An Evaluation of Trading Bands as Indicators for Network Telescope Datasets

Conference Paper · September 2011

CITATIONS
5

READS
300

2 authors, including:

Barry Irwin
Noroff University College
183 PUBLICATIONS **877** CITATIONS

SEE PROFILE

An Evaluation of Trading Bands as Indicators for Network Telescope Datasets

Bradley Cowie[1] and Barry Irwin[2]
Security and Networks Research Group
Department of Computer Science
Rhodes University
Grahamstown, South Africa
E-mail: [1]g06c5476@campus.ru.ac.za [2]b.irwin@ru.ac.za

***Abstract*—Large scale viral outbreaks such as Conficker, the Code Red worm and the Witty worm illustrate the importance of monitoring malevolent activity on the Internet. Careful monitoring of anomalous traffic allows organizations to react appropriately and in a timely fashion to minimize economic damage. Network telescopes, a type of Internet monitor, provide analysts with a way of decoupling anomalous traffic from legitimate traffic. Data from network telescopes is used by analysts to identify potential incidents by comparing recent trends with historical data. Analysis of network telescope datasets is complicated by the large quantity of data present, the number of subdivisions within the data and the uncertainty associated with received traffic. While there is considerable research being performed in the field of network telescopes little of this work is concerned with the analysis of alternative methods of incident identification. This paper considers trading bands, a subfield of technical analysis, as an approach to identifying potential Internet incidents such as worms. Trading bands construct boundaries that are used for measuring when certain quantities are high or low relative to recent values. This paper considers Bollinger Bands and associated Bollinger Indicators, Price Channels and Keltner Channels. These techniques are evaluated as indicators of malevolent activity by considering how these techniques react to incidents indentified in the captured data from a network telescope.**

***Index Terms*—Network telescope, trading bands**

I. Introduction

THE monitoring of network traffic entering and exiting an organization is essential for aiding in the detection of malevolent activity that may be occurring. It is vital to detect incidents as quickly as possible in order to minimize the damage to an organization's assets and reputation. Network telescopes provide a way to measure the anomalous traffic on the Internet and thus act as an early warning system and as a source of data for the post analysis of Internet wide incidents. Network telescopes are allocated a section of IP space, typically a /24 or /16 subnet, on which there are no legitimate hosts [1]. A monitor is then deployed to log all traffic destined for that IP space. It is then possible to infer that all traffic received is either malicious or due to incorrectly configured devices as there are no legitimate hosts to solicit traffic. Network telescopes have been used extensively to detect and analyse worm outbreaks such as Code Red [2], Witty [3] and Conficker [4]. While there is considerable research being performed in the field of network telescope analysis little of this work considers alternative ways to signal potential incidents. The field of technical analysis, a sub-branch of economics, makes use of a number of well researched techniques and indicators for identifying trends and potential breakouts in finical markets. This paper considers some of the trading bands techniques from the field of technical analysis. In particular Bollinger Bands, Keltner Channels and Price Channels shall be considered. These approaches are evaluated by considering the emergence of the variants of Conficker [5] and a case of distributed denial of service (DDoS) observed by a network telescope at Rhodes University.

This work was undertaken in the Distributed Multimedia CoE at Rhodes University, with financial support from Telkom SA, Comverse, Stortech, Tellabs, Easttel, Bright Ideas 39 and THRIP.

II. Paper Outline

The remainder of this paper is organized as follows. Section III considers the background related to this paper while section IV discusses the origin, nature and organization of the data to be analysed. Section V briefly discusses incidents observed by the network telescope that were used in the evaluation of the technical analysis indicators. Section VI briefly describes the technical analysis indicators that were used with sample application. Section VIII evaluates the usefulness of the applied technical analysis. Finally section IX concludes the research conducted in this paper while section X discusses related future work.

III. Background

This section describes research within the field of network telescopes, the discipline of technical analysis, the fundamentals of trading bands and provides background information on the case studies considered in section VIII.

A. Related research in network telescopes

A considerable amount of work has been conducted by the Information Security research community at large with regards to work in the field of network telescope analysis. In particular the researchers at CAIDA [6] (the Cooperative Association for Internet Data Analysis) have produced work

defining the fundamentals of network telescope analysis [7] and have observed large scale network incidents as they occurred such as the Code Red worm [2], SQLSlammer [8] and the Witty worm [3]. CAIDA researchers have also developed frameworks for creating highly distributed network telescope nodes for the monitoring and analysis of network traffic on a global scale [9]. Another organization that has made extensive use of network telescopes is Team Crymu. Team Crymu is a non-profit organization that attempts to make the Internet a more secure place by monitoring malicious activity on the Internet and alerting various agencies to potential incidents [10]. Team Crymu combine a number of their network telescopes into what is known as the "Internet Garbage Meter" [11]. This provides an indication to the level of anomalous traffic traversing the Internet.

B. Technical Analysis

Technical analysis as defined by John Bollinger, a prominent market analyst and the inventor of the Bollinger Band, as "the study of market-related data as an aid to investment decision making" [12]. Technical analysis employs indicators, techniques and trading rules that consider the current and historical direction of prices and other market related quantities in order to make better decisions with regards to the selling and buying of stocks. As the value of quantities tend to fluctuate unpredictably in the short-term, moving averages and other filtering techniques are used to smooth out these spikes in the dataset. Two of the moving averages used in this paper are the simple moving average (SMA) [13] and the exponential moving average (EMA) [13]. The forms of the SMA and EMA are given by equations (1) and (2) respectively.

$$SMA(x,n) = \frac{x_1 + x_2 + x_3 + ... + x_n}{n} \tag{1}$$

$$EMA(x,n) = \frac{2x_n - x_{n-1}}{n+1} \tag{2}$$

The concept of a loopback period is a fundamental notion used by the trading channels discussed in this paper. A loopback period is the last n periods that are to be considered as data for calculating technical analysis indicators. For example, a SMA may have a 20 day loopback period. This means that the values collected over the last 20 days will be used in conjunction with equation (1) to calculate the 20 day SMA.

C. Trading bands

Trading bands are used for a variety of different trading approaches within economics. A trading band is simply a envelope or a channel around a quantity that has been observed for a number of periods. These bands are constructed by plotting two lines that are a distance away from a quantity or a measure of central tendency for that quantity. Trading bands define a upper band and a lower band. For the most part the upper band will be above the measured quantity and the lower band will be below. The distance of these lines is dependent on the trading band type but is usually either a measure of volatility, a fixed distance or a function of some other related value [14]. The upper and lower bands could be considered as forms of support and resistance. Support, a technical analysis concept, represents the values from which a decreasing quantity struggles to descend [15]. Resistance is the opposite of this and represents the values from which the quantity struggles to continue to rise [15].

D. Conficker

The Conficker worm, also known as DownAdUp, appeared in late 2008 and has become one of the most prevalent worms to infect machines across the Internet due to technical versatility of the worm [16]. Conficker exploited vulnerabilities in the Remote Procedure Call (RPC) stack through specially crafted RPCs over port 445/TCP [17]. Conficker made use of a number of "secondary tricks" such as brute forcing network passwords, infection through removal media such as USB flashdrives and encrypted payloads. These techniques ensured the worm spread far and protected itself from external takeover [16]. It is theorized that the primary goal of the worm was to construct a large botnet that could be sold to perform illegal activities. Conficker had five main variants according to the Conficker Working Group [18]. The outbreaks of variants A to E of Conficker shall be used as case studies to observe the behaviour of the trading bands.

IV. Data collection and summarization

The data used in this paper was captured by a passive network telescope during the time period August 2005 and September 2009 at Rhodes University. Approximately 40 million packets were captured in this period. This data was processed and imported into a SQL database consisting of entries containing the relevant components of each packet header. The complete packet header was not included due to space and processing constraints. The actual payloads could not be included as the telescope used was passive implying that the telescope never responds to any packets received. From this it follows that the 3-way TCP handshake cannot be completed and hence no data transfer occurs. This data was then reduced to a smaller subset of numeric measures which provided a description of the data considering averages, medians, deviations and extrema.

V. Notable incidents observed in the dataset

It is critical to note that network telescopes are limited by the type of incidents that are observable. For example, a worm's propagation algorithm could be designed such that it will attempt to avoid scanning or infecting IPs that belong to network telescopes. Network telescopes will receive no traffic from this worm and it becomes impossible to infer from the telescope data that any incident is taking place. Much in the same way DDoS attacks are only observable if part of the network telescope IP space is spoofed resulting in ICMP type 11 messages being returned to the network telescope [19]. Having come to this conclusion it is now possible to consider cases identified in the datasets using literature and previously explored methods.

A. A case of DDoS

A common approach to performing DDoS is to spoof an IP range and then use this range to attack a host. This of course, assuming sufficient load, causes the server to stop responding to requests resulting in time-outs. These time-outs cause the generation of ICMP Type 11 packets which are sent back to the spoofed address space. Occasionally it occurs that this address space belongs to a network telescope. Figure 1 shows the occurrence of this activity between the 17th and 18th of February 2009. After some research it was shown that this was a DDoS attack directed towards a host in China. Monitoring the packet type property of ICMP provides a sample case of generally very low volume traffic with cases of extreme and sudden increase.

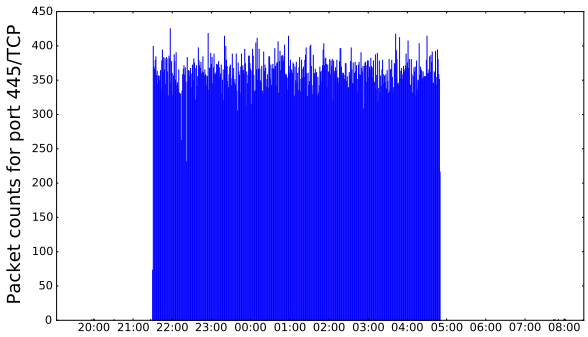

Fig. 1. Impulses depicting the sudden appearance of ICMP type 11 during the 17th and 18th of February 2009. Counts are binned at a per minute level.

B. Emergence of the Conficker variants

The Conficker Working Group have created a comprehensive time-line of the important events in the growth of the Conficker worm as agreed upon by a collection of experts involved in the analysis of Conficker [20]. Summarizing this time-line in terms of the emergence of the major variants of Conficker yields Table I. Figure 2 shows how these variants were observed by the network telescope together with the approximate outbreak of each of the variants listed in Table I. Conficker.A occurs at a time where the amount of 445/TCP traffic previously received was relatively stable. Conficker A itself represents a significant spike in the amount of 445/TCP traffic received by the telescope. Conficker.B's represents another fairly significant spike in 445/TCP following after a brief period of lower activity trailing a large spike in 445/TCP caused possibly by further scanning or hosts infected by Conficker.A attempting to infect the the IP space of the network telescope. Conficker.C marks a minor local extrema in the dataset. Conficker.D also marks a minor extrema in the dataset following on from a major extrema in the dataset. Conficker.E occurs after some stabilization of the received 445/TCP traffic and is represented by a fairly large spike in the data.

Variant Name	Date
Conficker.A	20 November 2008
Conficker.B	28 December 2008
Conficker.C	20 February 2009
Conficker.D	4 March 2008
Conficker.E	8 April 2008

TABLE I
EMERGENCE OF CONFICKER VARIANTS

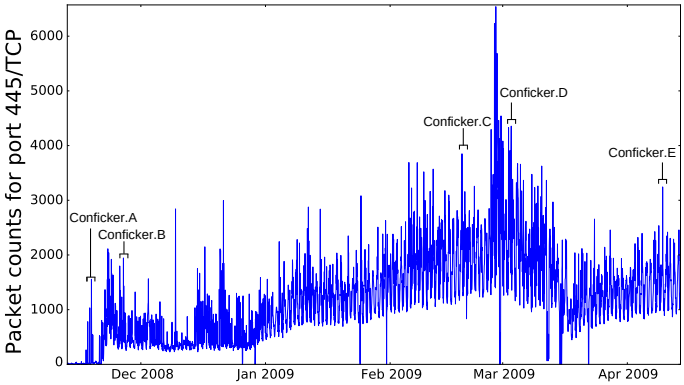

Fig. 2. Packet counts for port 445/TCP binned at a hourly level. The dates outlined in Table I are highlighted.

VI. TRADING BANDS

This section describes the trading bands that are to be evaluated for effectiveness. How each trading band can be constructed together with sample application to the network telescope dataset is provided. A short evaluation of each of the trading bands reacted to a scenario is included.

A. Donchian Price Channels

Price channels define a simple band through a set of three lines, one above the quantity, one below the quantity and the final being the midpoint between the other two lines. Let D_n denote a list of the last n values for the quantity then equations (3), (4) and (5) define the bands of a standard Price Channel with n usually considered to be 20 periods [21].

$$PC_{middle} = \frac{min(D_n) + max(D_n)}{2} \quad (3)$$

$$PC_{lower} = min(D_n) \quad (4)$$

$$PC_{upper} = max(D_n) \quad (5)$$

The typical approach to trading when using Price Channels is to observe when the commodities price rises above the previous high and then buy. When the prices drops below the previous low the trader should sell [21]. Figure 3 illustrates the application of Price Channels to data from the network telescope dataset. According to the Conficker Working Group the 20th to the 21th November is the date that Conficker.A launched. If the simplistic rule of commodity crossing the upper band is applied five signals are generated.

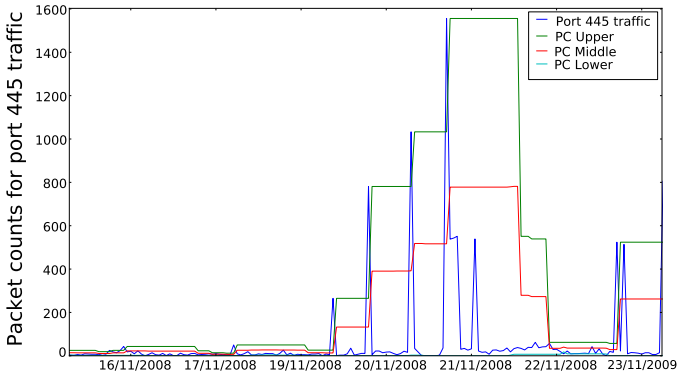

Fig. 3. Price channels for traffic received for port 445/TCP during the emergence of Conficker.A. The upper band of the Price Channel readjusts a number of times to accommodate for sudden spikes in 445 traffic.

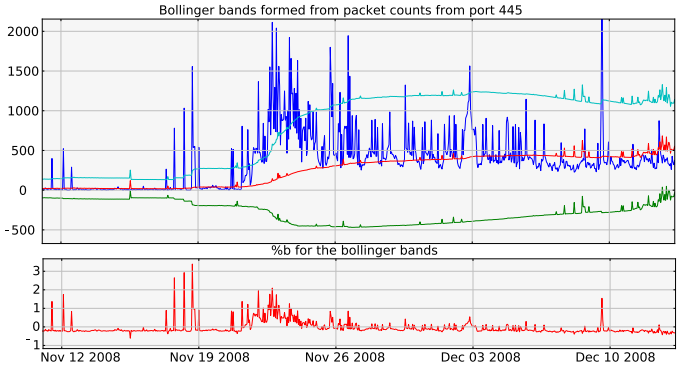

Fig. 4. Bollinger bands together with the %b indicator for traffic received from port 445/TCP. The %b value exceeds one at about the time of the Conficker.A breakout.

B. Bollinger Bands

Bollinger bands are a popular technical analysis tool that allow for a relative definition of the highness or lowness of a quantity as compared to previous values. Outside of the field of economics Bollinger bands have been used as to measure the accident rate as a safety indicator for the air travel industry and further as a method of patterned fabric inspection. Bollinger bands consist of two main components, a measure of central tendency together with a measure of volatility [12]. The commonly accepted measure of central tendency is a moving average of a quantity while the volatility is usually expressed by the standard deviation of said quantity. These two components yield three bands commonly known as the upper, middle and lower Bollinger Bands. These bands are defined by equations (6), (7) and (8).

$$B_{lower} = MA(n,d) - 2\sigma \tag{6}$$

$$B_{middle} = MA(n,d)) \tag{7}$$

$$B_{upper} = MA(n,d) + 2\sigma \tag{8}$$

Indicators that can be derived from Bollinger Bands are Bollinger Percent Band (%b) and Bollinger Bandwidth (BB). BB is defined as follows in equation (9) and %b is defined by equation (10). The %b indicator describes the current observation in relation to the upper and lower bands. When %b exceeds one the observation is above the upper band and when it is less than minus one it is below the lower band [22].

$$BB = \frac{upperBB - lowerBB}{middleBB} \tag{9}$$

$$\%b = \frac{last - lowerBB}{upperBB - lowerBB} \tag{10}$$

1) %b as a signal: When the value of %b is greater than one, the quantity has crossed over the upper Bollinger Band. Many traders use this as a signal to indicate that the quantity is oversold. While there is no directly analogous concept of oversold within the field of network telescopes the concept of crossing the band is still useful as illustrated in Figure 4. The %b indicator becomes greater than one a total of three times during the breakout time of Conficker.A and thus identifies it strongly.

2) BB as a signal: BB measures the distance between the upper and lower Bollinger Bands. As the bands narrow the BB value decreases and as the bands expand BB will increase. As Bollinger Bands make use of standard deviation an increase in BB is indicative of the volatility of the quantity. In finical markets BB is particularly useful for identifying “The squeeze". The squeeze is caused by a strong trend causing a large expansion in the band size. Eventually the trend will give way and the volatility will decrease causing the distance between the bands to be reduced. A squeeze is noted when the BB reaches a new six month low. It is assumed by most trading systems that high volatility in stocks will be followed by low volatility. This technique is used to determine which direction stocks will break out and thus buy or sell as appropriate [22]. It is possible to observe similar behaviour in network telescope datasets. For example, considerable amounts of pre-scanning activity occurs before a worm is released in order to build a list of vulnerable hosts that can be infected at the outset. Figure 5 shows an example of this behaviour. During early to late October 2008 there were suspected cases of Conficker pre-scanning. The Bollinger bands adjust to this by becoming slightly larger. Towards the end of October there are fewer spikes in 445/TCP traffic causing the bands to slowly contract causing an increase in the BB value. Approximately a month later the outbreak of Conficker.A occurs causing a decrease in the BB value.

VII. Keltner Channels

Keltner channels make use of a moving average for the measure of the central tendency and the Average True Range (ATR) provides a measure of the volatility. ATR is based upon the True Range value. True Range for a given day is defined as being the largest of the current high for the day less the current low for the day, the absolute value of the high of the day less the previous close or the absolute value of the most recent period’s low less the previous close [23]. The Average True Range is then calculated as given by equation (11).

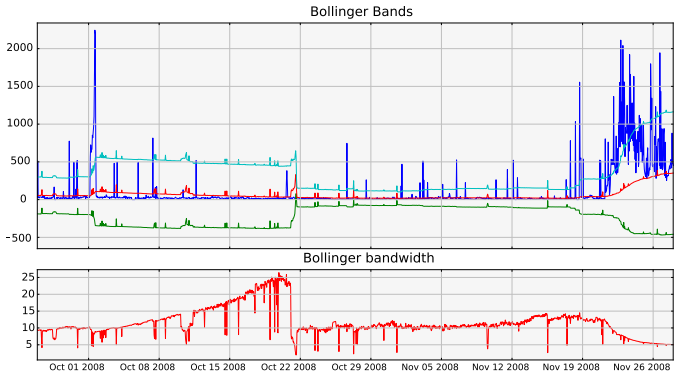

Fig. 5. Bollinger bands together with the BB indicator for traffic received from port 445/TCP. The graph shows suspected pre-scanning that occured before Conficker launched.

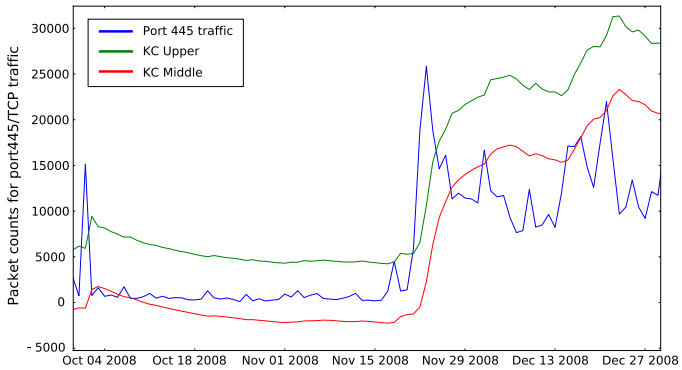

Fig. 6. Keltner channels constructed for traffic received from port 445/TCP. The bands highlight the outbreak of Conficker.A. Values were binned at a daily level.

$$ATR_n = \frac{ATR_{n-1} + TR_n}{14} \tag{11}$$

The Ketler Channel may then be calculated using equations (12) and (13).

$$KC_{lower} = MA(n,d) - k * ATR \tag{12}$$

$$KC_{upper} = MA(n,d) + k * ATR \tag{13}$$

The moving average to be considered in this paper will be a 20 day SMA and k shall be set to two. The simplistic rule of trading when the quantity crosses the channel lines is still applicable and will be the strategy of choice [24]. Figure 6 shows sample application of Keltner Channels to network telescope data. It is clear that the packet counts for 445/TCP clearly cross over the upper Keltner Channels at about the time Conficker.A emerged.

VIII. Results

In this section the techniques discussed in the previous section are evaluated using the cases discussed in section VI. Each trading band was observed at the specified cases and the output produced was considered in terms of whether it produced a visual signal that could be used to identify the incident. The results are categorized as strong identification, weak identification and failed at identification. Strong identification implies that the signal generated is clear and unambiguous. Weak identification implies that the signal hints at the possibility of a potential incidents but the signal generated is not clear. These results are summarized in Table VIII. A brief discussion of each of the trading bands with regards to the observed results is now provided.

A. Price Channels

The Price Channels combined together with the simple cross over rule identify all five cases of Conficker and the case of DDoS successfully. The rule defined is simple and easy implement and so is the construction of the bands. The bands react immediately whenever the rule comes into place but do not re-adjust until either the loopback period no longer contains the outlier or a new extrema is found. Thus bands tend to be rigid. This is a useful property for identifying incidents that occur on fairly smooth data. Price Channels have the most success in identifying incidents however they also suffered from the most over signalling. Price Channels could be seen as a measure of support and resistance within the field of network telescopes.

B. Bollinger bands and %b

Bollinger bands are far more volatile than Price Channels as the volatility is directly related to the deviation in the quantity. This property is useful when examining ports that are extremely spiky such as TCP ports 135, 139, 445 and 1433. The %b indicator provides a simple and easy to automate strategy to identify potential incidents. As the bands are more reactive, the amount of over signalling occurs is far less when compared to Price Channels. It is noted that %b failed to identify some of the Conficker variants. This is due to the fact that %b is extremely effective at identifying large spikes in the dataset but smaller spikes such as Conficker.C do not represent a significant enough change in previous readings to be registered as an incident.

C. Bollinger bandwidth

Bollinger bandwidth appears to be unsuitable for incident identification due to the fact that it is difficult to interpret this indicator when considering large spikes in the dataset. As previously mentioned BB may be a useful identifier for identifying pre-scanning.

D. Keltner Channels

The bands of the Keltner Channel appear to be far less volatile than Bollinger Bands. As a visual analysis tool Keltner Channels tend to take a while to re-adjust after a major spike in traffic. The bands seem to remain the same distance apart until large spikes are present in the dataset. Keltner Channels identified the majority of the incidents successfully and suffered minimal over signaling. With some modifications Keltner Channels could be used within the context of network telescope analysis as a incident identification tool.

Indicator	DDoS	Conficker				
		A	B	C	D	E
Price channels	Strong identification	Strong identification	Strong identification	Strong identification	Weak identification	Strong identification
Bollinger %b	Strong identification	Strong identification	Failed	Weak identification	Failed	Failed
Bollinger BB	Strong identification	Weak identification	Failed	Failed	Failed	Failed
Keltner channels	Strong identification	Strong identification	Weak identification	Weak identification	Failed	Weak Identification

TABLE II
COMPARISON OF THE ABILITY OF THE TRADING BANDS TO SIGNAL INCIDENTS OBSERVED IN THE DATASET

IX. CONCLUSION

This paper has considered a number of techniques from the field of technical analysis as applied to data from a network telescope and has shown that there is scope to apply some of the techniques and approaches from trading bands to the field of network telescope data analysis. It was found that Bollinger Bands produce effective boundary lines when used together with the %b and BB indicators to generate signals. The %b indicator was observed to be a useful indicator for identifying large spikes in datasets. BB shows potential as a possible indicator of pre-scanning activity. Price channels are useful for establishing the concepts of support and resistance. Keltner Channels were shown to be useful for identifying incidents with minimal over signaling. The work conducted in this paper lays the foundations for further exploration in the application of technical analysis techniques to network telescope datasets.

X. FUTURE WORK

The researchers plan to examine the following concepts and issues in future work :

- The loop-back period is one of the fundamental parameters to the trading bands discussed in this paper. Finding optimum values for these parameters for each trading band would improve the usefulness of the trading bands.
- Experiment with volume and momentum based indicators such as the Relative Strength Index, Moving Average Convergence-Divergence and Absolute Breadth Index.
- Consider the application of smoothing functions to the datasets to reduce the "spiky" nature of the data. Smoothing functions that maintain local extrema, such as Stravisky Golay filtering, should be prioritized.
- Development of more complex identification strategies in the same vein as the trading strategies used by market analysts.
- Form more generalized patterns that describe incidents. Similar to how W and M patterns are used in technical analysis.

REFERENCES

[1] D. Moore, C. Shannon, G. Voelker and S. Savage (2004), *Network Telescopes: Technical Report*. [On-line]. pp 1, Available: http://www.caida.org/publications/papers/2004/tr-2004-04/, [10 April, 2010].

[2] D. Moore, C. Shannon and K.Claffy, "Code-Red: A Case Study on the Spread and Victims of an Internet Worm", *IMW '02: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. pp 273–284, 2002.

[3] D. Moore and C. Shannon, "The Spread of the Witty Worm", *IEEE Security and Privacy*, vol 2, pp 46–50, 2004.

[4] R. Weaver, "A Probabilistic Population Study of the Conficker-C Botnet", *Proceedings of the 11th international conference on Passive and active measurement*, pp 181–190, 2010.

[5] US-CERT (2009, March 29), *Conficker Worm Targets Microsoft Windows Systems*. [On-line]. pp 1, Available: http://www.us-cert.gov/cas/techalerts/TA09-088A.html, [May 5, 2011].

[6] *The Cooperative Association for Internet Data Analysis*. [On-line], Available: http://www.caida.org/, [2 April, 2010].

[7] S. Payne (2006, June 19), *A Guide to Security Metrics*. [On-line]. pp 1–2, Available: http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55, [May 7, 2011].

[8] D. Moore, V. Paxson, S. Savage and C. Shannon, "Inside the Slammer Worm", *IEEE Security and Privacy*, vol 1, pp 33–39, 2003.

[9] K. Claffy, Y. Hyun, K. Keys, M. Fomenkov and D. Krioukov, "Internet Mapping: From Art to Science", *CATCH '09: Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security*, pp 47–59, 2009.

[10] *Team Crymu*. [On-line], Available: http://www.team-cymru.org/About/, [3 April, 2010].

[11] *Team Crymu Internet Garbage Meter*. [On-line], Available: http://www.cymru.com/Reach/garbage.html, [3 April, 2010].

[12] J. Bollinger, *Bollinger on Bollinger Bands*. USA : McGraw-Hill, pp 10-12, 2002.

[13] J. Murphy, *Technical Analysis of the Financial Markets: A Comprehensive Guide to Trading Methods and Applications*. New York City, New York : New York Institute of Finance, pp 199–200, 1999.

[14] J. Bollinger, "Construction" in *Bollinger on Bollinger Bands*. USA : McGraw-Hill, pp 50-51, 2002.

[15] J. Murphy, "Basic concepts of trend" in *Technical Analysis of the Financial Markets: A Comprehensive Guide to Trading Methods and Applications*. New York City, New York : New York Institute of Finance, pp 55-65, 1999.

[16] B. Nahorney (2009, June 2), *The DownAdUp Codex*. [On-line]. pp 1–3, Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf, [May 8, 2011].

[17] P. Porras and V. Yegneswaran, "A Foray into Confickers Logic and Rendezvous Points", *In USENIX Workshop on Large-Scale Exploits and Emergent Threats*, vol 2, 2009.

[18] *Conficker Working Group*. [On-line], Available: http://www.confickerworkinggroup.org/wiki/, [3 April, 2010].

[19] D. Moore, C. Shannon, D. Brown and S. Savage "Inferring Internet Denial-Of-Service Activity", *ACM Transactions on Computer Systems*, vol 24(2), 2006.

[20] Conficker Working Group (2009, April 26), *Conficker Timeline*. [On-line], Available: http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline, [3 April, 2010].

[21] *Price Channels*. [On-line], Available: http://stockcharts.com/help/doku.php?id=chart_school:technical_indicators:price_channels, [3 April, 2010].

[22] J. Bollinger, "Bollinger Band Indicators" in *Bollinger on Bollinger Bands*. USA : McGraw-Hill, pp 60-67, 2002.

[23] J. Wilder, *New Concepts in Technical Trading Systems*. North Carolina, Greensboro : Trend Research, vol 1, pp 21-23, 1978.

[24] R Colby, *The Encyclopaedia Of Technical Market Indicators*. USA: McGraw-Hill, vol 1, pp 337-340, 2002.

Bradley Cowie has obtained a BSc(Hons) in Computer Science from Rhodes University whilst under the supervision of Dr. Barry Irwin. Bradley is currently working towards his MSc in Computer Science with his research interests being in the fields of network telescope analysis and visualization.