Sample Average Approximation Approach for Solving a Class of Two-Stage Stochastic Integer Programs

Fatma Syarah, Togi, Herman Mawengkang

Abstract:Two-stage stochastic integer programming problems arise in many practical sit-uations, such as production and manpower planning, portfolio selections and so on. In general, the deterministic equivalences of these problems can be very large, and may not be solvable directly by general-purpose optimization approaches. Sample average approximation is an approach for solving chance constrained programming is adopted. After using scenario analysis technique, a direct search approach based on reduced gradient method is used for solving the deterministic model which would be a nonlinear integer program.

I.INTRODUCTION

In the two-stage stochastic programming approach for optimization under uncertainty, the decision variables are partitioned into two sets. The *first stage* variables are those that have to be decided before the actual realization of the uncertain parameters becomes available. Subsequently, once the random events have presented themselves, further design or operational policy improvements can be made by selecting, at a certain cost, the values of the *second stage* or *recourse* variables. The objective is to choose the first stage variables in a way that the sum of first stage costs and the expected value of the random second stage or recourse costs is minimized.

A standard formulation of the two-stage stochastic program is

$$\min_{x\in X}\left\{g(x) := c^T x + E[Q(x,\xi(\omega))]\right\} \tag{1}$$

Where

$$Q(x,\omega) := \inf_{y\in Y}\left\{q^T y : Wy \geq h - Tx\right\} \tag{2}$$

For governments, large enterprises, individuals, small businesses, and other parties participating in modern society, one of the major concerns is the aspect of stochastic integer programs. With cyber attacks and criminals complicating the nature of this field via sophisticated approaches, it is apparent that the need for a deeper focus on stochastic integer programs' risk management cannot be overemphasized [1]. Whereas investments in perimeter defences have increased, internal threats emerging from third parties such as vendors and contractors and even company employees add to security incidents[2]. Major approaches that have been advocated in a quest to reverse this trend include solid employee training in relation to stochastic integer programs and embracing a close management and monitoring of third parties that include contractors and vendors, poised to curb enterprise level security breaches [3], This paper formulates a stochastic integer programs risk management strategy.

Revised Manuscript Received on December 22, 2018.

Fatma Syarah,University Negeri Medan/Graduate School of Math., University of Sumatera Utara, Indonesia

Togi, Department of mathematics, University of Sumatera Utara,Indonesia

Herman Mawengkang, University of Sumatera Utara,Indonesia

II. THE SAMPLE AVERAGE APPROXIMATION METHOD

The obtained sample average approximation is expressed as

$$\min_{x\in X}\left\{\hat{g}_N(x) := c^T x + N^{-1}\sum_{n=1}^{N} Q(x,\xi^n)\right\} \tag{3}$$

of the stochastic program (1), which is then solved by a deterministic optimization algorithm.

Also, the sample average function is $N^{-1}\sum_{n=1}^{N} Q(x,\xi^n)$.

The plan is grounded in security prioritization and, operational and thought leadership. The main aim is to harmonize risk management language, methodologies, and technologies across the selected enterprise. In addition, the plan seeks to improve the company's visibility into its stochastic integer programs risk landscape via the identification of strengths and opportunities for improvement. By steering a better-informed risk tolerance culture, the aim of the plan is to identify potential security solutions, develop operational and capital expenditures, and better set stochastic integer programs priorities at the company.

One of the areas of focus will be the people. Specifically, company employees will receive regular training and briefings to gain an awareness of company security escalation paths and resources. This provision of staff awareness pipeline is deemed important because they are expected to be in charge of strategy implementation towards assuring stochastic integer programs. Another area

of focus concerns the process. To achieve risk-informed procedures and processes, the strategy seeks to ensure that the target firm actively adapts to sophisticated and evolving threats, a changing stochastic integer programs landscape, and predictive indicators to assure preparedness for future uncertainties. In addition, focusing on the process of strategy implementation will aid in ensuring that the company responds to events in a timely manner. The third area of focus will concern the technology. Specifically, the strategy seeks to ensure that the tools deployed in the company and industry's environment are reviewed regularly for coverage against changes in internal ecosystems and the threat environment. Indeed, the focus on technology is informed by the need for the strategy to ensure that the company's tools deployed anticipate any emergent threats. The last area of focus concerns the ecosystem, constituting third parties and other industry players. Indeed, the strategy seeks to advocate for the organization's success in risk management and active sharing of data with partners in a quest to ensure that the current and accurate information leads to improved ecosystem stochastic integer programs prior to the occurrence of events. In summary, major components of the strategy include the ecosystem, technology, process, and the people (company employees). From the perspective of compliance, the strategy will ensure that the target groups' right to privacy (such as company employees and third-party vendors and contractors) is not contravened.

III. CONVERGENCE ANALYSIS

The central approach adopted is the qualitative stochastic integer programs risk assessment. According to Goolsby (2013)[4], this method implies that the subjective qualities associated with the respective risks are used as key predictors and aid in indicating merit in relation to other or related risks. As affirmed by Liff (2012)[5], one of the alternatives is to assess risks as high, medium, or low. Therefore, this methodology is informed by the probability that a risk is likely to occur. The approach also centers on the probability that the perceived impact is likely to pose on the targeted firm. Therefore, this plan seeks to categorize risks based on their source and the effect or vulnerabilities that they are likely to have on the enterprise, as well as the organization's stakeholders. From the context of stochastic integer programs, the adoption of a qualitative methodology in the current plan implies that focus will be on the discovery and review of the company's assets (such as human resources, processes, software, and hardware) to establish known weaknesses against potential vulnerabilities' databases. By measuring the respective risks against relative scales, the plan seeks to determine the probability that the perceived threats could exploit a system's vulnerability. Indeed, this method (qualitative methodology of identifying and evaluating stochastic integer programs risks in systems) has been selected because it is not only less expensive and faster but also enables companies to streamline their timetables while minimizing the respective budgets [6].

A. Discrete First Stage

We begin by briefly reviewing results in (13) on the convergence of the SAA method when applied to stochastic programs with a finite set of first-stage decisions.

Let us consider instances of two-stage stochastic programs (1) with the following characteristics:

(i) The set of first-stage decisions X is finite (but maybe very large).

(ii) The recourse function $Q(x,.)$ is measurable and $E|Q(x,\xi(\omega))\}$ is finite for every $x \in X$

In situations where the stochastic integer programs risks are low, it has been documented that it is very difficult to circumvent or pass through the device or control and the system requires experienced experts or very high skill levels. In addition, low risks imply that little or no sensitive data is lost or leaked and poses very little impact on system users and company critical infrastructure. Thus, low risks are marked by an existence of log management and related controls responsible for reporting, blocking, and detecting intrusion with ease[7]. In situations where risks are deemed by the qualitative approach as moderate, the attacker could circumvent or pass through the system successfully only in the existence of certain conditions, requiring moderate skill. In such a case, full breach is improbable and sections of system users or critical infrastructure may be affected, depicting the presence of insufficient log management and related controls responsible for the detection and blockage of intrusions [8]. Lastly, high risks imply that the attackers not only circumvent or pass through the device or control successfully but also require little skill and are likely to gain full access to critical infrastructure and operate the system users' accounts, depicting probable breach. As observed by Tabor (2013)[9], high stochastic integer programs risks depict an absence of adequate detection controls.

$$1-P\left(\hat{X}_N^{\delta} \subset X^{\varepsilon}\right) \leq |X\}e^{-N\gamma(\delta,\varepsilon)} \tag{4}$$

$$\gamma(\delta,\varepsilon) \geq \frac{(\varepsilon^{*}-\delta)^2}{3\sigma^2} \geq \frac{(\varepsilon-\delta)^2}{3\sigma^2} \tag{5}$$

where $\varepsilon^{*} := \min_{x \in X|X^{eg}} g(x) - v^{*} \operatorname{dan} \sigma^2$ is the maximal variance of certain differences between values of the objective function of the SAA problem Internal attacks form the major source of threat in many systems. Specifically, the analysis establishes that rogue employees accessing the administrators' accounts, sensitive data, or networks could cause real damage, rated at the medium risk rating and priority rating, with the impact and likelihood of occurrence standing at 3. Regarding the compromise of corporate services, it is established that the damage is likely to stretch beyond the loss of the ability to run daily functions within the stock inventory-systems and the online store. With the risk rating and priority rating suggesting that this destabilization of corporate services could yield medium-level damage, additional adversities. For example, a compromise to a company's corporate services is projected to yield substantial financial losses

accruing due to the loss of corporate data and the loss of contract or business. Financial loss is also projected to face organizations due to disrupted trading (such as stalled progress in online transactions), loss of money, and a loss of financial data; such as payment card details and bank details. Indeed, the latter adversities are not only likely to arise due to compromised corporate services but also as a result of unauthorized access and even data misuse by authorized employees, especially those who access company sensitive information and exhibit malicious intentions.

$$N \geq \frac{3\delta^2}{(\varepsilon-\delta)^2}\log\left(\frac{|X|}{\alpha}\right) \tag{6}$$

Additional costs are also projected to be incurred by firms towards repairing the affected devices, networks, and systems, should the aforementioned stochastic integer programs threats be implemented while targeting the respective systems and company functions. Apart from the financial loss, another risk that VG Trading Company faces entails reputational damage. According to Walker and Conway (2015)[10], trust forms an essential element steering company customer relationships. Therefore, the selected company's cyber attacks accruing from the misuse of sensitive information by sections of its employees could damage the reputation of the organization and even erode the trust of current and future customers. From this risk of reputational damage, specific adversities are predicted to include reduction in profits, loss of sales, and loss of customers. Similarly, the risk of reputational damage arising from the leakage of customer information is likely to stretch beyond the affected customer bases to impact on suppliers, compromising the company's relationship with investors and partners, as well as third parties vested in firms.

B. Continuous First Stage

Should cyber insecurity events occur, it is projected that hidden costs are likely to amount to about 90 percent of the organization's total business impact but these results are likely to emerge about two or more years after the occurrence. Well-known and surface cyber incident costs are expected to include technical investigations, stochastic integer programs improvement costs, attorney fees and litigation, crises or public relations communications, regulatory compliance or fines, post-breach customer protection, and customer breach notifications. On the other hand, an occurrence of a stochastic integer programs event is likely to prompt less visible, hidden, or below the surface costs such as the loss of intellectual property, devaluation of the trade name, costs related to the value of lost contract revenue, lost value of customer relationships, operational disruption, increased cost to raise debt, and insurance premium increases. Imperative to highlight is that operational disruption forms a major business impact that the threats are likely to cause, translating into economic costs. The following table indicates specific costs of impacts, should a breach such as a loss of customer information occur.

$$N \geq \frac{3\delta^2}{(\varepsilon'-\delta)^2}\left(n_1\log\frac{D}{v}-\log\alpha\right) \tag{7}$$

$$N \geq \frac{12\delta^2}{(\varepsilon-\delta)^2}\left(n_1\log\frac{2DL}{\varepsilon-\delta}-\log\alpha\right) \tag{8}$$

From the above business impact analysis, it is evident that the "below the surface costs" of the breach outperform the "surface costs" accruing from a stochastic integer programs event such as that which involves the leakage of sensitive customer data. From the qualitative perspective, the two dominant issues likely to accrue include the loss of customers and the loss of reputation.

C. Continuous First Stage and Discrete Distribution

$$\min_{x\in X}\left\{g(x) := c^T x + \sum_{k=1}^{K} p_k Q(x,\xi_k)\right\} \tag{9}$$

here

$$Q(x,\xi_k) := \inf_{y\in Y}\left\{q_k^T y : Wy \geq h_k - T_k x\right\} \tag{10}$$

In situations where data breaches are reported, companies have struggled to recover from cyber-attacks and, in the processes, lost millions of dollars. Damaged reputations are also seen to be exacerbated by increasing volumes of cyber breaches [3].The development of a response strategy is important and the need to integrate it into the business continuity program of the firm is informed by the need to respond with well-coordinated plans, should events occur. Indeed, it has been documented that through business continuity plans, organizations tend to reduce the mean-time required to address data breaches to a significant extent, seeking further to reduce possibilities of the recurrence of such events in future[4]. It has been established further that through well-defined business continuity plans, companies cut costs associated with data breaches, having kept business operations up and running.

$$\mathsf{C}(z,\xi) := \left\{x \in \mathbb{R}^{n_1} : h - z - 1 \leq Tx < h - z\right\} \tag{11}$$

where the notation "$\leq$" and "$<$"is understood to be applied componentwise. It follows then that for any $z \in \mathbb{Z}^{m_2}$ the function $\sum_{k=1}^{K} p_k Q(\cdot,\xi_k)$ is constant over the set $\mathsf{C}(z) := \cap_{k=1}^{K}\mathsf{C}(z,\xi_k)$ Note that $\mathsf{C}(z)$ is a neither open nor closed polyhedral region. Now let

$$\mathsf{Z} := \left\{z \in \mathbb{Z}^{m_2} : \mathsf{C}(z) \cap X \neq \varnothing\right\}$$

Let us define

$$V := \bigcup_{z\in Z} \mathrm{vert}(\mathsf{C}(z) \cap X) \tag{12}$$

One of the recommended strategies entails the

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

employment of a cloud-based business continuity program. According to Liff (2012), cloud services ensure that the critical applications and data of organizations are

secure off-site on the servers of the cloud service providers. In future, it is recommended that firms embrace cloud-based business continuity programs due to the capacity of the latter to enable the organization to leverage lower specification systems. In case of a disaster, it has been avowed that the use of the cloud enables firms to ramp up their systems in a quick manner (Reddy & Reddy 2014). The provision of pay-as-you-use model in cloud-based services implies that the firm's decision to employ these services will lead to significant reductions in the cost of cloud-based BC/DR when compared to situations where the firm embraces data storage and redundant hardware hosted in remote facilities. According to Sabrine, Muriel and Stéphane (2015)[8], the current age holds that when a company experiences a few minutes off down time, revenue loss is likely to accrue in terms of hundreds of thousands of dollars. Therefore, cloud-based services as part of the business continuity plan are projected to assure an interruption-free data flow following adversities such as data breaches, translating into assured maximum productivity.

$$\min_{x\in V}\left\{ g(x) = c^T x + \sum_{k=1}^{K} p_k Q(x,\xi_k) \right\} \tag{13}$$

It was proposed in (28) to solve (13) by enumerating the finite set *V.*

$$cl(\mathsf{C}(z)) = \left\{ x \in \mathbb{R}^{n_1} : x \geq 0, T_x \leq h^k - z, T_x \geq h^k - z - 1, \forall k \right\}$$
$$= \left\{ x \in \mathbb{R}^{n_1} : x \geq 0, T_x \leq \underline{h} - z, T_x \geq \bar{h} - z - 1 \right\}$$

where $h = \min_k \{h^k\}$ and $\bar{h} = \max_k \{h^k\}$ and the max and min operations are component-wise. Assuming that $X = \left\{ x \in \mathbb{R}^{n_1} : Ax \leq b, x \geq 0 \right\}$, where *A* is an $m_1 \times n_1$ matrix, we have that for any $z \in Z$

$$(\mathsf{C}(z)) \cap X = \left\{ x \in \mathbb{R}^{n_1} : Ax \leq b, x \geq 0, T_x \leq \underline{h} - z, T_x \geq \bar{h} - z - 1 \right\}$$

The above system is defined by at most $n_1 + m_1 + 2m_2$ linear inequalities (including non-negativity), and thus has at most

$$\binom{n_1 + m_1 + 2m_2}{n_1} < (n_1 + m_1 + 2m_2)^{m_1 + 2m_2}$$

extreme points. We thus have the following upper bound on the cardinality of *V*

$$|V| < [K(D+1)]^{m_2} (n_1 + m_1 + 2m_2)^{m_1 + 2m_2} \tag{14}$$

The crisis and emergency management teams ought to be well prepared to handle stochastic integer programs disruptions such as IT systems failure and data breaches. From the perspective of crisis communication, it is recommended that emergency notifications are relayed to the intended audiences via mobile and related channels, targeting stakeholders and the employees. Indeed, the crisis communication as a leadership strategy should seek to direct the target groups regarding the required follow up actions. Therefore, there is a need to establish a crisis team to aid in control platforms such as social media sites in a quest to curb reputational impacts that the adversities could pose, should stochastic integer programs events be detected or reported. It is further notable that the formulation of a crisis team should strive to embrace business impact analysis as part of the post-event recovery to assure the restoration of operations. By establishing a crisis team, it is predicted that systems' perceived experience of cyber-attacks will be marked by the capacity to assure business continuity due to the capacity of this team to identify the most critical assets (applications or functions) and engage in the evaluation of the impact posed by a cyber-related disaster to business operations. The crisis team will also aid in the analysis of the impact of the disaster across dimensions such as upstream and downstream process impact, employee impact, third-party impact, and financial stability, aiding in recommending targeted corrective measures that seek to restore the brand image and company reputation. Imperative to note is that the crisis team needs to exhibit detailed work-around to assure access to critical applications, should a cyber disaster or incident occur. Through crisis team training, it is projected that organizations will be marked by proactive incident response.

$$\min_{x\in V_n}\left\{ \hat{g}_{N(x)} = c^T x + \frac{1}{N}\sum_{n=1}^{N} Q(x,\xi^n) \right\} \tag{15}$$

where *VN* is the sample counterpart of the set *V* . That is

$$V_n := \cup_{z\in Z_N} \mathrm{vert}(\mathsf{C}_N(z) \cap X) \tag{16}$$

$$1 - P\left(\hat{X}_N^{\delta} \subset X^{\varepsilon} \right) \leq |V| e^{-N\gamma(\delta,\varepsilon)} \tag{17}$$

$$N \geq \frac{3\delta^2}{(\varepsilon-\delta)^2}(m_2 \log[K(D+1)]) + (m_1 + 2m_2)(n_1 + m_1 + 2m_2) - \log\alpha) \tag{18}$$

IV.SOLVING THE SAA PROBLEM

On the one hand, it has been established that sections of employees could pose stochastic integer programs threats due to malice and misuse of data [9]. On the other hand, it has been documented that all employees have a role to play in ensuring that they are part of the post-attack process and business recovery [10]. According to Walker and

Conway (2015)[11], the period following a cyber attack demands that it is not just the IT team but all departments participate in training regarding the manner in which they ought to communicate with the respective

clients. Similarly, effective employee training towards business continuity following cyber attacks has been asserted to be characterized by adequate preparation to work with legal teams towards addressing the cyber attacks' repercussions. Hence, it is recommended that an effective cyber response plan seeking to assure business continuity is customized to the firm's preferences and needs, ensuring that the employees' specific roles in its stochastic integer programs are identified and appropriate training effected based on the resultant roles. The need for business continuity demands further that the employees are trained on safe Internet practices and emailing after a crisis to assure recovery from breaches.

V.Initialization:

Preprocess the problem by constructing a hyper-rectangle of the form $\mathcal{P}^0 := \prod_{j=1}^{m_1}\left[l_j^0, u_j^0\right)$ such that $\chi \subset \mathcal{P}^0$. Add the problem

$$\text{Min } \hat{G}_N(\chi) \text{ subject to } \chi \in \mathcal{X} \cap \mathcal{P}^0$$

to a list L of open subproblems. Set $U \leftarrow +\infty$ and the iteration counter $i \leftarrow 0$.

A.Iteration *i*:

Step *i*.1: If $\mathcal{L} = \emptyset$, terminate with solution χ^*, otherwise select a sub-problem *i*, defined as

$$\text{Min } \hat{G}_N(\chi) \text{ subject to } \chi \in \mathcal{X} \cap \mathcal{P}^i,$$

from the list L of currently open subproblems. Set L ← L \ {*i*}.

Step *i*.2: Obtain a lower bound β^i satisfying

$$\beta^i \le \inf\{\hat{G}_N(\chi) : \chi \in \mathcal{X} \cap \mathcal{P}^i\}.$$

If $\mathcal{X} \cap \mathcal{P}^i = \emptyset$, $\beta^i = +\infty$ by convention. Determine a feasible solution $\chi^i \in \mathcal{X}$ and compute an upper bound $\alpha^i \ge \min\{\hat{G}_N(\chi) : \chi \in \mathcal{X}\}$ by setting $\alpha^i = \hat{G}_N\left(\mathcal{X}^i\right)$.

Step *i*.2.a: Set $L \leftarrow \min_{l \in L \cup \{i\}} \beta^l$.

Step *i*.2.b: If $\alpha^i < U$, then $\chi^* \leftarrow \chi^i$ and $U \leftarrow \alpha^i$.

Step *i*.2.c: Fathom the subproblem list, *i.e.*, $L \leftarrow L \setminus \{l : \beta^l \ge U\}$.

If $\beta^i \ge U$, then go to Step *i*.1 and select another subproblem.

Step *i*.3: Partition $\mathcal{P}^i$ into $\mathcal{P}^{i_1}$ and $\mathcal{P}^{i_2}$. Set $L \leftarrow L \cup \{i_1, i_2\}$, *i.e.*, append the two subproblems

$$\text{Min } \hat{G}_N(\chi) \text{ subject to } \chi \in \mathcal{X} \cap \mathcal{P}^{i_1} \text{ and Min } \hat{G}_N(\chi) \text{ subject to } \chi \in \mathcal{X} \cap \mathcal{P}^{i_2}$$

to the list of open subproblems. For selection purposes, set $\beta^{i_1}, \beta^{i_2} \leftarrow \beta^i$. Set $i \leftarrow i + 1$ and go to Step *i*.1

Details of each of the steps of the above algorithm are discussed in (1). Here, we briefly describe some of the key features.

B.Lower Bounding: As mentioned earlier, at iteration *i*, we shall only consider partitions of the form $\mathcal{P}^i := \prod_{j=1}^{m_2}\left[l_j^i, u_j^i\right)$ where l_j^i is sufficiently small such that $(h_j^n - l_j^n)$ is integral for some *n*. Consider the problem :

$$\beta^i := \min f(x) + \theta$$
$$s.t.\ x \in X,\ Tx = \chi,\ l^i \le \chi \le u^i,$$
$$\theta \ge \frac{1}{N}\sum_{n=1}^{N} \Psi^n\left(u^i - \varepsilon\right),$$

C.Upper Bounding: Let χ^i be an optimal solution of problem (20). Note that $\chi^i \in \mathcal{X}$, and is therefore a feasible solution. We can then compute an upper bound $\alpha^i := g(\mathcal{X}^i) \ge \min\{g(\chi) | \chi \in \mathcal{X}\}$.

D.Fathoming: Once we have isolated a region over which the second stage value function is constant, the lower and upper bounds over this region become equal. Subsequently such a region is fathomed in Step *i*.2.c of the algorithm. In other words, if, for a partition $\mathcal{P}^i$, the second stage expected value function $\hat{\Psi}_N(\cdot)$ is constant, then the partition $\mathcal{P}^i$ will be fathomed in the course of the algorithm.

E.Branching: To isolate the discontinuous pieces of the second stage value function, we are required to partition an axis j' at a point $\chi_{j'}$ that $\Psi^n(\cdot)$ is possibly discontinuous at $\chi_{j'}$ for some *n*. We can do this by selecting $\chi_{j'}$ such that $h_{j'}^n - \chi_{j'}$ is integral for some *n*.

VI. STATISTICAL BOUNDS

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Recall that $\hat{v}_N$ and v^* denote the optimal values of the SAA problem and the true problem, respectively. The following methodology of constructing statistical lower and upper bounds was suggested in (23) and developed further in (19).

It is well known that

$$E(\hat{v}_N) \leq v^*$$

Then the quantity

$$\hat{v}_N^M = \frac{1}{M}\sum_{m=1}^{M} \hat{v}_N^m$$

is an unbiased estimator of $E(\hat{v}_N)$, and therefore is a statistical lower bound to v^*.

$$s^2_{\bar{v}_N^M} := \frac{1}{M(M-1)}\sum_{m=1}^{M}\left(\hat{v}_N^m - \bar{v}_N^m\right)^2$$

Now consider a feasible solution $\bar{x} \in X$. For example, we can take $\bar{x}$ to be equal to an optimal solution $\hat{x}_N$ of an SAA problem.

$$\hat{g}_{N'}(\bar{x}) = c^T\bar{x} + \frac{1}{N'}\sum_{n=1}^{N'} Q(\bar{x}, \xi^n)$$

We have that $\hat{g}_{N'}(\bar{x})$ is an unbiased estimator of $c^T\bar{x} + E\left[Q(\bar{x}, \xi)\right]$. Consequently, since $(\bar{x})$ is a feasible point of the true problem, $\hat{g}_{N'}(\bar{x})$ gives a statistical upper bound

REFERENCES

1. Abomhara, M. & Koien, G. M. (2015). Stochastic integer programs and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Stochastic integer programs*, 4, 65-88
2. Amoroso, E.G. (2013). *Cyber attacks: Protecting national infrastructure*. Elsevier, Waltham, M.A
3. Crowell, R. M. (2010). *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare*. Newport: Naval War College
4. Goolsby, R. (2013). *On Cybersecurity, Crowdsorucing, and Social Cyber-Attack*. Arlington: Office of Naval Research
5. Liff, A. P. (2012). Cyberwar: A new "absolute weapon"?: The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, 35(3), 401-428
6. Porche, I. R., Paul, C., York, M., Serena, C. C., Sollinger, J.M. & Axelband, E. et al. (2013). *Redefining information warfare boundaries for an army in a wireless world*, RAND Institute, Santa Monica
7. Reddy, G. N. & Reddy, J. U. (2014). A Study of Stochastic integer programs Challenges and Its Emerging Trends on Latest Technologies. *International Journal of Engineering and Technology*, 4(1), 48-51
8. Sabrine, S., Muriel, C. & Stéphane, B. (2015). Infowar on the Web. *Proceedings of the ACM Web Science Conference on ZZZ - WebSci '15*, 1-3
9. Tabor, R. (2013). NATO Information Operations in Theory and Practice: Battling for Hearts and Minds in Afghanistan. *AARMS*, 12(1), 155-164
10. Van Niekerk, B. & Maharaj, M.S. (2012). Mobile devices and the military: Useful tool or significant threat? *Journal of Information Warfare*, 11(2), 1-11
11. Walker, C. & Conway, M. (2015). Online terrorism and online laws. *Dynamics of Asymmetric Conflict* 8:2, pages 156-175