REMARKS

This Amendment is being filed in response to the Office Action mailed May 8, 2015.

Status of the Claims

Prior to the amendment, claims 1 to 31, 33 and 34 were pending. The claims are amended as shown in the enclosed claim set. Following the amendment, claims 1 to 15, 17 to 31, 33 and 34 are pending. The amendments to the claims do not add subject matter. Applicant respectfully requests favorable reconsideration of the application in view of the amendments and the following remarks.

Claim 1 has been amended to specify *"An apparatus including one or more computer processors and a non-transient computer readable memory"*. Support for the amendment may be found in the published PCT application, for example, in the description on page 14, line 30 to page 15, line 9 and in Figure 4.

Claim 1 has also been amended to include the subject matter of claim 16, namely, that future threat activity is predicted using a Monte Carlo method. Claim 16 is cancelled.

Claims 2 to 15 and 17 to 26 have been amended to specify *"The apparatus"*. The amendments are made to provide articles which are consistent with dependence from claim 1.

Claims 13 and 26 have also been amended to specify a *"Monte Carlo"* method for consistency with claim 1 as amended.

Claim 27 has been amended to specify additional details of a method for predicting future threat activity using a Monte Carlo method. The amendments are made for consistency with amended claim 1.

Claims 28 to 30 and 33 have been amended to specify *"The method"*. The amendments are made to provide articles which are consistent with dependence from claim 27.

Claim 31 has been amended to specify additional details of steps which the computer system is caused to perform upon execution of the computer program. The amendments are made for consistency with amended claim 1.

Claim objections – informalities

Under point 5, the Examiner considers that claims 1 to 26 and 28 to 30 have missing or inappropriate articles in the claim language.

In response, claim 1 has been amended to specify *"An apparatus"*, claims 2 to 15 and 17 to 26 have been amended to specify *"The apparatus"*, and claim 16 has been cancelled. Claims 28 to 30 have also been amended to specify "The method". Thus, claims 1 to 15, 17 to 26 and 28 to 30 as amended include appropriate articles.

Therefore, withdrawal of the informalities objections against claims 1 to 15, 17 to 26 and 28 to 30 is respectfully requested.

Clarity – 35 USC § 112

Under point 6, the Examiner considers that claims 1 to 26 are indefinite. In particular, the Examiner considers that claim 1 is indefinite because the claim is drawn to an apparatus with a processor, which is then configured to read a memory, but that the apparatus only contains a processor. Claims 2 to 26 are considered indefinite because of dependence from claim 1.

In response, claim 1 has been amended to specify *"An apparatus including one or more computer processors and a non-transient computer readable memory"*. Thus, claim 1

as amended is clear and specifies an apparatus which includes a non-transient computer readable memory.

Therefore, withdrawal of the rejection of claims 1 to 26 as being indefinite under 35 USC § 112 is respectfully requested.

Under point 9 the Examiner considers that claims 31 and 34 are indefinite. In particular, the Examiner considers that the limitation *"**causes** the computer system to..."* (Examiner's emphasis) is unclear. The Examiner states that *"It's unclear as to what 'causes' is intended to include or excluded. There is no further discussion in the specification regarding the scope of the act that "causes". Broadly interpreted, an administrator/operator turns on a switch or makes a connection would be able to cause a system to do something"*. Claim 34 is considered indefinite because of dependence from claim 31.

The applicant respectfully disagrees with the Examiner's reasoning. In particular, the applicant notes that *"something"* is an unreasonably broad interpretation of predicting future threat activity as defined in claim 31. Furthermore, *"an administrator/operator turns on a switch or makes a connection"* is an unreasonably broad interpretation of a computer program when executed by a computer system. It is submitted that the Examiner's broad interpretation ignores the relevant context of the limitation *"causes the computer system to..."*.

Claim 31 has been amended in response to a different rejection. Claim 31 states:

> A non-transitory computer readable medium **having a computer program thereon**, which **when executed by a computer system** having one or more computer processors and a non-transient computer readable memory, **causes the computer system to predict**, for each of a plurality of threats, **future threat activity** using a Monte Carlo method based on stochastic modelling of past observed threat events

> capable of affecting at least one computer network in which a plurality of systems operate [...] (applicant's emphasis in bold)

It is clear from the language of claim 31 that the computer system is caused to predict future threat activity by executing the computer program stored on the non-transitory computer readable medium. The scope of claim 31 is also clear and well defined, in that a computer program is only within the scope of the claim if, when the program is executed on a computer system, the execution of the program results in the computer system predicting future threat activity as specified in claim 31.

Therefore, withdrawal of the rejection of claims 31 and 34 as being indefinite under 35 USC § 112 is respectfully requested.

Non-statutory subject matter – 32 USC § 101

Under point 8, regarding claims 1 to 26, the Examiner considers that claim 1 calls for an apparatus, but that the body of claim 1 does not positively recite any hardware embodiment. In particular, the Examiner considers that one or more processors could be implemented as software processors. Claims 2 to 26 are considered to relate to non-statutory subject matter because of dependence from claim 1.

Without conceding to the Examiner's interpretation, claim 1 has been amended in response to a different rejection (see discussion of point 6 above) to specify "*An apparatus including one or more computer processors and a non-transient computer readable memory*". Thus, claim 1 positively recites hardware in the form of a non-transient computer readable memory.

Therefore, withdrawal of the rejections of claims 1 to 15 and 17 to 26 as being directed to non-statutory subject matter under 35 USC § 101 is respectfully requested.

Under point 8, in relation to claims 27 to 31, 33 and 34, the Examiner considers that

the claims as a whole do not amount to significantly more than abstract idea. In particular, the Examiner considers that the claim(s) is/are directed to the abstract idea of predicting future threat activity. The Examiner also notes that claim 1 includes significantly more [than an abstract idea] as it also relates to simulations of threats.

In response to the rejection, claims 27 and 31 have been amended to include additional details of how future threat activity is to be predicted. Claim 27 as amended specifies:

> [...] the method comprising:
> predicting, **for each of a plurality of threats**, future threat activity **using a Monte Carlo method** based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate, **wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses;**
> **wherein for each given threat the method comprises:**
> **modelling a set of past observed threat events to obtain an estimate of at least one model parameter;**
> **performing a Monte Carlo simulation of the given threat by:**
>
> **predicting future threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable, and**
>
> **predicting a distribution of future threat events by repeating the simulation using a plurality of variables.** (applicant's emphasis in bold)

Claim 31 has been amended in a similar way. Consequently, claims 27 and 31 specify predicting future threats using features corresponding to claim 1. As noted by the Examiner, claim 1 includes significantly more than an abstract idea. Thus, because claims 27 and 31 as amended specify predicting future threats using features corresponding to claim 1, claims 27 and 31 as amended include significantly more than an abstract idea.

Therefore, withdrawal of the rejections of claims 27 to 31, 33 and 34 as being directed to non-statutory subject matter under 35 USC § 101 is respectfully requested.

Novelty – 35 USC § 102

Under point 12, the Examiner considers that claims 27, 31, 33 and 34 are anticipated by Yun et al. Applicant respectfully traverses the rejections for the reasons noted below.

Without conceding to positions in the Office Action and for the sole purpose of advancing prosecution, the applicant has amended claims 27 and 31 to specify predicting future threat activity "*using a Monte Carlo method*".

Yun et al ("Yun") does not mention Monte Carlo methods or modelling using Monte Carlo methods. Furthermore, a Monte Carlo method describes a procedure which is different to a Markov chain prediction model.

Thus, at least by virtue of using Monte Carlo methods, independent claims 27 and 31 are new over Yun.

Dependent claim 33 is new over Yun at least by virtue of dependence from claim 27.
Dependent claim 34 is new over Yun at least by virtue of dependence from claim 31.

Therefore withdrawal of the rejections of claims 27, 31, 33 and 34 as being anticipated under 35 USC § 102 is respectfully requested.

Obviousness – 35 USC § 103

Joint inventors and commonly owned subject matter

Under point 14 the Examiner considers that the present application currently names joint inventors.

The applicant respectfully points out that the present application has a single inventor, namely Phillipe Evrard.
Furthermore, the assignment, as listed on the USPTO PAIR database, specifies a single assignor, namely Phillipe Evrard, and a single assignee, namely Quantar Solutions Limited.

Thus, the present application has a single inventor and a single assignee.

Independent claims

Under point 15, the Examiner considers that claim 1 is obvious over Yun et al. in view of Horng et al. Applicant respectfully traverses the rejection for the reasons noted below.

Without conceding to positions in the Office Action and for the sole purpose of advancing prosecution, the applicant has amended claim 1 to specify predicting future threat activity "*using a Monte Carlo method*".

As already explained, Yun does not mention Monte Carlo methods or modelling using Monte Carlo methods, and a Monte Carlo method describes a procedure which is different to a Markov chain prediction model. Horng et al. ("Horng") does not mention Monte Carlo methods or modelling using Monte Carlo methods, and thus cannot cure the deficiency of Yun.

Thus, whether alone or in combination, Yun and Horng do not describe predicting future threat activity using a Monte Carlo method based on stochastic modelling of past observed threat events.

Furthermore, Horng does not describe predicting future threat events using at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable.

Horng describes a random factor, b (see for example paragraphs [0011], [0025], [0032] and [0035] of Horng). However, the random factor, b, is not a randomly drawn variable, i.e. a generated random or pseudo-random number. Instead, the random factor, b, is a parameter which is calculated from the known data traffic elements x and mean value sequences z (see in particular Equations A.4 to A.9). Yun does not mention "*random*" variables, and thus cannot cure the deficiency of Horng.

Thus, whether alone or in combination, Yun and Horng do not describe predicting future threat events using at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable

Therefore, because the features described above are not described in Yun or Horng, the person of ordinary skill in the art simply cannot arrive to the claimed apparatus by combining Yun and Horng.

Furthermore, the asserted combination of Yun and Horng combines two documents which are unrelated, as shall be explained in detail below.

Horng describes:

> [0008] The present invention relates to **detection of distributed denial of service (DDOS) attacks**. According to the invention, **grey theory is applied in the detection method**. Grey theory was first disclosed in 1982 by Dr. Chu-Lung Dang. It enables analysis of parameters and model construction **in a system model with a degree of uncertainty and inadequate supporting information**. Related details can be obtained in the bibliography located at: (applicant's emphasis in bold)

It is clear that Horng applies grey theory to detecting distributed denial of service ("DDOS") attacks. Horng describes using grey theory to compare data sets in order to trigger a defense procedure when the analysis (comparison) result meets a predetermined condition (see for example paragraphs [0012] and [0030]). As is seen most clearly in Figure 2b of Horng, the predictive sequence of Horng is merely compared to an actual sequence, and the predictive sequence does not forecast for times in advance of the actual sequence.

Thus, Horng is concerned with detection of threat activity and is not concerned with predicting future threat activity.

Furthermore, a DDOS attack is completely different to a plurality of electronic threats including a plurality of computer viruses. In contrast to a computer virus or malicious code, a DDOS attack involves up to millions of computers and botnets that have the objective of overwhelming a network with traffic in order to be unstoppable by security systems. Unlike a virus/malicious code attacker, the roots and identities of individual machines involved in a DDOS are impossible to identify due to the volumes, and consequently cannot be individually stored and used as a basis for subsequent modelling.

Thus, Horng is concerned with an entirely different class of threat to Yun. Therefore, for the reasons explained above, the skilled person simply would not consider Horng to be related prior art.

Furthermore, the asserted combination of Yun and Horng combines two documents which are incompatible, as shall be explained in further detail below.

It is respectfully submitted that the skilled person would understand that, far from being a method of stochastic modelling, grey theory is in fact almost the opposite of stochastic modelling. The underlying principles of grey theory shall be explained, in order to highlight the differences to stochastic modelling.

Uncertainty can be divided into two categories: stochastic and fuzzy. Stochastic uncertainty can be analyzed through the use of probabilistic statistics. A large number of data are required to apply the mathematical statistics used to determine the statistical rule of the original data by a large sample. Stochastic methods are used to model systems in which the nature of the underlying processes themselves introduces uncertainty, for example, modelling Brownian motion or quantum mechanics.

In contrast, fuzzy uncertainty can be analyzed by fuzzy mathematics or grey system theory. Grey prediction needs minimal data to construct a grey differential equation for prediction. It should be noted that Grey theory requires smoothing in order to generate a trend, as discussed further below. Grey theory is most useful when obtaining or analysing a complete dataset is impossible or impractical, for example,
the roots and identities of individual machines involved in a DDOS attack as explained earlier.

Grey models predict the future values of a time series based only on a set of the most recent data depending on the window size of the predictor. It is assumed that all data

values to be used in grey models are positive, and the sampling frequency of the time series is fixed. From the simplest point of view, grey models can be viewed as curve fitting approaches. The main task of grey system theory is to extract realistic governing laws of a system using available data. It may be considered that, even though the available data of the system, which are generally known numbers/values, are too complex or chaotic, they always contain at least some governing laws. If the randomness of the data obtained from a grey system is somehow smoothed, it is easier to derive any special characteristics of that system.

In summary, grey theory describes methods for coping with uncertainty which results from incomplete data. In contrast, stochastic modelling describes methods for predicting/extrapolating random processes, i.e. stochastic modelling and grey theory relate to uncertainties which have different underlying causes.

Thus, the asserted combination of Yun and Horng is inappropriate because of the different motivations and purposes of stochastic modelling and grey theory.

Therefore, for at least the reasons already explained, claim 1 is non-obvious over Yun in view of Horng. Withdrawal of the rejections of claim 1 as being obvious under 35 USC § 103 is respectfully requested.

As already explained, claims 27 and 31 have been amended to specify corresponding limitation to claim 1. Therefore, for the same or similar reasons as claim 1, claims 27 and 31 are also non-obvious over the cited prior art documents.

Dependent claims

Under points 15 to 22, the Examiner considers that the remaining dependent claims are obvious over various combinations of prior art. Applicant respectfully traverses the rejections for the reasons noted below.

Without conceding to the positions in the Office Action, the applicant notes that the dependent claims 2 to 15, 17 to 26, 28 to 30, 33 and 34 are each new and non-obvious at least by virtue of dependence from the respective independent claims.

Therefore, withdrawal of the rejections of the dependent claims as being obvious under 35 USC § 103 is respectfully requested.

CONCLUSION

In view of the foregoing it is believed the application is in condition for allowance and it is respectfully requested and that all pending claims be allowed and the case passed to issue.

Favorable reconsideration of the merits and prompt allowance of the application is respectfully requested.

This response is being filed with a request for two-month extension of time, the fee for which is enclosed herewith.

In the event that there are any questions, or should additional information be required, or if examination can be expedited through clarification or discussion, the Examiner is invited to contact Applicant at the number listed below.

Respectfully submitted,

/Phillip King-Wilson/

Applicant
8421 Woodleaf Boulevard
Wesley Chapel
Florida
33544
(813) 357-4113