Uncertainty Modeling: The Computational Economists' View on Cyberwarfare

Suchitra Abel

Abstract The current research scenario shows considerable work on the fundamental considerations for Cybersecurity. The physical world will fuse with the digital world in the future through enhanced technologies. However, there still exists the problem of radical uncertainty, particularly in the form of information theft. In this project we provide an analysis of the critical factors affecting the security of internet-based businesses; we also present a casual model-based security system that affects and helps the central characteristics of contemporary internet-based businesses.

1 Introduction

The internet, including the businesses that operate via Internet, can be perceived as a contingent commodity market. However, the economy has only imperfect solutions for situations where information purchase or theft for the sake of making explosives, for example, is done via the Internet. In this chapter, I will present a re-formulation of the traditional Economists' viewpoint that can be applied to modern Cyberwarfare. This is a systematic expression since the traditional Economists could not have thought of the current situation of Cyberwarfare. I will show how intelligent systems can tackle this problem and deal with the different parameters effectively.

We have to be prepared to increase the internet-based business community's awareness of our efforts in the form of programs designed to prevent crimes. Our work here will make it possible for companies to have emergency escalation procedures, mass notifications, and supporting systems.

S. Abel (✉)
Department of Computer Engineering, Santa Clara University, Santa Clara, CA 95053, USA
e-mail: sabel@cse.scu.edu

R.R. Yager et al. (eds.), *Intelligent Methods for Cyber Warfare*,
Studies in Computational Intelligence 563, DOI 10.1007/978-3-319-08624-8_12

2 Background of Research and Brief Literature Survey

Businesses are often driven by their need to maximize their utility, thus influencing their policies and decisions according to that need. Researchers have developed economic and mathematical models that explore numerous aspects of businesses. In the context of this concern, I hereby present an uncertainty model that will be effective in advancing a method that assists such businesses.

There are researchers who facilitated the development of the foundations of our current research on modeling for CyberWarfare. Cartwright [1, 2] and Fine [3] have produced some of the classics. In more recent times, Pearl [4–6] has been researching about causal models and structural models that utilize probabilistic logic. These researchers have provided the background and the inspiration behind the current work.

There are also practical problems of Cyber-threat that arise with companies like Adobe and Microsoft. Adobe has recently released security updates for Adobe Flash Player to address multiple vulnerabilities. Adobe has also released security updates for Adobe Reader and earlier versions for Windows and Macintosh, in order to address multiple exposures. These susceptibilities could cause a crash and potentially allow an attacker to take control of an affected system [7].

Microsoft has released updates to address vulnerabilities in Microsoft Windows, Microsoft Office, Internet Explorer, and Microsoft Server Software.These weaknesses could allow increasing code execution, elevation of privilege, denial of service, or information exposé [8].

These problems can inspire one to do further research on finding a solution of threat identification and consequent engagement. The following section is concerned with these practical aspects.

3 The Cyberwarfare Scenario

There is a rational need for uncertainty models specially targeted towards cloud computing and mobile cloud computing. In general, Cloud computing enables convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are businesses that rent Cloud services from Amazon [9], Google [10]. The businesses that rent Cloud services often have Research Divisions working on their security problems, inviting articles from outside the company too [11, 12].

Mobile Cloud security is another scenario that is becoming important. Smart phones, tablets, and cloud computing are converging in the new, briskly growing field of mobile cloud computing. In less than four years, there will be 1 trillion cloud-ready devices. One should learn about the devices (smart phones, tablets, Wi-Fi sensors, etc.), the trends (more flexible application development, changing

work arrangements, etc.), the issues (device resource poverty, latency/bandwidth, security, etc.), and the enabling technologies that come along with a mobile cloud environment [13].

Companies like Nokia and Microsoft are interested in Cybersecurity issues. The author provided an invited talk to the Nokia Research Lab, on this topic [14].

There is also emphasis, in the current research world, on finding a solution to Cyberwarfare, in the domain of internet-based businesses *in general*. The focus of the current chapter is not on overall mobile cloud security or even overall cloud security. Even without taking direction towards the line of cloud security or mobile security, there are many general issues concerning the computational Economists' view on Cyberwarfare, geared towards internet-based business in general, that are worthy of discussion. Alarming and often intimidating Cyber-attacks on internet-based business have reached an all-time high. Cybercrime is costing corporations this year, much more than last year. The statistics are in accordance with definitions used by the Department of Homeland Security, which confirms that there is a significant emergency or a dangerous situation involving an immediate peril [15].

The overall discussion of security measures using Bayesian modeling is certainly worth researching into. The next section shows that though the traditional Economists handled uncertainty in the context of businesses, they could not anticipate the complexities of modern businesses, for example, internet-based businesses that are open to the public all over the world, and are vulnerable to Cyber-attacks.

4 Traditional Economists: How they Would have Handled this Problem

This section expounds the traditional Economist's method of handling uncertainty in the context of businesses, and shows the shortcomings of such a method. In this model, the Internet site owners do bear the risks of misusing their proprietary information; they need to use subjective probabilities in determining their structures. It is decentralized decision making. There are administrative rules, legal rules (for example, no insider trading), etc. Of course, price of the commodity plays a vital role in who is acquiring the products. The buyers and the sellers do not have to know each other. The concept of free market does not mean the absence of rules, but how the rules ensure their freedom, in the highly competitive economy.

The traditional way of approaching this problem is to pursue standard mathematical methods, such as formulation of utility functions. The likely arguments of a typical Internet business's utility function, u, are its overall assets, a, the regular purchases for peaceful purposes, p, and the individual actions, Ind, of the company in trying to be persistent with such purchases. The business's utility function has the memorable Von Neumann-Morgenstern properties [16]. It empowers them to formulate preferences on all the arguments of their utility function [17, 18].

The scheme to prevent unexpected disruption-causing actions and to carry on typical purchases is the payoff function called g(S). This scheme can be classified according to their fundamental characteristics in the following spheres: first, one has to consider the region of the presence or absence of individual choice. There is individual choice if the individual actions, *Ind*, that compose a challenging argument in the Utility function. This might represent a level of investment. Next, there is the region of sequencing of moves between individual business's actions and customer actions. Lastly, one must not overlook the information, monitored by the scheme to prevent the disturbance. This information state, which may be a vector, is a function of the act of people who might interrupt the normal activities, and the actions of the individual business.

The scheme functions by establishing the payoff—financial gain of the individual business if the customers lead to legitimate business that one wants.

This also depends on the monitoring of the information state, such as: are the incoming customers authentic, or do they have the possibility to be disorderly?

There should be a break-even fiscal anticipation, for example, that the interference does not really halt the business. The scheme is to maximize the individual business's expected utility subject to the constraint.

We consider first a simple situation in which there is no room for individual choice.

Suppose that there is no individual choice to intervene. The scheme already devised by the business is the one that works—and it monitors the customers' activities. In this case, the sole determinant of the individual business' utility is the uncertainty regarding the customers' actions, p. These are obtained from standardized data retrieval about such actions. The distribution of p is given by the disruptive actions' density function f (p). The notion of p can be treated as continuous or as discrete.

The scheme to deal with customer actions p monitors the possibilities of p. In this case, the information state S = $\{p\}$. The scheme gives the individual business a payoff, g (p). This payoff, added to the initial assets of the particular business, called a_0, gives the total current *a,* argument of its utility function. In a purely numerical work, the individual business' expected utility under this scheme will be

$$\int \mathrm{u}\,(a_0 + \mathrm{g(p)}, \mathrm{p})\,\mathrm{f(p)}\,\mathrm{dp} \tag{1}$$

It is to be interpreted as the integration of the utility u with the two arguments, payoff added to the initial assets and the customer actions, and together with the disruptive actions' density function, f (p); this provides the expected utility.

The "dp" term comes from the following: the function f(p) is continuous for a $\leq$ p $\leq$ b. The interval from a to b can be divided into n equal subdivisions, each of width Δp, so that $\Delta \mathrm{p} = (\mathrm{b} - \mathrm{a})/\mathrm{n}$. The "dp" in the integral comes from the factor Δp.

The break-even constraint for this scheme is

$$\int \mathrm{g(p)}\,\mathrm{f(u)}\,\mathrm{d(u)} = 0 \tag{2}$$

This is the constraint, which should be obeyed, in order to maximize the individual business's expected utility. The "d (u)" term, with respect to the utility u, plays a role that is similar to the dp term in Eq. 1.

The scheme's objective is to maximize (1) with respect to (2). The scheme can employ the calculus of variations (calculating the maxima or minima of functional, which are often stationary). The business can employ the calculus of variations to derive the marginal efficiency condition for the optimal payoff function [19].

5 An Intelligent System to Address Critical Cases of Radical Uncertainty

5.1 Description of an Intelligent System

The model described in the previous section will not succeed in the case of radical uncertainty, since either there is not enough information available to use it as a parameter in a utility function, or its value is close to impossible to decipher. One can do immediate data analysis to give it some initial weight, but it really has no place in a calculus of variations. Instead of such calculations, we provide an AI based causal network, a solution that is well-suited to realizing the objective.

Bayesian causal networks represent independence (and dependence) relationships between variables. Thus, the links represent conditional relationships in the probabilistic sense.

My proposed system does not depend on the representative agent abstraction. There is no single type of consumer, nor is there a single type of economist who is analyzing the economy. Classically, models are used to generate quantitative statements. But the aggregate variables of a system can number up to hundreds, and the "representative consumer" or "representative economist" should be replaced by each economist/user of the system being represented as an individual.

For radical uncertainty, only immediately available knowledge can be used, and showing causal connections is critical. The cornerstone of our system is a causal model; such models are a system of processes that can account for the generation of the observed data. The ordering presented in the model respects the direction of time and causation. The judgments required in the construction of the model are meaningful, accessible and reliable. For example, we can assert that taking actions against the threat is independent of normal users accessing the site; we can translate this assertion into one involving causal relationships, once we know that the influence of normal business practices is mediated by the threat of the potential explosives-makers accessing the site. Dependencies that are not supported by causal links are spurious.

Conditional independence relationships are byproducts of stored causal relationships. So, representing these relationships directly would be a reliable way of expressing what we know about radical explosives-makers or material-purchasers.

5.2 Advantages of Bayesian Networks

An important point about building Bayesian networks on causal relationships is the ability to represent and respond to external or spontaneous changes, for example, sudden explosives-making purchase threats. Any local configuration of the mechanisms in the environment can be translated with only minor modification, into an isomorphic reconfiguration of the network topology. The use of causal relationships allows us to define the characteristics for the network topology.

As an example, suppose that in the process of doing normal business operations, suddenly the business schemes suspect an explosives maker's purchase threat. In this case, new nodes concerning suspected threat appear, with time stamp (before that, within a certain time period, normal purchases were completed and recorded). The previous nodes were connected to links; but now, when the abnormal nodes appear, we delete from the network all links incident to the node and its causal connections.

To represent the policy of *not* selling to this threat, we add necessary links and revise

P (buyers-nodes | requirement-nodes for purchase from this company).

Such changes would require much greater remodeling efforts if the network were not constructed in the causal direction but just having an associational order. This remodeling elasticity is the component that enables the agent to manage novel situations instantaneously.

It is quite conceivable to change certain node relationships without changing others. There is a modular configuration that permits one to deal with the effect of external interventions. The causal models are more informative than plain probability models. A joint distribution tells us how probable events are and how probabilities would change with subsequent observations. Causal models also tell us how these probabilities would change as a result of external interventions. Such changes cannot be deduced from a joint distribution, even if fully quantified.

Ideally, in the process of modeling, we need modularity. This is the ability of being made up of separate modules that can be rearranged, replaced, combined, or interchanged easily. The connection between modularity and involvements that are interventions is specified here. Instead of stating a new probability function for each of the many possible interventions, we indicate merely the immediate change implied by the intervention. We come to know the identity of the mechanism altered by the intervention, and the nature of the intervention.

A Bayesian network, in general, is a transporter of conditional independence relationships along the order of construction. The following product showing the distribution is:

$$P(x_1 \ldots x_n) = \pi\, P(x_i/pa_i) \tag{3}$$

pa_i are the select group of predecessors of x_i. The x's stand for the company components.

We can adjust this product's relevant factors and use the modified product to compute a new probability function.

If we have a distribution P defined on n discrete variables, ordered as $x_1, x_2, x_3 \ldots x_n$, then, utilizing the chain rule of probability calculus, we can decompose P as the product of n conditional distributions.

Suppose that the group of x's is independent of all other predecessors once we know the value of a select group of predecessors called pa_j. Then one can write:

$$P(x_1 \ldots x_{j-1}) = P(x_j/pa_j) \tag{4}$$

This will considerably simplify the input information required. We need only the possible realizations of the set pa_j. This is a minimal set of predecessors of x_j that is sufficient for determining the probability of x_j.

5.3 Causal Network Models

We will examine how the sequencing of moves and the information state, described in the previous section, interact in the determination of optimal schemes. First, let us consider a general case displaying how a business works with the information state and exerts its choice based on the sequences of moves. This is a case in which a certain information state is used to increase the possibility of business without disruption (desired result) by the sequencing of moves, but may also have direct effect on the business, both beneficial and adverse.

Suppose that we wish to assess the total effects of the information state on the desired result, when the following factors are present: (a) controlled experiments are not feasible, since the individual businesses insist on deciding for themselves which scheme to use (b) the business's choice of schemes depends on the previously gathered sequence of moves, a quantity though not totally known (obtained by data mining and other forms of data analysis), but known to be correlated with the current sequence of moves.

Let Seq-Moves-Before-Choice and Seq-Moves-after-Choice be the following: the first is the quantity (sequence of moves) before the individual business exerted its choice. The second is the quantity after the individual business exerted its choice. One can assign *probabilities* of the total effect of the information state on the desired result, based on the causal model. The subsequent diagram (labeled as Fig. 1) demonstrates this process.

In order to build a complete picture, we have to note that a business needs at least the following information: (1) Initial assets or products data (including numbers and prices). Let us call this x_1. (2) Demand appraisal that it needs to do; this is called x_2. Consequently, the business has to actually perform the act of sale to customers, called x_3. As a result of sales, the business will have profits, called x_4.

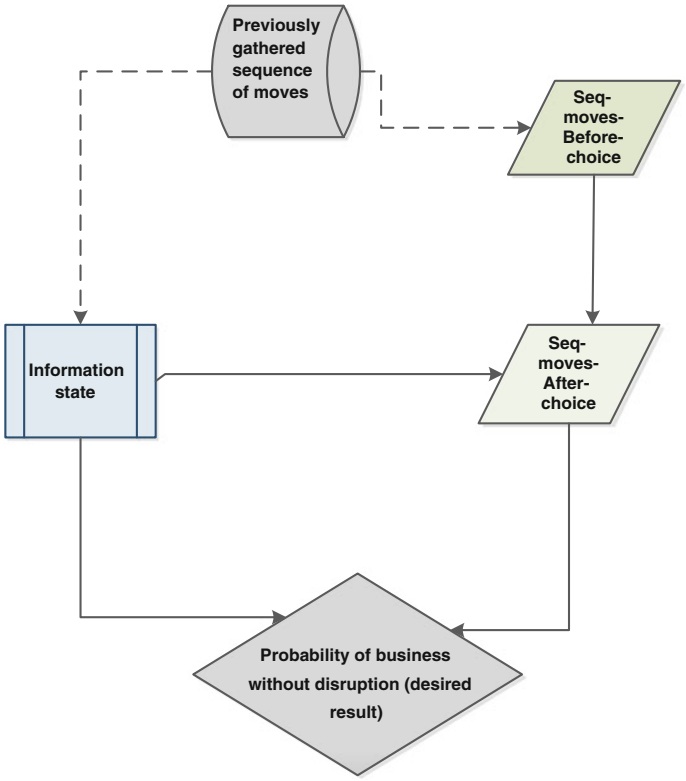

Fig. 1 A general causal model diagram showing the effect of the information state and the sequence of moves on the business

Therefore, next, let us draw a simple causal model, by constructing a directed acyclic graph (presented as Fig. 2). Suppose we know that two variables are dependent, data and demand appraisal (x_1 and x_2). In the case of suspected intervention, the arrows between x_2, x_3 and x_4 are removed, and the joint distribution also changes, leading to actions against the threat. y_1 through y_n are possible causal connections, with probability, of possible threats under radical uncertainty. (This is presented as Fig. 3).

As implied by our prior discussion, the principal concern in this chapter is to examine how the sequencing of moves and the information state interact in the determination of optimal business schemes.

In general, there often exist a set of schemes, implemented by a business, ensuring that the business is carried on, that is, that there are proper customers. This also includes the set of schemes to prevent the failure (built in by the business); the schemes ensure that the mechanisms are properly achieved, for example, by credit card monitoring, noting the buyer's involvement in the social media, etc.

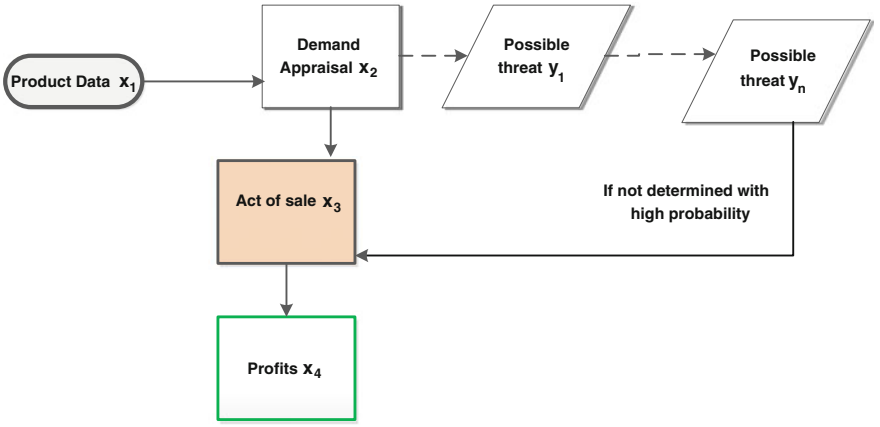

Fig. 2 Causal network model for uncertainty where the act of sale is completed

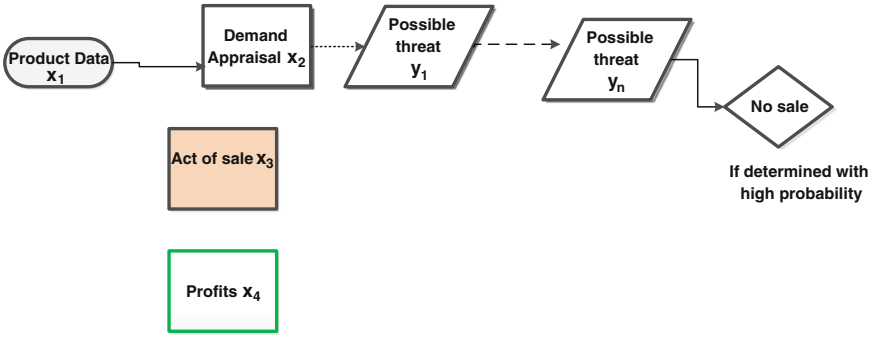

Fig. 3 Causal network model for uncertainty where threat is great, and therefore, no sale is generated

Next, there have to be, and indeed, there are, authentic internet based businesses. They might be, for example, businesses that supply materials for chemistry purposes.

What are the types of customers that the internet-based business has? There are non-disruptive customers who are using the businesses for peaceful purposes (the system might have some uncertainty about them). However, there are also distraction-causing customers or thieves—those that crash the system (they may be explosives makers). These cases cause radical uncertainty. They can be people or groups who are suspected of using these business websites to obtain material for warfare. Thus, there may be assumed unfavorable consequences. The operation of such markets provides the focus for our discussion. There is independence in the nature of these warfare schemed purchases, with respect to the internet businesses. We also assume that all such internet businesses have identical prospects, resources and utility functions. That is, they are not preferred businesses or have some pre-determined reputations.

We build a causal network model, of real world operations, in which the individual user (say, the Internet company owner) can formulate their own parameters of risk minimization and see how the values propagate to the ideal state. They all do not want the same solution. For some, a partial set of imperfect information might be enough.

Following are two diagrams of the causal network models. The first one represents the case where the act of sale is executed, since the threats do not have high probability. As a result, there are profits.

The second one represents the case of a causal network model for uncertainty where threat is great, as determined with high probability, and thus, no sale has come into effect. As a consequence, there are no profits from this particular action of "no sale".

6 Future Directions

In this section, the future directions of the current research are explored.

A new topic of research is the relevance of Bayesian modeling to Big Data.

Bayesian non-parametrics is an area in machine learning in which models grow in size and complexity as data accrue. As such, they are particularly relevant to the world of "Big Data", where it may be difficult or even counterproductive to fix the number of parameters a priori [20].

There is also a company [21] that is dealing with Big Data by producing a function called "BigData". The concept of Big Data is defined loosely as a data set that is too large for computer memory (RAM). A common strategy to deal with big data is to break it into smaller, manageable pieces, perform a function on those pieces, and combine the results back together. For this approach, the BigData function enables updating a model via Laplace Approximation.

The above mentioned work has been cited in several articles, such as [22].

Though Big Data is not the direct topic of this current project, it will ultimately be relevant to the current project, and therefore, I have mentioned it here. Big data-driven security system will be able to find the hidden patterns, the unexpected correlation, and the unexpected connections between data points tested under real-world conditions. Analyzing vast and complex data sets at high speed will allow us to spot the fake signal of an attack. This is because at some point, no matter how clever the attacker, they are liable to do something anomalous.

In a future direction of the work, in the new world of big data that provides cover for cyber attackers, we will concentrate on providing answers for devising a next-generation security system that can cope with emerging threats, The access controls will be smart in the new big data-driven security world. They will be able to inform or be informed by other controls [23].

My contribution in this regard will be substantial. Though the current work does not address any "self-learning" aspect, in the future, some aspects of "mutual learning" system have to be included. I think that the term "mutual learning" between

the different controls is significant in this respect, rather than the traditional self-learning, which did not have the same direction as the prevention of destructive attacks executed through the Internet. It will be interesting to see how the payoff function changes as a result, or whether the payoff function is replaced by some other mathematical concept.

7 Conclusion

We need to create a system that is inspiring, persuading and enlightening. For that purpose, we need to program and test the proposed system, using credible manifestos. That will involve supporting real-time simulation that allows consumers to explore the influence of a causal network model towards CyberWarfare.

As the expected immediate results of the system, we will ascertain what is required in the current state of CyberWarfare. According to the Homeland Security report, spanning from 2011 to 2013, [24] cybercrime is costing corporations more than the previous year; the increase in costs is largely due to hackers using stealthier techniques. There are insidious kinds of attacks like malicious code, denial of service, stolen devices, Web-based attacks and malicious insiders. According to this report, the strategy has to change from watching the outside wall to trying to figure out what is happening inside the network. The current research is geared towards this goal of strategy change.

References

1. Cartwright, N.: Probabilities and experiments. J. Econom. **67**, 47–59 (1995)
2. Cartwright, N.: Causality: independence and determinism. In: Gammerman, A. (ed.) Causal Models and Intelligent Data Management, pp. 51–63. Springer, Berlin (1999)
3. Fine, K.: Reasoning with Arbitrary Objects. Blackwell, New York (1985)
4. Pearl, J.: Probabilistic Reasoning in Intelligent Systems. Morgan Kaufman, San Mateo (1988)
5. Pearl, J.: Belief networks revisited. Artif. Intell. **59**, 49–56 (1993)
6. Pearl, J.: From Bayesian networks to causal networks. In: Gammerman, A. (ed.) Bayesian Networks and Probabilistic Reasoning, pp. 1–31. Alfred Walter, London (1994)
7. United States Computer Emergency Readiness Team, Security updates available for Adobe flash player, Adobe reader, and Acrobat, http://www.us-cert.gov/ncas/current-activity?page=1. Accessed 10 Sept 2013
8. United States Computer Emergency Readiness Team, Microsoft releases September 2013 security bulletin, http://www.us-cert.gov/ncas/current-activity, Accessed 10 Sept 2013
9. What is Cloud Computing? http://aws.amazon.com/what-is-cloud-computing/
10. Google Elbows Into the Cloud, http://www.nytimes.com/2013/03/13/technology/google-takes-on-amazon-and-microsoft-for-cloud-computing-services.html
11. Technical Report, HP Bristol, UK, Cloud stewardship Economics (2012)
12. Abel, S.: Application of Bayesian causal model for threat identification in the context of cloud usage by cloud Steward businesses, unpublished manuscript (2013)
13. Cox, P.A.: Mobile cloud computing, http://www.ibm.com/developerworks/cloud/library/cl-mobilecloudcomputing/,. Accessed 11 March 2011

14. Abel, S.: Cybersecurity using Bayesian causal modeling in the context of mobile computing, including image usage, in mobile devices—invited talk and powerpoint presentation at Nokia Research Lab, Sunnyvale, CA, 13 Aug 2013
15. Executive Order 13636: Improving critical infrastructure cybersecurity department of homeland security, integrated task force incentives study, analytic report, http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf. Accessed 12 June 2013
16. von Neumann, J., Morgenstern, O.: Theory of Games and Economic Behavior. Princeton University Press, Princeton (1944)
17. Mas-Colell, A., Whinston, M., Green, J.: Microeconomic Theory. Oxford University Press, Oxford (1995). ISBN 0-19-507340-1
18. Gilboa, I.: Theory of Decision Under Uncertainty. Cambridge University Press, Cambridge (2009)
19. Smith, D.R.: Variational Methods in Optimization. Dover, New York (1998)
20. Paisley, J.: Bayesian nonparametrics and big data, talk at the Columbia University School of Engineering, 22 Feb 2013
21. Statisticat, LLC, Big data and Bayesian inference, http://www.bayesian-inference.com/softwarearticlesbigdata. Accessed 22 Feb 2014
22. Maurya, M., Vishwakarma, U.K., Lohia, P.: A study of statistical inference tools for uncertainty reasoning in target tracking. Int. J. Comput. Networking Wirel. Mobile Commun. **3**(3), 1–10 (2013)
23. Intelligence-Driven Security: A new model using big data. Speaker: Mr. Art Coviello, Executive Vice President, EMC, Executive Chairman, RSA, In: The 3rd Annual International Cyber Security Conference, The Yuval Ne'eman Science, Technology & Security Workshop, Tel Aviv University, Israel
24. Homeland security report, http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-42_Feb13.pdf