mechanisms to self-adapt themselves against new attacks. This component learns new attacks signatures employing, for example, artificial neural network [27] and fuzzy sets [28] techniques, resulting in IDS reconfiguration. The component can also adjusts failure detection services parameters to better improve the detection accuracy of attacks against essential large-scale networked system services.

The *recovery* component restores essential services of the large-scale networked system. This component aggregates solutions to tolerate failures on essential services [10] and to compose clustering [29]. These solutions restore compromised large-scale networked system essential services based on service replication and service redundancy. Different failure-tolerant strategies can provide replication. For example, the primary-backup, replication schemes and failover services can replicate essential services. The configuration of different parameters must adapt to performance degradation challenges following the intelligence collective principle.

The *adaptation* component self-adjusts mechanisms associate with the *resistance*, *recognition* and *recovery* components. The adaptation component assumes that each entity from the large-scale networked system can witness different situations of performance degradation and they learn different lessons according to such situations. For adjusting such mechanisms, the adaptation considers event correlations for all entities from the networked system. The principle of the collective intelligence is considered to make decisions about performance degradation threats, thereby resulting in adaptation of each mechanism from the survival module. For example, through cooperation of all entities, decisions can be made to change the proposed challenge level of graphical puzzles, replace the failure-tolerance strategy, or firewalls rules and failure detectors services parameters, depending on the large-scale networked system necessities.

B. Collaboration Module

The collaboration module promotes the interaction among entities to share information about the status of the large-scale networked system following the the collective intelligence principle. The *Data collection* component extracts data from all entities regardless performance degradation situations to better adapt the networked system. The *Communication* component defines rules to establish a secure channel to exchange information among entities, e.g. determining the use of the Transport Layer Security (TLS) protocol. The *Agreement* component specifies algorithms to solve consensus issues among entities, employing, for example, the distributed k-means algorithm [30], or the consensus algorithm based on the distributed intelligence technique [31]. The *Data Sharing* component is responsible to exchange encrypted messages among the networked system entities. This component uses, for example, the secret key cryptography and hash functions to encrypt messages send them through Web Services [32].

C. Analysis Module

The module uses collected data to accurately determinate the best way to improve the large-scale networked system survivability. The *Evaluation* component has access to all collected data about the performance degradation events experienced by all entities. Moreover, data analysis provides information about the state of the networked system as a whole. Using this information, the *decision* component employs strategies previously used by other entities and coordinates actions to provide the survivability of the networked system essential services.

IV. DDoS Attacks Mitigation Through IdM System Re-organization and Optimization

To showcase our framework on the IdM System domain, we use the SAMOS scheme [33], [34], [35]. As discussed in Section III, the proposed SPARTA framework is composed of the *survival*, *collaboration* and *analyses* modules. The *resistance*, *recognition*, *recovery* and *adaptability* components are reflected in the SAMOS. This scheme is designed to act in scenarios where attackers overcome protective techniques against DDoS described by the *resistance* module. The SAMOS scheme is initiated by alerts generated by traditional resources monitoring techniques presented in the *recognition* module. SAMOS reorganizes IdP clustering, similar to techniques specified in the *recovery* component. This reorganization is performed by analyzing the data collected from all IdPs from the IdM system, as suggests the *adaptability* component.

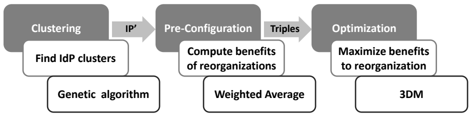

Fig. 2. SAMOS Steps

The components of the SPARTA framework *collaboration* module are also instantiated in the SAMOS scheme. Monitoring data collected from IdP memory and processing usage comprise the *data collect* component. The set of rules that IdPs must to follow in order to exchange these data comprises the *communication* component. Similarly, components from the *analysis* module in the SPARTA framework also are present in the SAMOS scheme. The collected monitoring data from IdPs memory and processing describe the IdM system as a whole. These data are input to the *evaluation* component. Optimization techniques employed to reorganize IdP clustering configurations in the SAMOS scheme contemplate the *decision* component of the SPARTA framework.

Figure 2 illustrates three steps of SAMOS: *Clustering*, *Pre-configuration*, and *Optimization*. *Clustering* identifies the maximum number of IdP clusters to mitigate the overload generated by a DDoS attack using a genetic algorithm. *Pre-configuration* computes all possible associations to reorganize the system by assigning a benefit to each association. *Optimization* employs optimization techniques to find a solution with the maximum benefit to reorganize the system.

A. SAMOS Performance Evaluation

Employing the framework reorganization concept, we developed the *MoniOptimize* tool [36]. The *MoniOptimize* tool performance evaluation is conducted over *CAFe Expresso*, a real testbed from the Brazilian identity federation. Six scenarios are building combining authentication and DoS attack workloads simultaneously. The first scenario evaluates the IdP behavior without our solution, comprehending the classical approach, those we named shortly as *classical*. In the second scenario the *MoniOptimize* tool acts identifying a cluster with two IdPs, we reference this scenario as *MO-2M*. In the third one, our tool acts clustering three IdPs (referenced as *MO-3M*). The others scenarios are build with 4, 5, and 6 IdPs in the cluster and received names following the same logical sequence.

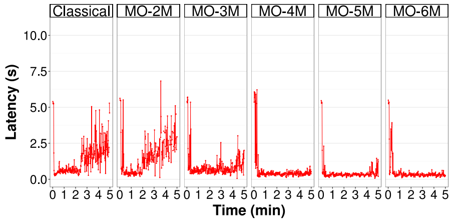

Fig. 3. Latency under DDoS attack and Authentication Workloads

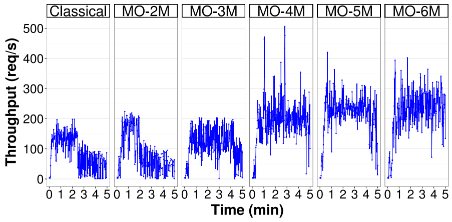

Fig. 4. Throughput under DDoS attack and Authentication Workloads

Figure 3 and 4 illustrates the *MoniOptimize* tool decreasing the latency and increasing the throughput of requests to the target IdP. The average latency is 1.33 seconds in in the *classical* scenario, increasing to 1.47 seconds in the *MO-2M* scenario and reaching 0.77 seconds in the *MO-3M* scenario. Results are improved adding more members into the IdP cluster. In *MO-6M* scenario, the average latency decreases to 0.4 seconds. The average throughput is 91.84 req/s in the *classical* scenario, increasing to 113.4 req/s in the *MO-3M* scenario, reaching 191.67 req/s in the *MO-4M* scenario. Using more IdPs in the cluster the results improves even more. In *MO-6M* scenario the average throughput increases to 220.7 req/s. These results show that the *MoniOptimize* tool reaches better results using IdP clusters with more IdPs.

V. Mitigating DDoS Attacks in SDN Controllers Through Reorganizations

In order to showcase our framework over the SDN domain we use the PATMOS protocol [37]. PATMOS defines a set of procedures to mitigate the DDoS attacks effects against SDN controllers. These procedures are organized into three phases: *Finding bottlenecks*, *Election* and *Composition*. The *Finding bottlenecks* phase identifies the controllers that are overloaded by the attack. The *Election* phase chooses a leader to coordinate the clustering process. Finally, in the *Composition* phase controllers are clustered to mitigate the attack effects. Fig. 5 illustrates PATMOS phases.

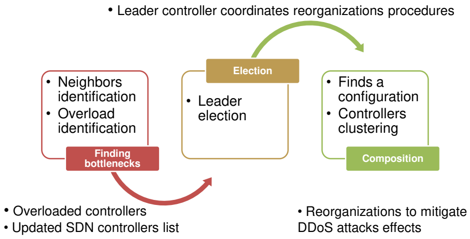
• Leader controller coordinates reorganizations procedures
• Neighbors identification
• Overload identification
Finding bottlenecks
Election
• Leader election
• Finds a configuration
• Controllers clustering
Composition
• Overloaded controllers
• Updated SDN controllers list
• Reorganizations to mitigate DDoS attacks effects

Fig. 5. Phases of PATMOS Protocol

Controllers play different roles and show different status in these phases. In the *Finding bottlenecks* phase, controllers play *ordinary* role under *normal* status to exchange control messages in order to identify controllers under *overloaded* status. In the *Election* phase controllers can perform *candidacy*, *leader*, *vice-leader* (VL) and *elite* roles. A *candidacy* votes to choose a leader with the better performance level. *Leader* is the better performance level controller. VL is the second best performance level controller to become leader if the current leader becomes a target of DDoS attacks. *Elite* controllers are the k higher performance level controllers, acting as a coordinator advisory group (CAG) members to elect a new VL if the leader becomes DDoS attacks target. In the *Composition* phase, the *leader* searches for the best cluster configuration to mitigate the attack effects. Controllers chosen by the *leader* to compose clusters play the *worker* role to process flow requests received from the overloaded controllers.

A. PATMOS Performance Evaluation

The simulations are conducted considering a SDN network with five controllers working collaboratively to compose a multi-controller SDN network represented through the SDN network simulator Mininet. Five scenarios are built, where the first one evaluates the controller behavior without PATMOS, serving as a base line, those we named shortly as *Classical*. In the second scenario PATMOS acts identifying a cluster with two controllers, we reference this scenario as *Patmos-2C*. In the third one, PATMOS identifies three controllers (referenced as *Patmos-3C*). The others scenarios are build with four and five controllers in the cluster and received names following the same logical sequence. In all the scenarios, the controller $C5$ is the target of the overload. Malicious and legitimate workloads are combined to evaluate PATMOS. The malicious one originated from a DDoS attack using 9 switches, 64 hosts, where 29 hosts attacking during 12 seconds, such as [7] and a legitimate one generated by the *cbench* benchmark tool using 16 switches, and 1000 hosts. Our simulations are performed focusing on latency and throughput.

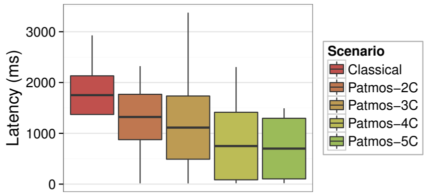

Fig. 6. Latency under DDoS attack and Benchmark Workloads

Figs 6 and 7 show PATMOS increasing the throughput and decreasing the latency of requests to the target controller. The mean of throughput is 23 req/s in the *Classical* scenario, increasing to 1735.41 in the *Patmos-2C* scenario, reaching 2435.89 req/s in the *Patmos-3C* scenario, and 4642.911 in the *Patmos-4C* scenario. In the *Patmos-5C* scenario the mean of throughput increased to 4433.160 req/s. The mean of latency is 1751.53 ms in the *Classical* scenario, decreasing to 1321.8203 ms in the *Patmos-2C* scenario, and reaching 1112.88 ms in the *Patmos-3C* scenario, and 749.7530 ms in the *Patmos-4C* scenario. In the *Patmos-5C* scenario the mean of latency decreased to 699.59 ms. These results show PATMOS reaching better results using more controllers in the cluster.

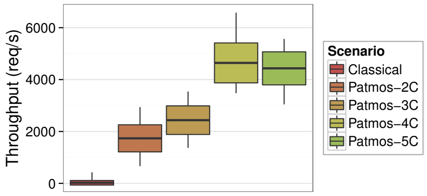

Fig. 7. Throughput under DDoS attack and Benchmark Workloads

VI. Conclusion

This paper presented the SPARTA framework for the survivability of the essential large-scale networked systems services under DDoS attacks. In order to showcase the proposed framework, we instantiated it under the IdM system domain through the SAMOS scheme and under the SDN field by the PATMOS protocol. We performance evaluations using a simulated SDN network and *CAFe Expresso*, a real testbed from the Brazilian identity federation. Results show the improvement of the networked systems, increasing the throughput and decreasing the latency of its essential services.

References

[1] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on Software-Defined Networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 27–51, 2015.

[2] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.

[3] L. Barreto, F. Siqueira, J. Fraga, and E. Feitosa, "An Intrusion Tolerant Identity Management Infrastructure for Cloud Computing Services," in *IEEE International Conference on Web Services*, 2013, pp. 155–162.

[4] N.-N. Dao, J. Park, M. Park, and S. Cho, "A Feasible Method to Combat Against DDoS Attack in SDN Network," in *International Conference on Information Networking*, 2015, pp. 309–311.

[5] A. Alsumayt and J. Haggerty, "A Survey of the Mitigation Methods against DoS Attacks on MANETs," in *Science and Information Conference*, Aug 2014, pp. 538–544.

[6] A. Lonea, H. Tianfield, and D. Popescu, "Identity management for cloud computing," in *New Concepts and Applications in Soft Computing*, ser. Studies in Computational Intelligence, V. E. Balas, J. Fodor, and A. R. Várkonyi-Kóczy, Eds. Springer Berlin Heidelberg, 2013, vol. 417, pp. 175–199.

[7] S. M. Mousavi and M. St-Hilaire, "Early Detection of DDoS Attacks Against SDN Controllers," in *International Conference on Computing, Networking and Communications*, Feb 2015, pp. 77–81.

[8] R. Macedo, "Um arcabouço para resiliência de sistemas em rede por conformação de agrupamentos *(In Portuguese)*," Ph.D. dissertation, Federal University of Paraná, http://www.nr2.ufpr.br/ ricardo/Docs/2016-Tese-Macedo-Final.pdf, 7 2016, curitiba, PR, Brazil.

[9] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, and T. Longstaff, "Survivable Network Systems: An Emerging Discipline," DTIC Document, Tech. Rep., 1997.

[10] D. Kreutz, E. Feitosa, H. Cunha, H. Niedermayer, and H. Kinkelin, "Increasing the Resilience and Trustworthiness of OpenID Identity Providers for Future Networks and Services," in *International Conference on Availability, Reliability and Security*, Sept, 2014, pp. 317–324.

[11] P. Levy, *Collective Intelligence: Mankind's Emerging World in Cyberspace*. Cambridge, MA, USA: Perseus Books, 1997.

[12] K. Chard, M. Lidman, B. McCollam, J. Bryan, R. Ananthakrishnan, S. Tuecke, and I. Foster, "Globus Nexus: A Platform-as-a-Service provider of research identity, profile, and group management," *Future Generation Computer Systems*, vol. 56, pp. 571 – 583, 2016.

[13] P. Fonseca, R. Bennesby, E. Mota, and A. Passito, "A Replication Component for Resilient OpenFlow-based Networking," in *IEEE Network Operations and Management Symposium*, April 2012, pp. 933–939.

[14] M. Nogueira, H. Silva, A. Santos, and G. Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 156–168, 2012.

[15] A. Deshpande, O. Obi, E. Stipidis, and P. Charchalakis, "Integrated vetronics survivability: Architectural design and framework study for vetronics survivability strategies," *Computer Standards & Interfaces*, vol. 39, pp. 1 – 11, 2015.

[16] R. Mehresh and S. Upadhyaya, "Surviving advanced persistent threats in a distributed environment – Architecture and analysis," *Information Systems Frontiers*, vol. 17, no. 5, pp. 987–995, 2015.

[17] K. Hassani, A. Asgari, and W. S. Lee, "A Case Study on Collective Intelligence Based on Energy Flow," in *IEEE International Conference on Evolving and Adaptive Intelligent Systems*, Dec 2015, pp. 1–7.

[18] F. Heylighen, *Self-organization in Communicating Groups: The Emergence of Coordination, Shared References and Collective Intelligence*, 2013, pp. 117–149.

[19] G.-J. Qi, C. C. Aggarwal, J. Han, and T. Huang, "Mining Collective Intelligence in Diverse Groups," in *Proceedings of the 22Nd International Conference on World Wide Web*. New York, NY, USA: ACM, 2013, pp. 1041–1052.

[20] F. Guenane, M. Nogueira, and G. Pujolle, "Reducing DDoS Attacks Impact Using a Hybrid Cloud-based Firewalling Architecture," in *Global Information Infrastructure and Networking Symposium*, Sept 2014, pp. 1–6.

[21] K. Singh and T. De, "DDoS Attack Detection and Mitigation Technique Based on Http Count and Verification Using CAPTCHA," in *International Conference on Computational Intelligence and Networks*, Jan 2015, pp. 196–197.

[22] M. H. Bhuyan, A. Kalwar, A. Goswami, D. K. Bhattacharyya, and J. K. Kalita, "Low-Rate and High-Rate Distributed DoS Attack Detection Using Partial Rank Correlation," in *IEEE International Conference on Communication Systems and Network Technologies*, April 2015, pp. 706–710.

[23] X. Qin, T. Xu, and C. Wang, "DDoS Attack Detection Using Flow Entropy and Clustering Technique," in *IEEE International Conference on Computational Intelligence and Security*, Dec 2015, pp. 412–415.

[24] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266 – 2279, 2013, towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet.

[25] R. Turchetti and E. Procopio Duarte, "Implementation of Failure Detector Based on Network Function Virtualization," in *IEEE International Conference on Dependable Systems and Networks Workshops*, June 2015, pp. 19–25.

[26] L. Baumgärtner, C. Strack, B. Bastian Hoßbach, M. Seidemann, B. Seeger, and B. Freisleben, "Complex Event Processing for Reactive Security Monitoring in Virtualized Computer Systems," in *ACM International Conference on Distributed Event-Based Systems*. New York, NY, USA: ACM, 2015.

[27] E. Hodo, X. Bellekens, A. Hamilton, P. L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System," in *International Symposium on Networks, Computers and Communications*, May 2016, pp. 1–6.

[28] R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness Based Semi-Supervised Learning Approach for Intrusion Detection System," *Information Sciences*, vol. 378, pp. 484 – 497, 2017.

[29] "Clustering - identity provider version 3," https://wiki.shibboleth.net/confluence/display/IDP30/Clustering, last access: Aug. 2015.

[30] Q. Liu, W. Fu, J. Qin, W. X. Zheng, and H. Gao, "Distributed K-means Algorithm for Sensor Networks Based on Multi-Agent Consensus Theory," in *IEEE International Conference on Industrial Technology*, March 2016, pp. 2114–2119.

[31] K. Utkarsh, A. Trivedi, D. Srinivasan, and T. Reindl, "A Consensus-based Distributed Computational Intelligence Technique for Real-Time Optimal Control in Smart Distribution Grids," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. PP, no. 99, pp. 1–1, 2016.

[32] M. S. Das, A. Govardhan, and D. V. lakshmi, "QoS Web Service Security Access Control Case Study Using HTTP Secured Socket Layer Approach," in *Proceedings of the The International Conference on Engineering & MIS 2015*. ACM, 2015, pp. 59:1–59:9.

[33] R. Macedo, A. Santos, Y. Ghamri-Doudane, and M. Nogueira, "A Scheme for DDoS Attacks Mitigation in IdM Systems Through Reorganizations," in *IEEE/IFIP Network Operations and Management Symposium*, 2016.

[34] ——, "Guard Mounting: Reorganizations to Mitigate DDoS Attacks over Identity Providers Clustering," in *Workshop on Wireless of the Students, by the Students, and for the Students*, 2015, pp. 28–30.

[35] R. Macedo, Y. Ghamri-Doudane, and M. Nogueira, "Mitigating DoS Attacks in Identity Management Systems Through Reorganizations," *Latin American Network Operations and Management Symposium*, 2015.

[36] R. Macedo, L. Melniski, A. Santos, E. Feitosa, and M. Nogueira, "MoniOptimiza: Uma Ferramenta para Monitoramento e Otimização de Federações de Identidades *(In Portuguese)*," *Workshop de Gestão de Identidades Digitais (alocado com o SBSEG 2015)*, 2015.

[37] R. T. Macedo, R. Castro, A. Santos, Y. Ghamri-Doudane, and M. Nogueira, "Self-Organized SDN Controller Cluster Conformations Against DDoS Attacks Effects," *IEEE GLOBECOM*, 2016.