Trials@uspto.gov
571-272-7822

Paper 11
Entered: February 10, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSCOUT SYSTEMS, INC.,
Petitioner,

v.

LONGHORN HD LLC,
Patent Owner.

IPR2021-01258
Patent 7,260,846 B2

Before KARL D. EASTHOM, GARTH D. BAER, and MATTHEW S. MEYERS, *Administrative Patent Judges.*

MEYERS, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

NetScout Systems, Inc. ("Petitioner") filed a Petition to institute an *inter partes* review of claims 1–12 (the "challenged claims") of U.S. Patent 7,260,846 B2 (Ex. 1001, the "'846 patent"). Paper 1 ("Pet."). Longhorn HD LLC ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp."). After receiving authorization, Petitioner filed a Reply (Paper 8), and Patent Owner filed a Sur-reply (Paper 9). *See* Paper 7.

We have authority, acting on the designation of the Director, to determine whether to institute an *inter partes* review. 35 U.S.C. § 314; 37 C.F.R. § 42.4(a) (2020). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted unless "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least [one] of the claims challenged in the petition."

After considering the Petition, the Preliminary Response, the Reply, the Sur-reply, and the evidence of record, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail with respect to at least claims 1–11. Although it is a closer question as to whether Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to claim 12, we determine, based on the record before us, that instituting a trial with respect to all challenged claims is not an efficient use of the Board's time and resources. Accordingly, we do not institute an *inter partes* review of any challenged claim on any asserted ground pursuant to 35 U.S.C. § 314. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359–1360

(2018) (requiring institution on all claims, if any); *see also* Patent Trial and Appeal Board Consolidated Trial Practice Guide, 64 (Nov. 2019) (providing guidance in view of *SAS*).[1]

B. Real Parties-in-Interest

Petitioner identifies itself as the real party-in-interest. Pet. 71. Patent Owner names itself as the real party-in-interest. Paper 4, 1.

C. Related Proceedings

Petitioner identifies, as matters involving or related to the '846 patent, *Longhorn HD LLC v. NetScout Systems, Inc.*, 2-20-cv-00349 (E.D. Tex.). Pet. 71. The parties also identify, as matters involving or related to the '846 patent, *Longhorn HD LLC. v. Juniper Networks, Inc.*, 2:21-cv-00099 (E.D. Tex., Mar. 19, 2021); *Unified Patents, LLC v. Longhorn HD LLC*, IPR2020-00879 (PTAB, May 7, 2020).[2] Pet. 71; Paper 4, 1.

D. The '846 Patent

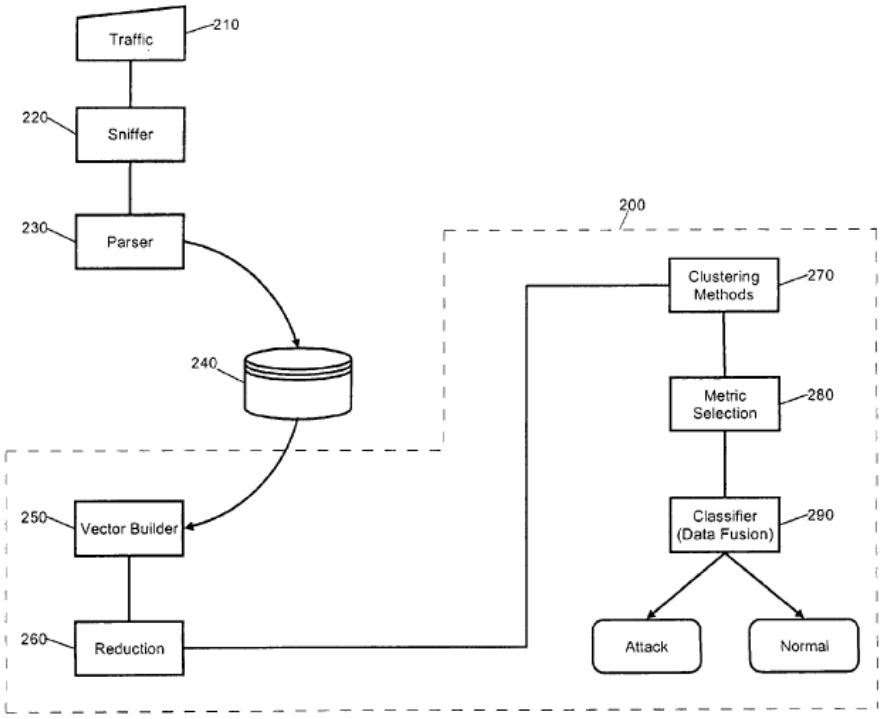
The '846 patent is titled "INTRUSION DETECTION SYSTEM." Ex. 1001, code (54). According to the '846 patent, "[t]o fill the security gap left open by firewall usage, information technologists incorporate intrusion detection system (IDS) technology within the enterprise." *Id.* at 1:44–46. The '846 patent is directed to an IDS that "can monitor [any] packets passing across a coupled communications path" and "identify protocol boundaries separating the various fields of each passing network packet and

[1] *Available at* https://www.uspto.gov/TrialPracticeGuideConsolidated.
[2] In IPR2020-00879, a Final Written Decision determined that claims 7, 8, 10, and 11 of the '846 patent are unpatentable. IPR2020-00879, Paper 35 at 53 (Nov. 9, 2021). Patent Owner filed a notice of appeal to the United States Court of Appeals for the Federal Circuit. IPR2020-00879, Paper 36 (Jan. 11, 2022).

can store data for selected ones or all of the fields in a database, such as a relational database." *Id.* at 4:25–31. "In particular, data for each field can be stored in a separate record to facilitate the robust analysis of the stored data at a substantially granular level." *Id.* at 4:31–33.

The '846 patent explains that "[o]nce sufficient data has be[en] stored in the database, multidimensional vectors can be constructed and reduced from the stored data" and "[t]he reduced multi-dimensional vectors can be processed using one or more conventional multi-variate analysis methods and the output sets produced by the multi-variate analysis methods can be correlated against one another according to one or more selected metrics." Ex. 1001, 4:34–40. Then, "[b]ased upon these correlations, both normal and anomalous events can be identified." *Id.* at 4:40–42.

Figure 2 of the '846 patent, reproduced below, is a flow chart illustrating a process for performing intrusion detection. Ex. 1001, 8:6–7.



As shown in Figure 2 (above), packet sniffer 220 can extract network traffic 210 flowing across a communications path coupled to IDS 200. *Id.* at 8:7–10. Parser 230 can de-construct the network packets along known protocol field boundaries, such as destination and source IP address, time-to-live, payload size, packet type, type of service, etc. *Id.* at 8:28–31. Subsequently, selected ones of the de-constructed fields can be stored in separate records in database 240 and can be associated with the particular socket to which the packet belongs. *Id.* at 8:32–35.

In block 250, a vector builder in a feature extraction process can select individual ones of the network packet fields to be included in the construction of a multi-dimensional vector. Ex. 1001, 8:39–42. Multi-dimensional vectors can be constructed using the chosen features produced in block 250. *Id.* at 8:51–53. Specifically, the vector builder can process the records in the database 240 to identify pertinent fields associated with a particular "conversation" or socket. *Id.* at 8:53–55. In block 260, a vector separation system can reduce the dimensionality of the multi-dimensional vectors in order to simplify a subsequent multi-variate analysis. *Id.* at 8:64–66. Components of the multi-dimensional vectors that appear to be redundant, irrelevant, or otherwise insignificant relative to other interested components can be eliminated across all or a selection of the multi-dimensional vectors to produce a set of reduced vectors. *Id.* at 8:66–9:7.

In block 270, one or more self-organizing clustering methodologies can be applied concurrently or sequentially to the set of reduced vectors. Ex. 1001, 9:8–10. After the reduced vectors have been processed by the multiple clustering methodologies in block 270, one or more metrics can be selected in block 280 for purposes of establishing a correlation between the

output sets of the processed reduced multi-dimensional vectors. *Id.* at 9:15–19. In block 290 a classifier can identify from any established correlations whether an anomaly has been detected. *Id.* at 9:21–23. The classification process of block 290 can identify either normal traffic or an attack. *Id.* at 9:25–26.

E. Illustrative Claim

Petitioner challenges claims 1–12 of the '846 patent. Pet. 1. Claims 1, 7, and 12 are independent claims. Claim 1 is illustrative and reads as follows:

> 1. An intrusion detection system (IDS) comprising:
>
> a traffic sniffer executing in a computing system for extracting network packets from passing network traffic;
>
> a traffic parser executing in a computing system configured to extract individual data from defined packet fields of said network packets;
>
> a traffic logger executing in a computing system configured to store individual packet fields of said network packets in a database;
>
> a vector builder executing in a computing system configured to generate multi-dimensional vectors from selected features of said stored packet fields;
>
> at least one self-organizing clustering module executing in a computing system configured to process said multi-dimensional vectors to produce a self-organized map of clusters;
>
> an anomaly detector executing in a computing system able to detect anomalous correlations between individual ones of said clusters in said self-organized map based upon at least one configurable correlation metric; and
>
> a classifier executing in a computing system configured to classify detected anomalous correlations as one of an alarm behavior.

Ex. 1001, 10:49–11:6.

F. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–12 of the '846 patent are unpatentable on the following grounds:

Claims Challenged	35 U.S.C. §[3]	References
1–5, 7–11	103	Rhodes[4], McCreery[5]
6	103	Rhodes, McCreery, Lee[6]
12	103	Rhodes, McCreery, Wetherall[7]

Petitioner also relies on the Declaration of Dr. Wenke Lee (Ex. 1003, "the Wenke Declaration") in support of its arguments.

II. ANALYSIS

A. Legal Standards

"In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (2012) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports

[3] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. §§ 102 and 103 effective March 16, 2013. Because the '846 patent's effective filing date predates the AIA's amendments to § 103, this decision refers to the pre-AIA version of § 103.
[4] Brandon Craig Rhodes, et al., "Multiple Self-Organizing Maps for Intrusion Detection", Computer Science and Information Technology Division Information Technology and Telecommunications Laboratory Georgia Institute of Technology (Ex. 1004, "Rhodes").
[5] US 5,787,253, issued July 28, 1998 (Ex. 1005, "McCreery").
[6] Wenke Lee, et al., "Data Mining Approaches for Intrusion Detection", (Jan. 26–29, 1998) (Ex. 1006, "Lee").
[7] US 7,970,886 B1, issued June 28, 2011 (Ex. 1007, "Wetherall").

the grounds for the challenge to each claim")). This burden of persuasion never shifts to the patent owner. *See Dynamic Drinkware, LLC v. Nat'l Graphics*, Inc., 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which that subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness when presented. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In analyzing the obviousness of a combination of prior art elements, it can be important to identify a reason that would have prompted one of skill in the art "to combine . . . known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418. A precise teaching directed to the specific subject matter of a challenged claim is not necessary to establish obviousness. *Id.* Rather, "any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id.* at 420. Accordingly, a party who petitions the Board for a determination of unpatentability based on obviousness must show that "a skilled artisan would have been motivated to combine the teachings of the prior art

references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) (quotations and citations omitted).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

B. Level of Ordinary Skill in the Art

We review the grounds of unpatentability in view of the understanding of a person of ordinary skill in the art at the time of invention. *Graham*, 383 U.S. at 17. Petitioner asserts one of ordinary skill in the art

> at the time of the '846 Patent would have had at least a bachelor's degree in electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of network security and performance monitoring systems, with additional education substituting for experience and vice versa.

Pet. 6 (citing Ex. 1003 ¶¶ 25–27).

Patent Owner does not dispute Petitioner's assessment at this stage of the proceeding. *See generally* Prelim. Resp.

Based on our review of the record at this stage, we find that Petitioner's proposal is consistent with the level of skill reflected in the prior art references of record. *See Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007) (listing the type of problems encountered in the art, prior art solutions to those problems, and the sophistication of the technology as factors that may be considered in determining the level of ordinary skill in the art). The prior art itself may be sufficient to demonstrate the level of skill in the art at the time of the invention. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (explaining that

specific findings regarding ordinary skill level are not required "where the prior art itself reflects an appropriate level and a need for testimony is not shown") (quoting *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 163 (Fed. Cir. 1985)).

Thus, for purposes of this decision, we adopt Petitioner's proposed definition of the level of ordinary skill in the art.

C. Claim Construction

In an *inter partes* review proceeding for a petition filed on or after November 13, 2018, a patent claim shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b).[8] This rule adopts the same claim construction standard used by Article III federal courts, which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*), and its progeny.

Petitioner submits that the Board should "adopt the claim constructions advanced by Patent Owner in the [c]o-pending [l]itigation, for purposes of this proceeding only." Pet. 18. According to Petitioner, in the co-pending litigation, "Patent Owner contends that all claim terms should be given their plain and ordinary meaning." *Id.* (citing Ex. 1037).

Patent Owner does not address Petitioner's contentions or otherwise address claim construction. *See generally* Prelim. Resp.

For purposes of this Decision, we determine that no construction of any term is necessary to resolve the issues presented by the arguments and evidence of record to reach a decision on institution. *See Nidec Motor Corp.*

[8] The Petition in this case was accorded a filing date of August 11, 2021. *See* Paper 3, 1.

v. Zhongshan Broad Ocean Motor Co., 868 F.3d 1013, 1017 (Fed. Cir. 2017) (per curiam) (claim terms need to be construed "only to the extent necessary to resolve the controversy" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Alleged Obviousness over Rhodes and McCreery

Petitioner asserts that claims 1–5 and 7–11 are unpatentable as obvious over Rhodes and McCreery. Pet. 18–58. Petitioner also relies on the testimony of Dr. Lee to support its arguments. *Id.* Patent Owner responds to Petitioner's assertions. Prelim. Resp. 1, 13–17.

1. Overview of Rhodes (Ex. 1004)

Rhodes is a paper titled "Multiple Self-Organizing Maps for Intrusion Detection," and relates to techniques "for detecting intrusive or abnormal behavior on computer systems" using a collection of Kohonen self-organizing maps. Ex. 1004, Abstract, 1. According to Rhodes, traditional intrusion detection system utilize techniques that "that involve pattern matching, expert systems, and traditional neural networks [that] require detectors to either be crafted by hand or trained upon examples of known intrusions." *Id.* Rhodes suggests that "unsupervised learning can provide a powerful supplement to these techniques." *Id.*

Rhodes discloses that a "Kohonen self-organizing map" is able "to learn the characteristics of normal system activity on a multiuser machine and identify variations from that norm that could indicate the presence of a virus." Ex. 1004, 2. Rhodes further discloses that these self-organizing maps "automatically categorize[] the varieties of input presented during training and can then express how well new inputs fit the patterns it has discerned." *Id.* at 3. More particularly, Rhodes discloses that "[a]n input to

a Kohonen map takes the form of a mathematical vector (an ordered list of coordinates)," but notes that "[t]he map must have been provided with some means of measuring how different two vectors are; for this paper we will call this function that compares two vectors our comparison function." *Id.* at 3 (emphasis omitted). Rhodes further discloses that when an input vector is presented to the map for evaluation,

> it is compared (using the map's comparison function) with every prototype vector in the grid. The map then outputs two pieces of information: the location (in grid coordinates) of the prototype that most closely matches the input vector, and the measure of how well the input vector fits the prototype (that is, the metric returned by the comparison function).

Id.

When presented with a set of input vectors to train on, Rhodes discloses

> the Kohonen map spontaneously organizes them so that similar vectors are clustered together on its surface, and that important variations among vectors are reflected in their arrangement. The distance between where two vectors are placed on its surface represents not their absolute dissimilarity — which we already knew how to compute — but their difference relative to the space of possibilities present in the training set.

Ex. 1004, 3–4. Rhodes suggests that many techniques may be used for measuring vector similarity, but notes that "many vectorization techniques will be suited for detecting some intrusions at the expense of others." *Id.* at 8. For example, Rhodes identifies that

> while a Kohonen map designed with buffer overflow attacks in mind will almost certainly be more flexible than a set of rules watching for the same type of activity, both may completely overlook some other kind of attack of which their designers were ignorant. The Kohonen map may thus have a limit to how far outside our expectations it can detect abnormal activity.

Id.

2. Overview of McCreery (Ex. 1005)

McCreery is titled "APPARATUS AND METHOD OF ANALYZING INTERNET ACTIVITY." Ex. 1005, code (54). McCreery relates to an internet activity analyzer that "includes a network interface controller, a packet capturing module, a packet analysis module, and a data management module." *Id.*, Abstract. According to McCreery, "[b]y capturing and analyzing data packets transmitted along a network transmission medium between nodes, the internet activity analyzer of the present invention facilitates the analysis of performance based upon reliable data without requiring access to the server." *Id.* at 2:50–54.

McCreery discloses "packet capturing module 322 communicates with the network interlace 316 through the system bus 302 and includes routines which capture and hold raw packets of data for processing by the analyzer 300." Ex. 1005, 7:26–29. McCreery then discloses that "packet analyzer 324 receives the raw packet data through the system bus 302 and includes routines which decode the raw packet data into coherent information." *Id.* at 7:33–40. McCreery further discloses that data management module 326 "accesses the information in the raw packet, decoded packet, raw transaction and translated transaction data buffers through the system bus 302 and includes routines for inferring network information about the data." *Id.* at 7:51–57. McCreery also discloses alarm generator 330 communicates with data management module 326 in order to issue alarms. *Id.* at 8:1–3. McCreery identifies that "alarm generator 330 includes threshold information, data defining the scope of interrogation, and

data identifying parties to notify in the event of alarm conditions." *Id.* at 8:3–6.

3. Analysis of Claim 1

Petitioner asserts claim 1 would have been obvious over Rhodes and McCreery. Pet. 29–43. We use Petitioner's notations to identify the claim elements, and focus on the dispositive claim limitation.

a) 1[f] an anomaly detector executing in a computing system able to detect anomalous correlations between individual ones of said clusters in said self-organized map based upon at least one configurable correlation metric[9]

(1) Petitioner's Contentions

Petitioner asserts that Rhodes discloses or renders obvious the subject matter of limitation 1[f]. Pet. 39–41 (citing Ex. 1003 ¶¶ 101–104; Ex. 1004, 3, 8–11). According to Petitioner, "Rhodes explains that it has 'constructed an anomaly detector based on a Kohonen map, and successfully detect[ed] two different exploit attempts.'" *Id.* at 39 (citing Ex. 1004, 9, 11). Petitioner asserts that Rhodes detects anomalous behavior using a "'comparison function' to measure 'how different two vectors are.'" *Id.* (citing Ex. 1004, 3). Petitioner explains that

> when an input vector is presented for evaluation in *Rhodes*, it is "compared (using the map's comparison function) with every prototype vector in the grid." *Id.* Then, the map outputs the location of the grid vector that most closely matches the input vector, and the measure of how well the input vector fits the grid

[9] Limitation 1[f] is substantially similar to limitation 7[e]. However, while limitation 1[f] recites "detect[ing] anomalous correlations between individual ones of said clusters detects" (Ex. 1001, 10:66–11:3), limitation 7[e] recites "establishing a correlation between individual output sets." *Id.* at 11:40–43.

> vector "(that is, the metric returned by the comparison function)."

Id. at 39–40 (citing Ex. 1004, 3, 8). Petitioner takes the position that Rhodes' system uses "a 'particular distance measure' as the metric, which resulted in the 'normal traffic' being characterized, or 'scored,' much differently than traffic associated with an intrusion" (*id.* at 40 (citing Ex. 1004, 9–11)), and concludes that "[t]his allowed the system to detect anomalous correlations between clusters based on a 'particular distance measure.'" *Id.* (citing Ex. 1004, 10–11).

(2) Patent Owner's Contentions

Patent Owner asserts that the Petition is deficient because Petitioner has not shown that Rhodes discloses or suggests "an anomaly detector executing in a computing system able to detect anomalous correlations between individual ones of said clusters in said self-organized map based upon at least one configurable correlation metric," as recited by limitation 1[f]. Prelim. Resp. 13–15. More particularly, Patent Owner argues that claim 1 "require[s] correlation [to be] done after the vector building step," but "Rhodes is silent with regard to the correlation between the output sets or clusters." *Id.* at 13.

b) Discussion

Having considered the conflicting positions of the parties, we conclude that Petitioner has not shown a reasonable likelihood that it would prevail in challenging the patentability of independent claim 1. Instead, we agree with Patent Owner that Petitioner has not demonstrated that the cited prior art discloses or suggests "detect[ing] anomalous correlations between individual ones of said clusters in said self-organized map based upon at

least one configurable correlation metric," as required-in-part by limitation 1[f].

Petitioner's analysis for this limitation begins with the contention that Rhodes detects anomalous behavior using a "'comparison function' to measure 'how different two vectors are.'" Pet. 39 (citing Ex. 1004, 3). In response, Patent Owner points out that "[c]laim 1 requires at least the following three structural elements: (1) a 'vector builder,' (2) a 'self organizing clustering module,' and (3) an 'anomaly detector[']', able to 'detect anomalous correlations between individual ones of said clusters', and (4) a 'classifier.'" Prelim. Resp. 13. Patent Owner argues that Petitioner's analysis "conflates these distinct limitations" and "ignores the explicit teachings of *Rhodes* that contradict its arguments" by "conflat[ing] the correlation of input vectors with the correlation of ***clusters*** or ***output sets***." *Id.* Stated differently, Patent Owner argues that "[t]he claims do not require correlation of input vectors, but rather correlation of the output sets." *Id.* at 15. We agree with Patent Owner.

Petitioner contends that Rhodes detects anomalous correlations using a "'comparison function' to measure 'how different two vectors are.'" Pet. 39 (citing Ex. 1004, 3). Petitioner explains that "when an input vector is presented for evaluation in *Rhodes*, it is 'compared (using the map's comparison function) with every prototype vector in the grid,'" and "[t]hen, the map outputs the location of the grid vector that most closely matches the input vector, and the measure of how well the input vector fits the grid vector." *Id.* at 39–40 (citing Ex. 1004, 3, 8). Petitioner asserts "Rhodes' system used a 'particular distance measure' as the metric, which resulted in the 'normal traffic' being characterized, or 'scored,' much differently than

traffic associated with an intrusion." *Id.* at 40 (citing Ex. 1004, 9–11). Petitioner, thus, concludes that "[t]his allowed the system to detect anomalous correlations between clusters based on a 'particular distance measure.'" *Id.* (citing Ex. 1004, 10, 11).

The problem with Petitioner's contention is that limitation 1[f] does not require an "anomaly detector" to detect anomalous correlations *between input vectors*, but instead, an "anomaly detector . . . to detect anomalous correlations *between* individual ones of said *clusters*." Ex. 1001, 10:66–11:3. In this regard, the'846 patent's specification discloses

> [o]nce sufficient data has be stored in the database, multi-dimensional vectors can be constructed and reduced from the stored data. The reduced multi-dimensional vectors can be processed using one or more conventional multi-variate analysis methods and the output sets produced by the multi-variate analysis methods can be correlated against one another according to one or more selected metrics.

Id. at 4:34–40; *see also id.* at 9:15–19 ("Once, the reduced vectors have been processed by the multiple clustering methodologies in block 270, one or more metrics can be selected in block 280 for purposes of establishing a correlation between the output sets of the processed reduced multi-dimensional vectors."). In contrast, the portions of Rhodes relied upon by Petitioner to address the argued limitation disclose that Rhodes detects anomalous behavior based on a correlation between input vectors, i.e., a "'comparison function' to measure 'how different two vectors are.'" Pet. 39 (citing Ex. 1004, 3); *see also id.* at 40 (citing Ex. 1004, 8 ("The most obvious measure of vector similarity is somehow aggregating the differences among their several coordinates.").

Relying on its expert, Dr. Lee, Petitioner asserts that one of ordinary skill in the art "would have understood that *Rhodes'* detection of anomalous

correlations from clusters in the self-organized map is based on a configurable correlation metric—distance." Pet. 40 (citing Ex. 1003 ¶¶ 101–102). Again, relying on Dr. Lee's declaration testimony, Petitioner concludes that one of ordinary skill in the art "would have understood or at least found it obvious that Rhodes discloses detecting anomalous correlations between individual clusters based upon a distance, such as a Euclidean distance, between clusters."). *Id.* at 41 (citing Ex. 1003 ¶¶ 101–102). Despite this conclusory statement, neither Petitioner nor its expert adequately explains how or why Rhodes's system, which at most suggests applying distances as correlations between vectors to form clusters, would have suggested applying these distances to clusters. In other words, as Dr. Lee states, and we agree, "*Rhodes* discloses a 'comparison function' to measure 'how different two vectors are.'" Ex. 1003 ¶ 101 (citing Ex. 1004, 3). Thus, we find that Petitioner fails to explain adequately why one of ordinary skill in the art would have understood Rhodes' disclosures regarding correlations or distances between vectors to refer to, or suggest, "detect[ing] anomalous correlations between . . . clusters . . . based upon at least one configurable correlation metric," as recited by limitation 1[f].

For at least these reasons, the arguments and evidence presented in the Petition fail to provide sufficient support for Petitioner's contentions that "*Rhodes* discloses or renders this limitation obvious." Pet. 39. Therefore, we determine that Petitioner has not shown a reasonable likelihood of demonstrating that independent claim 1 would have been obvious over Rhodes and McCreery.

4. Independent Claim 7

Independent claim 7 is similar to independent claim 1. Petitioner relies on its assertion for claim 1 and does not provide contentions for claim 7 that remedy the deficiency discussed with respect to claim 1. *See, e.g.*, Pet. 50 ("*Rhodes* discloses or renders obvious this limitation. *Supra*, claim 1[f] (describing how *Rhodes* discloses identifies anomalous behavior by using a 'comparison function' to measure how different two vectors are (i.e., establishing a correlation), where said comparison function is based on a 'particular distance measure')."). Accordingly, for the reasons discussed with respect to claim 1, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claim 7 is unpatentable under 35 U.S.C. § 103 as obvious over Rhodes and McCreery.

5. Claims 2–5 and 8–11

We have considered Petitioner's arguments and evidence for dependent claims 2–5 and 8–11. Petitioner does not provide contentions for these claims that remedy the deficiency discussed with respect to claim 1. Accordingly, for the reasons discussed with respect to claims 1 and 7, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 2–5 and 8–11 are unpatentable under 35 U.S.C. § 103 as obvious over Rhodes and McCreery.

E. Alleged Obviousness over Rhodes, McCreery, and Lee

Petitioner challenges claim 6 by adding Lee to the teachings of Rhodes and McCreery discussed above with respect to claim 1. Pet. 61–63. Petitioner relies upon Lee for teaching the added limitation of dependent claim 6 and, thus, does not remedy the deficiencies of the asserted art with respect to claim 1. Accordingly, for the same reasons discussed above,

Petitioner fails to demonstrate a reasonable likelihood of prevailing in its assertion that the subject matter of claim 6 would have been obvious over the combination of Rhodes, McCreery, and Lee.

F. Alleged Obviousness over Rhodes, McCreery, and Wetherall

Petitioner asserts that claim 12 would have been unpatentable as obvious over Rhodes, McCreery, and Wetherall. Pet. 63–70.

1. Overview of Wetherall (Ex. 1007)

Wetherall is titled "DETECTING AND PREVENTING UNDESIRABLE NETWORK TRAFFIC FROM BEING SOURCED OUT OF A NETWORK DOMAIN." Ex. 1007, code (54). Wetherall relates to "the monitoring and regulation of routing devices of network domains to detect and prevent undesirable network traffic from being sourced out of the network domains." *Id.* at 1:10–14. More particularly, Wetherall provides a "monitor/regulator" that "monitor[s] network traffic leaving a network domain" and "determines if undesirable/inappropriate network traffics are leaving the network domain based on the observed characteristics of the outbound and inbound network traffics." *Id.* at 1:65–2:1. Wetherall discloses a routing device that is "equipped to provide aggregate characteristic statistics on network traffics 106' routed." *Id.* at 4:25–27. Wetherall discloses that these aggregate characteristic statistics include not only "statistics for traffics of particular types routed in both the outbound and inbound directions," but "also include volume of data destined for specific destination addresses, lengths of packets, distribution of Time To Live values, and so forth." *Id.* at 4:27–46.

2. Analysis of Claim 12

Claim 12 differs from claims 1 and 7 in that it does not "detect anomalous correlations between individual ones of said clusters" or require the step of "establishing a correlation between individual output sets." Ex. 1001, 10:66–11:2, 11:40–42. Instead, claim 12 requires "establish[ing] correlations between fields of different network packets." *Id.* at 12:39–46.

Petitioner argues that claim 12 would have been obvious for many of the reasons it sets forth regarding claim 1. *See* Pet. 66–70. However, with respect to limitation 12[a], Petitioner recognizes that "*Rhodes* does not expressly disclose processing traffic destined for multiple target devices in multiple independent network domains." *Id.* at 67. To address this feature, Petitioner relies on Wetherall. *Id.* Petitioner asserts that "*Wetherall* explains its monitor/regulator 'observe[s] network traffics' and aggregate[s] statistics of network traffic or any data 'necessary to provide the desired level of granularity in discerning undesirable versus desirable . . . traffics.'" *Id.* (citing Ex. 1007, 4:38–46). Petitioner further asserts that "*Wetherall's* monitor/regulator 'monitors and regulates network traffics sourced out of multiple network domains.'" *Id.* (citing Ex. 1007, 8:20–9:36). Petitioner concludes that one of ordinary skill in the art "would have understood that the monitor/regulator (104a, 104b) regulates network traffic destined for multiple target devices in multiple network domains to detect undesirable traffic." *Id.* at 68 (citing Ex. 1003 ¶ 153).

Patent Owner does not address Petitioner's contentions regarding Wetherall. Nor does Patent Owner contest Petitioner's contention regarding whether the asserted combination "establish[es] correlations between fields of different network packets," as required by limitation 12[d]. Rather,

Patent Owner argues that Petitioner's analysis of claim 12 is deficient "because it requires 'identifying a network attack, a network fault, or a change in network performance based upon said established correlations,'" as recited by limitation 12[e]. Prelim. Resp. 15, n. 2.

> To address limitation 12[e], Petitioner asserts
>
> *Rhodes* alone or in view of *McCreery* discloses this limitation. *Supra*, Ground 1, claims 1[g], 7[f] (describing how *Rhodes* discloses an "alarm threshold" which a PHOSITA would have understood to include an identification of a network attack, a network fault, or a change in network performance when this threshold is breached).

Pet. 70.

Having considered the conflicting positions of the parties, whether Petitioner has shown a reasonable likelihood that it would prevail in challenging the patentability of independent claim 12 presents a closer question than the other challenges discussed above. Unlike claims 1 and 7, claim 12 does not require a correlation of between clusters or output sets. Claims 1 and 7 also differ from claim 12 in that claims 1 and 7 require classifying detected anomalies, whereas claim 12 simply identifies a network anomaly. Here, Petitioner has shown sufficiently that "*Rhodes* discloses an 'alarm threshold' which a PHOSITA would have understood to include an identification of a network attack, a network fault, or a change in network performance when this threshold is breached." Pet. 70; *see also id.* at 42 (citing Ex. 1004, 10 ("*Rhodes* additionally explains that 'an alarm threshold' can be established for vectors that produce sufficiently anomalous results when compared to the training vectors.")); Ex. 1003 ¶ 153.

Other than simply asserting that Petitioner's analysis is deficient, Patent Owner does not respond to Petitioner's contention that Rhodes' IDS

"identif[ies] a network attack, a network fault, or a change in network performance based upon said established correlations," as required by claim 12. Prelim. Resp. 15. However, even if we were to determine that Petitioner has established a reasonable likelihood of prevailing on its assertion that claim 12 would have been obvious over the combination of Rhodes, McCreery, and Wetherall, we do not institute trial because we find it would not be an efficient use of the Board's time and resources as discussed below.

III. DISCRETIONARY DENIAL

At institution, the Board is required to make "a binary choice—either institute review or don't." *SAS*, 138 S. Ct. at 1355. When a petition fails to meet the reasonable likelihood standard as to some challenges, the Board evaluates "all the challenges and determine[s] whether, in the interests of efficient administration of the Office and integrity of the patent system, the entire petition should be denied." *See* Consolidated Trial Practice Guide 64 (citing 37 C.F.R. §§ 316(b), 326(b)). In determining whether to institute in circumstances such as those presented here, we take into account the efficient use of the Board's time and resources. *See Deeper, UAB v. Vexilar, Inc.*, IPR2018-01310, Paper 7 at 41–43 (PTAB Jan. 24, 2019) (designated informative); *Chevron Oronite Co. v. Infineum USA L.P.*, IPR2018-00923, Paper 9 at 10–11 (PTAB Nov. 7, 2018) (designated informative).

In *Chevron*, the Board found that instituting a trial with respect to twenty challenged claims would not be an efficient use of the Board's time and resources because, in light of its decision on a matter of claim interpretation, the petitioner had demonstrated, at best, a reasonable likelihood of prevailing with respect to only two of the twenty challenged claims. *Chevron*, Paper 9 at 11. Similarly, in *Deeper*, the Board concluded

that "instituting a trial with respect to all twenty-three claims and on all four grounds based on evidence and arguments directed to only two claims and one ground would not be an efficient use of the Board's time and resources." *Deeper*, Paper 7 at 43.

Here, the Petition challenges 12 claims of the '846 patent. Pet. 1. As discussed above, Petitioner fails to demonstrate a likelihood of prevailing with respect to its challenges to at least 11 of these claims. Were we to institute review, the resulting trial would nonetheless go forward on all 12 claim challenges. We find that instituting trial, therefore, would not be an efficient use of the Board's time and resources. Consequently, we exercise our discretion to deny institution of the entire Petition under 35 U.S.C. § 314.[10]

IV. ORDER

In consideration of the foregoing, it is hereby ordered that the Petition is *denied* as to all challenged claims, and no trial is instituted.

[10] Patent Owner argues that we should exercise our discretion to deny institution of *inter partes* review in this case under 35 U.S.C. § 314(a) on other bases. Prelim. Resp. 5–12; Sur-reply 1–4. Because we decline to institute an *inter partes* review on the bases set forth above, we need not determine whether it would be appropriate to discretionarily deny the Petition under § 314(a) based on Patent Owner's arguments.

PETITIONER:
Eric Buresh
Mark Lang
ERISE IP, P.A.
eric.buresh@eriseip.com
mark.lang@eriseip.com

PATENT OWNER:
Vincent J. Rubino
Peter Lambrianakos
Enrique W. Iturralde
FABRICANT LLP

John A. Rubino
RUBINO LAW LLC
jarubino@rubinoip.com