Journal of Telecommunications and the Digital Economy

Volume 7 Issue 1
March 2019

Publisher: Telecommunications Association Inc.

ISSN 2203-1693

JTDE Volume 7, Number 1, March 2019

Table of Contents

8K Arrives

Editorial

Mark A. Gregory
RMIT University

Abstract: Papers in the March 2019 issue of the *Journal* include discussion on the National Broadband Network, technical papers on the Internet, MANET and Cloud security and a fascinating look back at the *Eucla Recorder*. The history of Australian telecommunications paper covers the Australian Post Office's involvement in the Apollo 13 emergency and a review of laser developments. In the present day, 8K televisions are set to launch in Australia on 1 April 2019 and in the process move entertainment and telecommunications into the next phase of development. The *Journal* welcomes contributions.

In This Issue

In this issue of the *Journal* papers cover public policy, new technology solutions and historical insights. The National Broadband Network is discussed in two papers that focus on how to transition to FTTP and the threat of fixed broadband services. Technology papers cover the Internet, MANET and Cloud security.

The Historical Technical News Items present two historic reprints from 1970 covering the Australian Post Office's involvement in the Apollo 13 emergency and a non-theoretical review of laser developments.

The Wireless Threat to Fixed Broadband Services provides results from a survey of broadband customers in Australia in November 2017 that showed an increasing acceptance of mobile broadband, in line with other market trends, but identified significant dissatisfaction – one quarter of mobile broadband respondents and about one third of fixed broadband respondents – with current services.

Tunnelling the Internet proposes an approach that utilises tolled priority allocated mini-tunnels to reduce regional congestion. A system that includes brokerage for access to the congestion-bypassing mini-tunnels is proposed.

A Threat Computation Model using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security proposes a novel approach to compute the

http://doi.org/10.18080/jtde.v7n1.190

probability distribution of cloud security threats based on a Markov chain and Common Vulnerability Scoring System.

How to Transition the National Broadband Network to Fibre To The Premises discusses the migration from the MTM NBN to a Fibre to the Curb or ubiquitous Fibre to the Premises (FTTP) NBN.

An Artificial Immune System-Based Strategy to Enhance Reputation in MANETs proposes an Artificial Immune System-based reputation (AISREP) algorithm to compute trust and thereby provide a resilient reputation mechanism.

The Eucla Recorder (1898 – 1900) explores the Eucla story, offering a vivid snapshot of the community's preoccupations and challenges at the end of the 19th century through the pages of its monthly newspaper, the *Eucla Recorder*.

8K Television arrives

The arrival of 8K technology in Australia changes the entertainment landscape by delivering the best possible viewing experience to local consumers. Samsung, followed later in the year by Sony and LG, will launch 8K on 1 April 2019.

8K models have four times more pixels than equivalent 4K models and provide improved contrast, brightness and picture detail.

Early adopters of 8K will find, as with all new television technologies in the past, that models will be expensive initially. The soon-to-be-released Samsung QLED 8K models include the 65-inch (1.65 m; $9999), 75-inch (1.90 m; $12,999) and 85-inch (2.16 m; $17,499).

For Australian viewers the introduction of 8K television will highlight two issues. The first is the lack of 8K content available locally other than test videos that are available through Google's YouTube. The second is the lack of modern telecommunications infrastructure in Australia that can support the high capacity, reliability and low latency needed for 8K streaming.

After spending about $51 billion on the multi-technology mix National Broadband Network (NBN) many Australians will be provided with broadband connections that will only provide access to heavily compressed, poor-quality, high definition (HD) and 4K streaming and this means that 8K streaming is likely to be delayed for some time.

While the focus is on 8K, it is timely to revisit why 3D technology has been ditched by the electronics industry. Some of the reasons for the 3D demise include vendors failing to adopt a common approach leading to a variety of 3D glasses and viewing experience, the premium

http://doi.org/10.18080/jtde.v7n1.190

price being charged for 3D televisions, 3D Blu-ray players and the need for two channels to support 3D broadcast and streamed television.

For broadcast television and streaming media providers struggling to find a way to offer standard definition (SD) and HD within the available spectrum or broadband capacity, the requirement for a second channel for 3D was insurmountable. The additional cost would need to be passed on to consumers.

The spectrum and broadband capacity limitations affecting broadcast television and streaming media has led to increased compression. Consumers are now often provided with a very poor-quality viewing experience.

Whilst it might have been assumed that the introduction of 4K would lead to the phasing out of SD broadcast and streamed media, the broadcast television and streaming media providers have doggedly stuck with the format and have resisted moving to support 4K. Live sport continues to be broadcast using the SD format, a travesty in 2019.

The introduction of 8K will put increased pressure on the local telecommunications and media entertainment industry to move beyond SD and HD and to embrace 4K and 8K as the standard formats.

However, for this to occur, the government will need to revisit spectrum allocations and the state of the NBN. High compression leading to poor quality is not a solution to this problem.

The *Journal*, Looking Forward

The *Journal* welcomes papers on the telecommunications and the digital economy, including, theory, public policy and case studies.

Technological change is happening at a rapid rate and consumers anticipate that governments and industry keep pace to ensure that the benefits can be fully utilised. The *Journal* is calling for papers on how new technologies will affect Australian telecommunications consumers.

The topics of *International Telecommunications Legislation and Regulations* and *International Mobile Cellular Regulation and Competition* are set to continue for some time, as the opportunity to attract papers from around the globe continues. We encourage papers that reflect on where the global telecommunications market is now, how it got to where it is, and what is going to happen next.

Papers are invited for upcoming issues. With your contributions, the *Journal* will continue to provide readers with exciting and informative papers covering a range of local and international topics. The Editorial Advisory Board also values input from our readership, so please let us know what themes you would like to see in the coming year.

http://doi.org/10.18080/jtde.v7n1.190

All papers related to telecommunications and the digital economy are welcome and will be considered for publication after the double-blind peer-review process.

Mark A. Gregory

http://doi.org/10.18080/jtde.v7n1.190

Historic Technical News Items

Simon Moorhead
Ericsson Australia and New Zealand

Abstract: Two historic technical news items from 1970 covering the Australian Post Office's involvement in the Apollo 13 emergency and a non-theoretical review of laser developments.

Keywords: Telecommunications, History, Apollo 13, Lasers

Introduction

These two short historical papers were published as technical news items in the *Telecommunication Journal of Australia* in June 1970.

The first paper details the Australian Post Office's (APO's) involvement in the Apollo 13 emergency in April 1970. Most readers who witnessed Neil Armstrong's historic moon walk in July 1969, on the Apollo 11 mission, would be aware of the emergency situation that befell the later Apollo 13 mission, due to an explosion in the service module.

The astronauts were able to return to Earth safely, but their rescue required an enormous effort and ingenuity by the National Aeronautics and Space Administration (NASA) and its contractors, as well as assistance from many American allies, including the APO.

The paper describes how the APO quickly deployed an AWA microwave link from the Parkes high gain radio telescope (made famous in the 2000 film *The Dish*) to the NASA tracking station at Honeysuckle Creek, because the astronauts no longer had access to powerful transmitters in the service module and Parkes could receive their weaker signals.

The APO was also asked via the American Embassy to protect from interference the communications frequencies used by the astronauts in their emergency descent. This necessitated checking the operating frequencies of all microwave systems near the flight path and either changing operating frequencies or re-routing traffic and temporarily disabling the systems.

The Apollo 13 rescue was successful and was later immortalised in the 1995 film *Apollo 13* starring Tom Hanks. Recently, in December 2018, the Special Broadcasting Service (SBS) in Australia broadcast a documentary entitled "Mission Control: The Unsung Heroes of Apollo",

http://doi.org/10.18080/jtde.v7n1.180

which featured details of many of NASA's achievements, including the moon walks and the Apollo 13 rescue.

The second paper provides a non-theoretical review of a decade of developments in laser technology. It was written by A. Tucker (Tucker, 1970) who was the Science Correspondent of *The Guardian* newspaper in London. It was supplied for publication in the *Telecommunication Journal of Australia* by the Information Service of the British High Commission.

It covers the unique properties of the laser, the short wavelengths, potential deployment in space, use for measurements where great precision is required, use for medical procedures and the possibility of transmission in glass fibres, which was yet to be perfected. It ends with the profound statement: "*one thing is certain, lasers are still in their infancy and we are only just beginning to exploit their enormous potential for human good*".

References

"Australian Post Office involvement in the Apollo 13 emergency" (1970, June). Technical news item, *Telecommunication Journal of Australia, 20*(2), 177-178.

Howard, R. (Director). (1995). *Apollo 13* [Motion picture]. USA: Universal Pictures.

Mission Control: The Unsung Heroes of Apollo [Television broadcast]. (2017). Australia: SBS – broadcast on Saturday, 30 December 2018.

Sitch, R. (Director). (2000). *The Dish* [Motion picture]. Australia: Warner Bros.

Tucker, A. (1970, June). The light with a thousand uses, Technical news item, *Telecommunication Journal of Australia, 20*(2), 179-180.

http://doi.org/10.18080/ajtde.v7n1.180

The Historic Papers

TECHNICAL NEWS ITEM

AUSTRALIAN POST OFFICE INVOLVEMENT IN THE APOLLO 13 EMERGENCY

As a result of experience with the earlier missions in the Apollo programme the arrangements used during the earlier stages of the Apollo 13 flight to interconnect the various N.A.S.A. installations in Australia by A.P.O. network circuits were well proven and could be set up and operated in what had come to be regarded as standard arrangements for Apollo missions.

However, the emergency situation which resulted from the explosion in the service module of the spacecraft led to requests being made to the Post Office by the N.A.S.A. authorities and by the U.S. Embassy for special facilities and actions which were successfully fulfilled in spite of the limited time available and the amount of office and field work involved.

The first request was made shortly after the explosion when it became necessary for the astronauts to close down communications from the command module and to work instead from the low power radio equipment in the lunar module. To maintain satisfactory communication and telemetry operations between the lunar vehicle and earth while Australian earth stations were in use it was vital that the higher aerial gain and superior receiver facilities at the Parkes radio telescope be pressed into service.

These facilities had been used on earlier missions, but with improvements in facilities in the spacecraft were not required under normal circumstances during the Apollo 13 flight. The temporary interconnections which had been used during earlier flights had therefore been dismantled.

In the emergency situation which developed on Tuesday April 14th the Post Office undertook to re-establish a broadband connection between the Parkes radio telescope and the N.A.S.A. station at Honeysuckle Creek which involved installing a microwave system between the Parkes station and the nearest Departmental microwave station at Coonambra and to also install a microwave system between the N.A.S.A. station at Honeysuckle Creek and the Williamsdale radio relay station. Existing radio bearers between Coonambra and Sydney, Sydney and Canberra, Canberra and Williamsdale also required to be interconnected to complete the circuit from Parkes to Honeysuckle Creek.

Equipment for the connection was found to be available from A.W.A. and teams of Departmental and A.W.A. staff worked overnight to complete and commission the installations by Wednesday morning.

The Department has received the following comment on its work on this project:

"The Director of manned flight support in expressing his thanks for the Australian support of the Apollo 13 mission has singled out those responsible for bringing up the Parkes antenna and associated data systems in record time. He has also stated that this response was so impressive that special mention of it was made to President Nixon during his visit to Goddard Space Flight Centre".

The second issue resulting from the emergency was raised in a Note from the Embassy of the U.S.A. on Thursday 16th April and which was receiv-

http://doi.org/10.18080/ajtde.v7n1.180

ed at Post Office Headquarters late on Thursday morning.

The U.S. Note advised details of the latest recovery plan and requested the co-operation of the Government of Australia in protection of the communication frequencies to be used by the spacecraft in its emergency descent. The Note included the following request:

"Although no radio interference has been experienced on the above frequencies to date, the Apollo 13 emergency situation is such that the United States is asking all countries to co-operate in avoiding any radio operation which might possibly interfere with reception anywhere on earth of the spacecrafts transmissions."

With less than two days available the Department undertook the work of identifying the services which "might possibly interfere", of assessing the level and effect of the interference and of considering the possible consequences of closing down the interfering services.

By late on Thursday three types of radio services emerged as interference sources:

(a) communication and radiolocation type transmissions of the Defence group;
(b) Radiolocation services ("Shoran") used by geophysical survey parties;
(c) trunk line radio systems operated by the Post Office.

The transmissions under control of the Defence Department were immediately regulated by signals from Canberra to all Services and to the Supply Department prohibiting transmissions on all N.A.S.A. operating channels and on potentially interfering channels until after splashdown.

A State by State (including New Guinea) check of the operations of Shoran users was undertaken and the controlling operators and ten field parties using this facility were asked to cease Shoran operations until after the return of the Apollo 13 spacecraft. One operator was located in West Irian which is beyond the range of Australian control but his agreement was nevertheless received to a request to stop transmissions during the emergency.

The greatest area of potential interference arose from the use of frequencies closely adjoining the spacecraft frequencies by the trunk line microwave radio systems of the Post Office and also by microwave radio systems operated by the Post Office and Commercial television companies to relay television programmes from television studios to the associated transmitting stations.

As studies continued it became apparent that many of these systems lay close to the track to be taken by the spacecraft on the last stage of its descent, while others were capable of interfering with reception in the special aircraft which were to be deployed along the recovery track to act as radio relay stations.

As the location of the aircraft and likely track of the spacecraft became known a hard core of about 50 microwave links emerged as the most troublesome.

By changing from "working" to "standby" frequencies some of the interference sources could be eliminated while in some cases the radio system could be closed down without serious effect upon trunk telephone traffic.

In the case of television relays, changes to alternative frequencies required the use of temporary systems in view of the short time available and the difficulty of retuning working equipment for operation on another frequency. As all National and most Commercial television stations proposed staying open all night to transmit the satellite television relay from the recovery area it was imperative that no television relays be dislocated. Two particularly difficult situations arose from this requirement.

The microwave radio systems in use between Sydney and the satellite earth station at Moree in northern N.S.W. and between Victoria and Tasmania via Flinders Island were very serious sources of interference. Both these links were critical in distributing the satellite relay which was to be received at Moree and relayed to all States by the Post Office broadband network.

By closing down the offensive channel on the Moree-Sydney system and operating on the protection bearer, with staff in attendance to remedy any faults that might occur, the satellite transmissions were successfully relayed without risking interference to the spacecrafts transmissions.

In the case of the Victoria-Tasmania radio system, telephone traffic (which was not high in the early hours of Saturday morning) was re-routed via King Island, the offending bearer was closed down and the remaining bearer was used for the television relay to Tasmania.

The cessation of transmission on all of the frequency assignments which were finally listed as potentially dangerous sources of interference to the critical descent and recovery of the spacecraft was completed by late in the evening of Friday April 17 some hours before the onset of the critical phase of the descent and all services were restored to normal during Saturday morning after the astronauts had "splashed down" safely.

http://doi.org/10.18080/ajtde.v7n1.180

THE LIGHT WITH A THOUSAND USES*

Looking back over the decade since the invention of the Laser (Light Amplification by the Stimulated Emission of Radiation) it seems surprising that for the first two or three years of its existence it was dubbed 'a solution in search of a problem'.

Like the Maser (the M is for Microwave—the rest of the acronym is the same), the laser is a device for generating an extremely narrow and powerful beam of electromagnetic waves.

The maser grew out of a need for very powerful microwave beams for communication purposes on earth and for the progress of radar systems both in defence and in space and astronomy research.

But whereas the maser fitted straight into an existing technology and a pre-defined purpose, the laser—producing visible light whose energy over the cross section of its tiny beam could be a million times as powerful as a sunbeam of the same area—was a development that seemed bizarre rather than useful.

Unique Properties

But the ingenuity of men is such that no potentially useful device, however bizarre, goes unused for long.

While physicists worked steadily on the laser to give it greater power or different wavelengths of operation, the physicist-engineers of our age of electronics and automated medicine looked hard at the unique properties of the new invention.

First, it produced electromagnetic waves which—like the waves you tune in to on the radio—were 'coherent'.

This is simply the physicist's word for 'in step', and in this instance it meant that the visible light not only had extreme purity of colour but that, like radio waves, it was an electromagnetic emission to which a receiver could be tuned.

A signal of other frequencies could be imposed on it and detected at the receiving end.

Now, a laser beam is so narrow and spreads so little that, if sent to the moon 240,000 miles away, it is only half a mile or so wide when it gets there.

Ordinary radio waves can be beamed to some extent, but this accuracy of beaming offers advantages of a kind unthought of in ordinary radio.

Value of Secrecy

First, there is the potential value of secrecy: such a beam can be directed at a particular receiver. Second, and perhaps more important, such a beam loses its power much more slowly with distance than other kinds of electromagnetic transmission.

In other words it offers a chance both of communicating over very great distances in space and also of measuring great distances accurately because again the reflected signal retains its energy more successfully than waves of lower frequency.

It is very much to the credit of India's technology, and to the vision of the late Dr. Homi J. Bahbah, that one of the first successful laser communication systems in the world operated between the Atomic Energy Commission headquarters in Bombay and the research centre out at Trombay. The distance—about 15 miles—may seem small, and in fact points to a serious snag in this most promising theoretical possibility.

Fairly Short Range

This is that, on earth, the atmosphere absorbs and scatters the energy of a light beam and even using the light at its most penetrating infrared frequencies (we cannot see infrared light but we feel it as warmth), the possible range for communication on earth is fairly short.

But this is also true of microwave beams (typically a microwave beam has a wavelength of a few centimetres, a radio signal has a wavelength of anything from a few metres to several thousand metres, while a laser beam's wavelength is a few thousandths of a millimetre!) and in that case the problem is not important because the receiver has to be in a direct line of sight.

The fact that the surface of the earth is curved and that high frequency radiation travels in a straight line means that the range is necessarily limited.

Why cannot lasers be used in place of microwaves, so that advantage can be taken of their higher frequency and therefore inherent ability to carry more information? The answer is that mist, rain and even smoke particles interfere with a light beam much more seriously than with a beam of longer wavelength.

A good analogy here is that you can shout through a forest successfully because the diameter of tree trunks is small compared to the wavelength of sound. But you could not shout through a forest of gasometers because the obstructions are of a similar size to the wavelength of sound and therefore absorb and reflect the noise energy. Smoke particles look like gasometers to light waves!

Space Role

So it seems that, as far as communications go, the laser will find its greatest use in space, although in Britain, the United States of America and elsewhere, experiments are being pushed forward with the idea of 'piping' laser light inside tiny glass fibres.

This is rather like sending sound down a tube—the traditional basis of ship's speaking tube communication systems—although on an extremely miniature scale. The light simply reflects off the internal surface of the glass fibre whenever there is a bend and is steered to the fibre's end.

Since glass is cheaper than wire, and since a light beam could carry several thousand simultaneous voice communication channels, there is a potential application of lasers which could revolutionise telephone communications and lead to very much lower costs.

Again the problem lies in developing glassy materials which absorb none of the light.

That has not yet been achieved anywhere, nor is a real solution in sight.

Another Potential Use

Accordingly, you could say that, in the communications field, the laser remains promising rather than useful, but the very fact that it is reflected by smoke particles or water droplets opens up another potential use, one which has already led to the development of very advanced equipment by instrument makers in Britain.

As in radar, or any other pulsed signal system where you can measure the time taken for a reflected pulse to return to the sender, a laser beam can be used for the measurement of range.

Because a laser has such a very short wavelength the measurement can be extremely accurate—as has been shown by the possible engineering applications developed by Britain's National Physical Laboratory at Teddington, 13 miles south of London. But, with much longer ranges in mind, the laser beam is also partially reflected by clouds.

Partial Reflection

The 'partial reflection' is important for it means that, in meteorological use, it is possible to direct a beam upward and get not only a measurement

* This non-theoretical review of a decade of developments in LASER technology written by A. Tucker, Science Correspondent of 'The Guardian' (London) was supplied by the Information Service of the British High Commission.

http://doi.org/10.18080/ajtde.v7n1.180

of the height of the lowest cloud layer, but also still fainter detectable measurements of a whole series of upper cloud layers that are invisible from the ground.

This measurement of the vertical structure of cloud systems is of importance to the forecaster and the technique has the advantage of also showing—by the degree of absorption of light—the density of the invisible cloud layers.

In a world occasionally worried by the potential threat of more sinister clouds, those of chemical or biological droplets being used as weapons, it is comforting to know that this radar technique can spot a spraying aircraft very easily, by day or night.

Further, because of its accuracy, laser rangefinding can be used to detect the tiny movements which precede a slippage in an opencast mine, an earthquake tremor or a geological fault, or the variation in distance of celestial objects like the moon.

Indeed, among the first objects left on the surface of the moon by men will be a laser reflector designed to provide astronomers with the most accurate measurements of the moon's wobbly orbit they have ever had.

Power Density

These uses, like that of employing a laser beam as a guide of straightness when making long tunnels, lean on only some of the laser's properties. But the most striking property of all is that of power density. A laser beam is capable of vaporising any material on earth.

Small boys are prone to play with a magnifying glass in such a way that the focused rays of sunlight burn holes in wood or plastic. The laser beam can be a million times hotter, a property which sounds, and certainly is, dangerous but which can be turned to a number of extremely valuable uses.

In fine engineering and in modern electronics—particularly in the manufacture of the latest tiny micro-miniaturised components—there is a need for etching, cutting and boring techniques on a scale far too small for conventional tools. Now a laser beam can have a diameter as small as a hundredth of an inch and can easily vaporise hard metals and metals or materials like gold or silicon used extensively in electronics.

It is, therefore, not surprising that for special tasks of etching circuit designs, punching tiny holes or cutting very refined shapes, the laser has already established itself as a technique of major importance. Its power can be controlled very accurately, as can its guidance, and both can be automatically controlled and 'programmed' for use on a production line.

Further, the technique can be used for carrying out welding on a scale much smaller than any known before. But welding and cutting accurately are activities by no means confined to engineering. For reasons that are not yet fully explained the laser beam affects living cells in a curiously clean way. Its damage is very closely confined to its point of impact.

Can Help Surgery

This means that it could become a valuable tool in surgery, offering the medical profession refinements of technique that are available in no other way. Already in Britain, International Research and Development at Newcastle upon Tyne, in the north of England with the backing of the National Research Development Corporation and the electronics firm of Elliot-Automation, have developed very small portable laser surgeon's welding tools which have been used in the treatment of a condition known as 'detached retina'.

The retina is the sensitive curved region at the back of the eye on which the image falls and is processed by the nervous system. Some diseases, or age alone, can lead parts of this very delicate area to separate from supporting tissue so that sight is either damaged or lost.

Re-attachment can be carried out in several ways but it has been found that a tiny burst of laser light—which does no damage to the clear lens of the eye through which it has to pass—forms a tiny and neat weld at the point at which it strikes the retina. The process is so simple and painless that it has immense promise and is already being used experimentally in several hospitals.

Equally there is promise that the laser will be valuable in excising surface tumours, for it creates an incision that is sealed, thus markedly reducing the likelihood of tumorous material entering the bloodstream and being distributed round the body.

Further, since laser light can be 'piped', there is a chance that it might eventually be used through flexible glass-fibre bundles for delicate treatments internally.

So, already, there is a very wide range of uses for this curious device which depends on making light buzz up and down inside a tube with reflecting ends and of such a length that the light's journey-time resonates at the natural molecular frequency of the material through which it is passing.

If that material is continually 'excited' by the addition of energy, the added energy will be given off as light each time the internally reflecting bunch of light waves passes by.

Great Precision Needed

In this way the energy of the 'bunch', whose frequency is that of the material, increases step by step and, if the mirror at one end is momentarily removed, will leave the tube as a burst of laser light.

If one of the end mirrors is only partially reflecting, then a continuous beam of lower energy will be emitted and different materials and tube lengths lead to laser light of different wavelengths. The engineering precision needed to make a laser of high efficiency is very great, but the truth is that if you put mirrors of the right kind on the ends of a neon light tube you would have a laser of sorts.

That it took half a century for the tubular gas-discharge lamp to evolve into something far more powerful and yet only a few years for the more powerful development to find a host of uses, is an indication of the strangely erratic development of science and technology.

One thing is certain, lasers are still in their infancy and we are only just beginning to exploit their enormous potential for human good.

http://doi.org/10.18080/ajtde.v7n1.180

The Wireless Threat to Fixed Broadband Services

Nigel Pugh
Managing Director, Venture Insights

Abstract: This paper provides results from a survey of broadband customers in Australia in November 2017. Respondents included both NBN customers and non-NBN broadband customers. The survey showed an increasing acceptance of mobile broadband, in line with other market trends, but identified significant dissatisfaction – one quarter of mobile broadband respondents and about one third of fixed broadband respondents – with current services. Factors that may affect a decision to switch from fixed to mobile broadband, or *vice versa*, included price, reliability, bundling of phone with broadband, and the capability of streaming video on demand. Negative perceptions of the NBN are also significant. Overall, we identify that about 30% of existing fixed broadband households would consider switching to a wireless broadband service. We also note the future rollout of 5G wireless service and the resultant market positioning of telcos, which may support further positive perceptions of wireless broadband.

Keywords: Fixed-mobile substitution, Fixed wireless, Australian market

Introduction

Advances in mobile broadband technologies combined with increases in smart device penetration have delivered significant growth in wireless broadband usage. As consumers rely more and more on wireless broadband connectivity, specific customer segments may look to cut their fixed broadband connection and rely solely on wireless devices for broadband connectivity.

Fixed to mobile broadband substitution may therefore threaten the viability of fixed networks by reducing the overall fixed customer base. This risk has been recognized in Australia's NBN Co (which is currently rolling out a fixed broadband access network to most Australian premises), where NBN Co's chairman, Dr Ziggy Switkowski, has been quoted as saying "wireless broadband will be a legitimate alternative to fixed broadband in the 2020s for some applications – more than we may have assumed 5 years ago" (Switkowski, 2017). The Australian Competition and Consumer Commission (ACCC) has also highlighted the potential of 5G to increase fixed to mobile and wireless substitution (ACCC, 2018a, chapter 6). More

http://doi.org/10.18080/jtde.v7n1.178

recently, Optus launched its 5G fixed wireless broadband service aiming for an initial 47 Fixed Wireless sites by March 2019 (Optus media release, 31 January 2019) and Telstra highlighted 5G fixed wireless broadband use cases in its 5G update (Telstra 5G Update, 5 December 2018).

To examine the issue of fixed to mobile broadband substitution in more detail, Venture Insights conducted an Australian consumer market survey to investigate the:

- Current level of mobile substitution for broadband services;
- Current level of satisfaction with fixed and wireless broadband services;
- Willingness to move from fixed to wireless broadband services.

The survey was conducted online in November 2017 and was composed of a nationally representative sample of 1,446 broadband households. The survey data collection was co-funded by Venture Insights and the ACCC. In addition to questions about broadband connections (as described in the next section) and broadband usage, we also collected data on location (postcode), household size, household income, type of dwelling (house or apartment) and whether the premises were owned or rented.

Broadband Connections

To understand the range of household broadband services in use, respondents were asked to categorise their primary household broadband connection. Of the 1,446 households, 911, or 63% of the total (the 'non-NBN group'), had a broadband connection not supplied by NBN Co and 535, or 37% (the 'NBN-connected households'), had an NBN connection.

For the non-NBN group, the key access types were ADSL or ADSL2 (70%), Hybrid Fibre-Coax (HFC) (13%), Fixed Wireless (5%) and Mobile only services—3G/4G (10%). This distribution is shown in Figure 1.

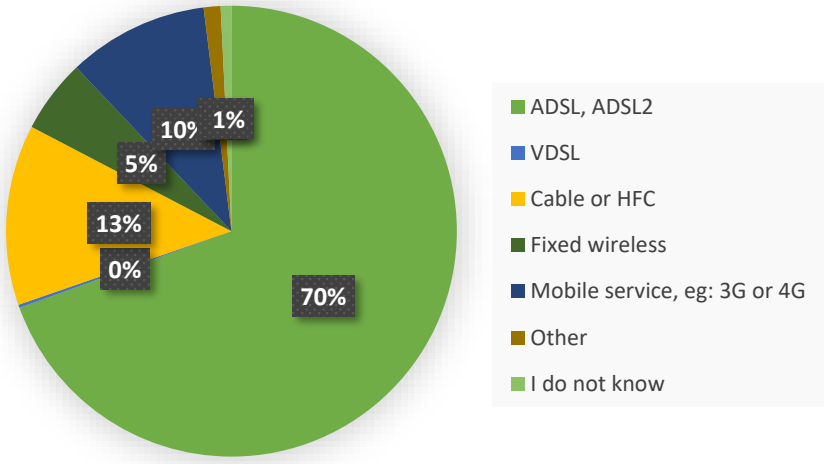

Figure 1. Non-NBN respondents' primary household broadband connection type (Source: Venture Insights Survey, November 2017, n=911)

http://doi.org/10.18080/jtde.v7n1.178

In this group, 92 respondents – or 6.4% of the total survey sample – claimed to rely on mobile broadband (3G/4G) only. For these respondents, the key demographics were skewed towards (i) lower household income brackets, (ii) the rental market, (iii) regional locations, and (iv) living alone. In addition, 95% of these respondents indicated that their usage was less than 200 GB per month. These results suggest that price of broadband is an important consideration for these households, in addition to the convenience of wireless if moving house (rental market) and low data usage not justifying having both fixed and mobile broadband connections.

For the NBN-connected households, the key access types (shown in Figure 2) were Fibre to the Premises (FTTP) (32%), Fibre to the Node (FTTN) (37%), HFC (4%), Fixed Wireless (9%) and Satellite (6%). In this survey, the Fixed Wireless category may be slightly overestimated, because respondents may have confused Fixed Wireless with fixed Wi-Fi in the premises. We checked that all respondents who claimed to be connected via NBN Fixed Wireless were located within an NBN Fixed Wireless coverage area and excluded those respondents who were not.

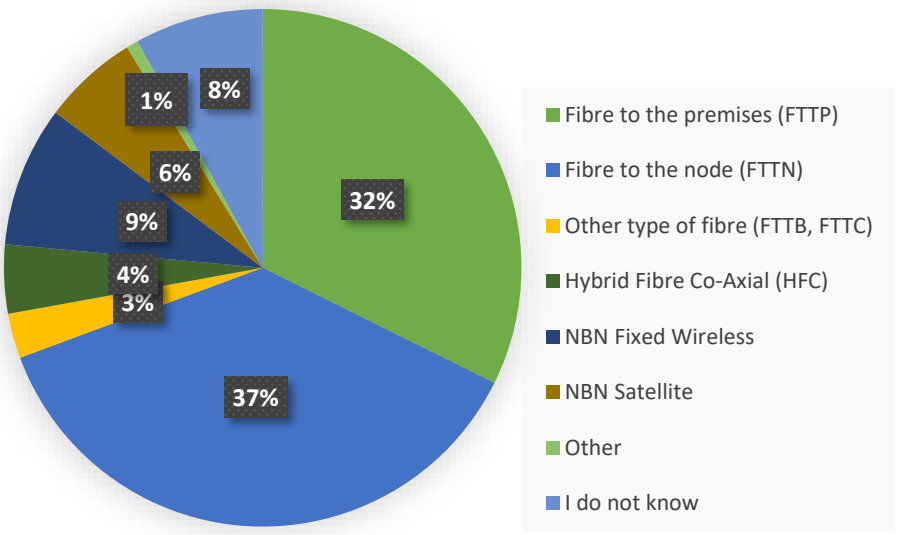

Figure 2. NBN-connected households' primary household broadband connection type (Source: Venture Insights Survey, November 2017, n=535)

Fixed Wireless and satellite services (both NBN and non-NBN) represented 8.8% of the total sample size. (Venture Insights includes Fixed Wireless and Satellite broadband services in its annual forecasts of fixed broadband in the Australian market.)

It is also worth noting that, of the total fixed broadband respondents (NBN and non-NBN), 50% estimated that their monthly data usage was less than 200 GB. This represents a large segment of the fixed market that could potentially be serviced by wireless solutions.

http://doi.org/10.18080/jtde.v7n1.178

The Australian Market Background

Figure 3 shows Venture Insights' market estimates of fixed broadband take-up in Australia since 2010. The estimates show a steady increase, especially over the past five years, to approximately 81% of households in 2017. When we add in the mobile-only broadband homes from the recent survey, the total household broadband take-up rate becomes 87.4%.

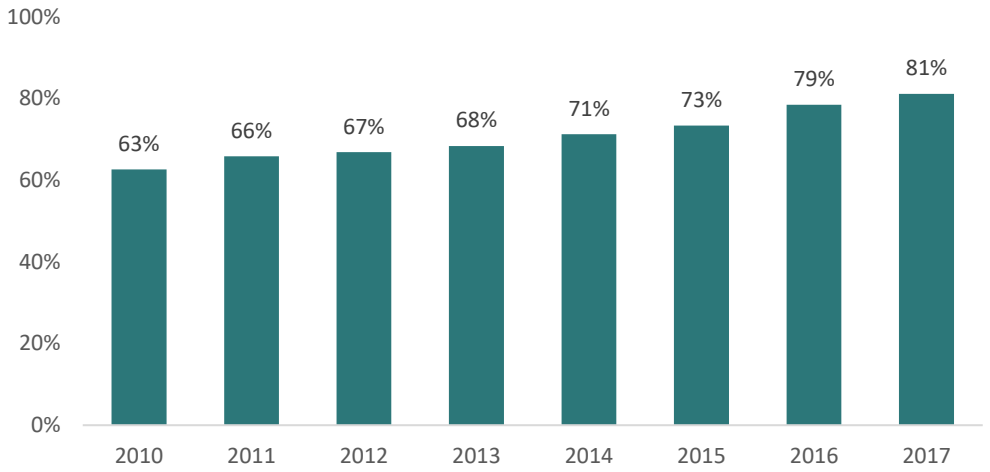

Figure 3. Australian fixed broadband take-up (% of households)
(Source: Venture Insights)

The popularity and growth of fixed broadband penetration is driven by several factors:

- **Netflix effect:** Between 2015 and 2017, there has been strong take-up of subscription video on demand (SVOD) by subscribers and households (see Figure 4), driven by the rise of SVOD providers such as Netflix. This has also driven data usage, since many households are often viewing separate video streams on multiple devices at the same time.

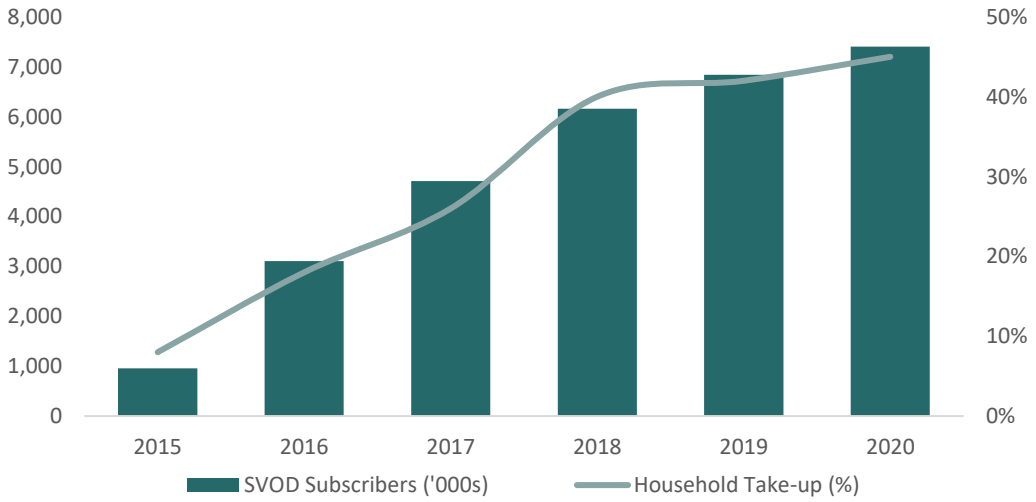

Figure 4. Subscription Video on Demand take-up in Australia
(Source: Venture Insights)

http://doi.org/10.18080/jtde.v7n1.178

- **Connected devices:** The number of connected devices per household continues to grow and includes PCs, smart TVs, tablets, music streaming devices such as Sonos, digital assistants such as Google Home, smartphones and home security devices. We expect the number of devices per capita to grow to 9.5 by 2021 (from 5.5 in 2015 – Cisco, 2017) thereby continuing to position the broadband router and the fixed broadband connection as the work hub for the home.
- **Affordability:** There are a range of price competitive plans, with many plans offering unlimited data. In the past year, fixed broadband prices have reduced between 5%-30% depending on the plan and provider. Figure 5 shows some fixed broadband prices in Australia offered by retail service providers.

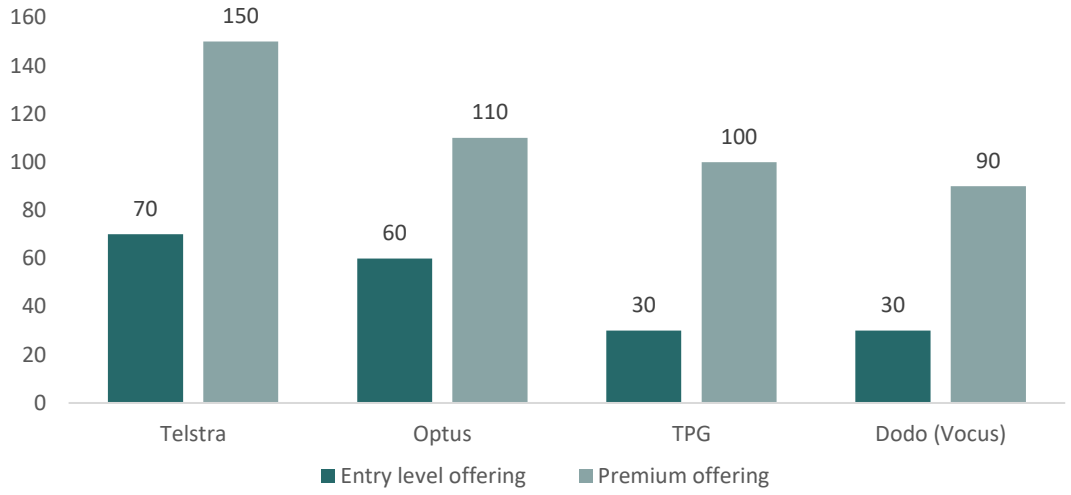

Figure 5. Fixed broadband pricing by Australian Retail Service Providers (as of October 2017) (AUD per month)
(Source: Venture Insights, Retail Service Provider websites)

The above drivers for fixed broadband growth indicate a strong need for affordable and reliable broadband services which allow for growing data usage. Unlimited data allowances would provide peace of mind for broadband consumers, but note that, as indicated above, 50% of the total fixed broadband respondents (NBN and non-NBN) estimated their data usage at less than 200 GB per month.

Fixed-Mobile Substitution

We asked our survey respondents about their level of satisfaction with their current service and about their reasons for considering, or not considering, a change to an alternative broadband technology. The survey identified a number of factors, including perceptions of the National Broadband Network (NBN), that may influence consumer behaviour in choosing a broadband access service.

http://doi.org/10.18080/jtde.v7n1.178

From Fixed to Mobile

When asked about their level of satisfaction with their fixed broadband service, 67% of fixed broadband respondents indicated they were satisfied with their household fixed broadband service, leaving 16% as neither satisfied or dissatisfied and another 17% as fairly or very dissatisfied. Of the total fixed broadband customers, 16% indicated they were considering cancelling their fixed service and switching to a wireless service within 2 years and 14% indicated they would consider switching to wireless when they were migrated to the NBN. Figure 6 below lists the reasons for wanting to switch to wireless, with the key reasons being:

- Concerns over the NBN;
- Wireless faster than their fixed connection;
- Wireless is cheaper;
- Portability.

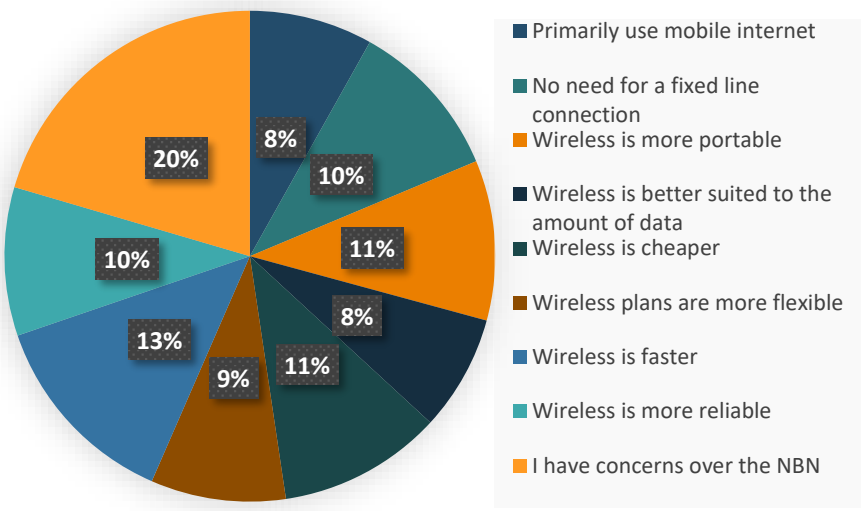

Figure 6. Fixed broadband respondents' top 3 reasons for considering switching to wireless broadband (Source: Venture Insights survey, November 2017, n=346. Each respondent selected top 3 reasons; percentages indicate total responses.)

Conversely, the key reasons for fixed broadband respondents not considering a switch to wireless (Figure 7) were:

- Keeping their fixed phone/broadband bundle;
- Reliability of fixed service;
- Fixed is cheaper;
- Fixed is faster.

http://doi.org/10.18080/jtde.v7n1.178

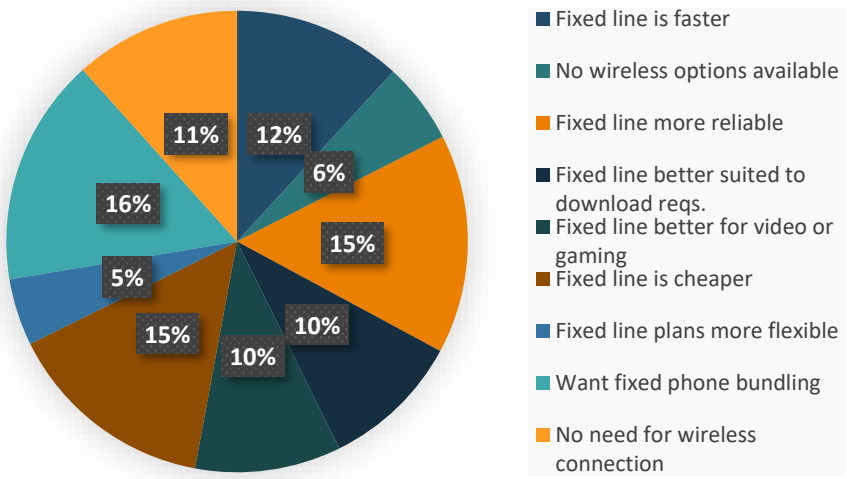

Figure 7. Fixed broadband respondents' top 3 reasons for not considering switching to wireless broadband (Source: Venture Insights survey, November 2017, n=816. Each respondent selected top 3 reasons; percentages indicate total responses.)

The fixed broadband respondents who raised concerns about switching to NBN reflect a rise in customer complaints (in line with a rise in NBN connections) to the Telecommunications Industry Ombudsman (TIO) and the associated media coverage. Figure 8 shows that TIO complaints increased by more than eight times from 2014 to 2017 but have levelled off with marginally fewer complaints in 2018.

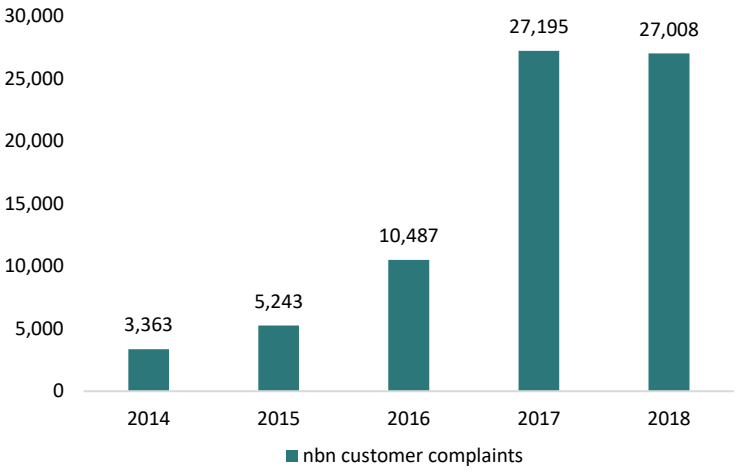

Figure 8. Consumer complaints about the NBN (Source: Telecommunications Industry Ombudsman)

As a result of the rise of consumer complaints, the Government asked the ACMA to look into the issues around the NBN. In August 2017, the ACMA began a program of work to gather information to better understand the type, incidence and cause of the problems consumers face when migrating to and using the NBN. A report on key findings was issued in December 2017 (ACMA, 2017a). In December 2017, the ACMA announced a suite of new telco rules (to be in place by 1 July 2018) aimed at improving the customer experience (ACMA, 2017b).

http://doi.org/10.18080/jtde.v7n1.178

In addition, the ACCC has initiated the Measuring Broadband Australia (MBA) program which will source internet performance data from customers of retail service providers across Australia. The third report of the MBA program was issued in November 2018 (ACCC, 2018b). The MBA program will allow customers to compare broadband speeds delivered in peak and off-peak, which will enable customers to make better choices.

Interestingly, both survey groups — fixed broadband respondents who are interested in switching to mobile and those not interested in switching — raised the same (but opposite) reasons: wireless being cheaper vs fixed being cheaper; and wireless being more reliable vs fixed being more reliable. As a result, it is clear there are differing views on the benefits of mobile versus fixed broadband technologies: this will likely reflect the lack of uniformity in coverage and quality issues within both technologies and other factors such as types of internet usage and time of day.

Whilst this may ultimately mean customers may have to experience both technologies before being able to make an informed comparison, these differences, combined with a willingness to switch, indicate that new wireless broadband services will be able to gain market share from fixed services. Whilst we do not believe wireless will be a replacement for fixed broadband services, it is clear that specific customers segments are at risk.

The differing views on the benefits of mobile versus fixed broadband technologies also highlight:

- the opportunity for telcos to further communicate their service capabilities; and
- that NBN must continue to focus on resolving its perceived quality issues, while also ensuring a competitive product roadmap is in place for future broadband products.

From Mobile to Fixed

Of the current wireless broadband respondents, 75% indicated they were satisfied with their wireless broadband service (compared with 67% for fixed broadband respondents). The satisfaction rate reflects the growing use and acceptance by consumers of accessing the internet through devices such as smartphones. More than 80% of Australia's adult population now use smartphones, up from just under 65% four years ago – see Figure 9.

http://doi.org/10.18080/jtde.v7n1.178

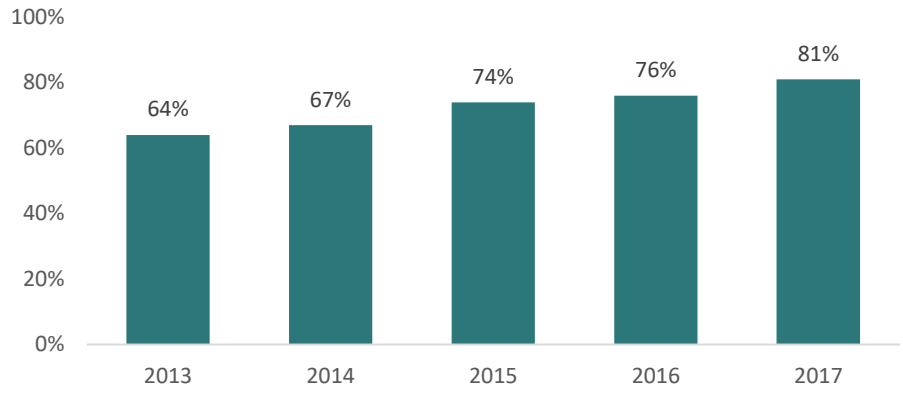

Figure 9. Smartphone take-up (% of Australian adults)
(Source: Venture Insights, ACMA)

Mobile internet traffic has grown by nearly 9 times over the last four years (see Figure 10), reflecting customers' increased consumption of video content on mobile through SVOD apps and rising video content on social media (especially Facebook and YouTube).

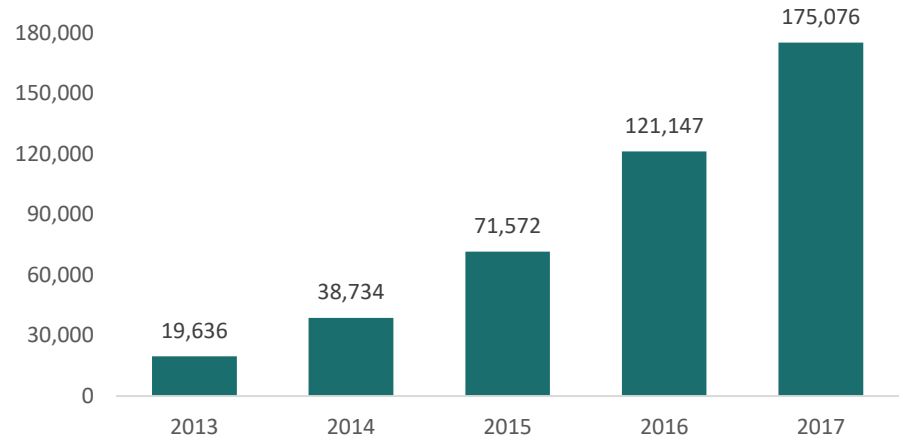

Figure 10. Internet traffic – mobile handset only (Terabytes)
(Source: Venture Insights, ACMA)

However, of the dissatisfied wireless broadband customers, the key reasons given were: (i) monthly costs; (ii) unreliability; and (iii) data allowance. In addition, 14% indicated they were considering cancelling their wireless service within 2 years (to switch to fixed) and 9% indicated they would consider switching to fixed when they were migrated to the NBN (or when the NBN becomes available). The key reasons (see Figure 11) for considering a switch to fixed were:

- Streaming (e.g. Netflix) – which reflects the increase of SVOD, discussed above, and simultaneous streaming to multiple devices within the household;
- Price – which is likely to be linked to the next issue of increased data consumption;
- Data allowance – reflecting increases in streaming requirements or changes in household consumption patterns;

http://doi.org/10.18080/jtde.v7n1.178

- Fixed phone bundling. This is interesting as the trend towards cutting the fixed phone has been increasing over time and bundling is the key reason why fixed phone disconnections are not increasing more rapidly.

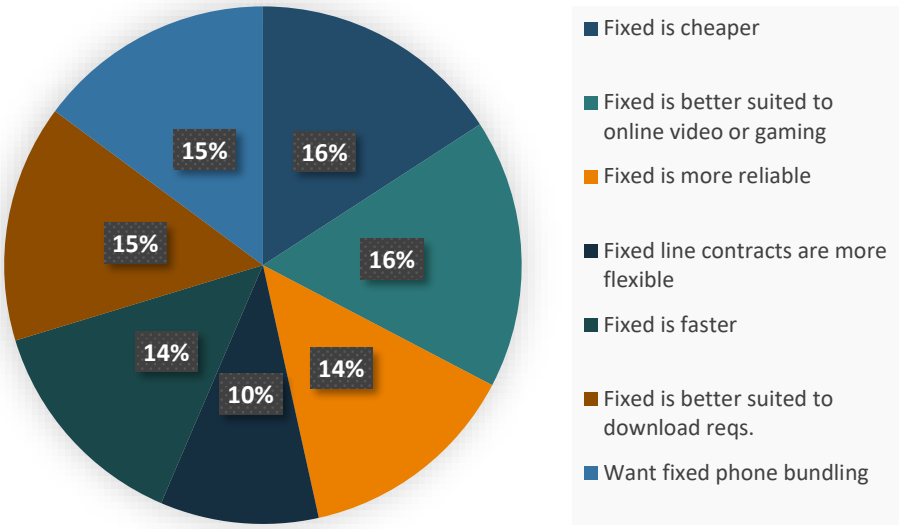

Figure 11. Wireless broadband respondents' top 3 reasons for considering switching to fixed broadband (Source: Venture Insights survey, November 2017, n=50. Each respondent selected top 3 reasons; percentages indicate total responses.)

Conversely, the key reasons for not considering a switch to fixed were: (i) no need for fixed; (ii) portability; (iii) concerns with the NBN; and (iv) no fixed-line options available.

Similar to the fixed broadband respondents' reasons for switching/not switching, there are clearly differing views of the capabilities and experience of the two technologies. The actual trade-offs between fixed and wireless speeds and price points may in practice be different from the respondents' answers. However, the consumer view of wireless being a potentially better product for some respondents, combined with some negative perceptions of the NBN product (for both sets of respondents), will enable competitor fixed wireless and mobile only products to gain market share, especially if the negative perceptions of the NBN are not addressed.

Advances in Mobile Technology – 5G

With the planned rollout of 5G mobile networks across all mobile network operators in Australia, we can expect increased marketing and positioning of 5G services as providing an even better experience than 3G and 4G services across a range of factors — see Figure 12.

http://doi.org/10.18080/jtde.v7n1.178

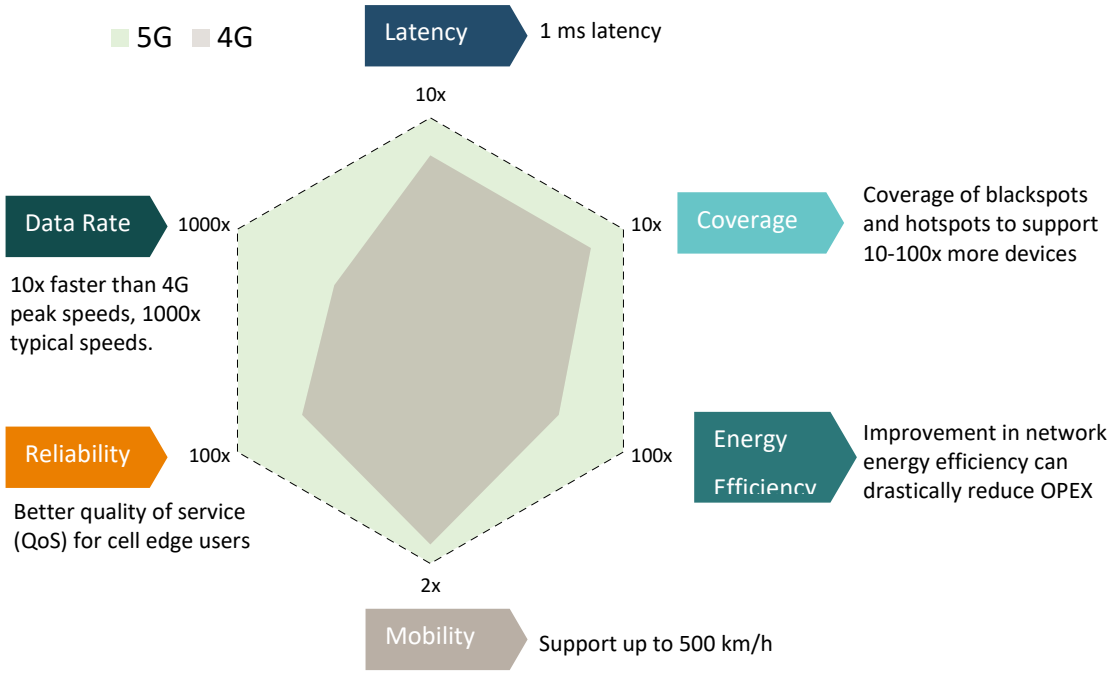

Figure 12. Performance metrics – 5G versus 4G (Source: Venture Insights)

We expect that, over time, the difference in capacity between mobile and fixed Internet will diminish, making mobile a more viable universal Internet access solution for many users. Thus, whilst 5G will initially continue to complement fixed broadband, over time it may erode fixed broadband market share. This, of course, will depend on the operators' design of the 5G network (small cell sizes, spectrum availability etc.) and the usage requirements of customer segments (for example, a large family actively using a range of internet services and applications versus low usage individuals or households).

Market positioning for 5G

There is a range of activity in the Australian market as operators position themselves for the launch of 5G networks and fixed wireless broadband solutions. Optus has launched its 5G fixed wireless service, Telstra has highlighted 5G fixed wireless broadband use cases and Vodafone has indicated they are looking at fixed wireless alternatives – subject to NBN wholesale pricing. These activities will further increase consumer interest and options for wireless broadband services.

In addition, Vodafone and Telstra provide options to include a wireless SIM in their fixed broadband WiFi routers – allowing users to switch between wireless and fixed to ensure reliable connectivity. As such, as network technologies improve, these operators could opt to switch low-usage customers to wireless only without changing the hardware or causing any disruption to users.

http://doi.org/10.18080/jtde.v7n1.178

Finally, Fixed Wireless players, such as Uniti Wireless, Spirit, BigAir and Nuskope, have emerged to provide wireless broadband services (many aiming to capture both consumer and business broadband market share from NBN in particular regions).

Conclusion

There is clear potential for growing wireless-only household broadband services. Our survey results, identifying the growing acceptance of wireless services combined with some doubts about NBN service quality, indicate 30% of existing fixed broadband households would consider switching to a wireless broadband service.

However, there are differing views on the benefits of mobile versus fixed broadband technologies. This will likely reflect the lack of uniformity in coverage and quality issues across both service types, as well as other factors such as types of internet usage and time of day. The results of the ACMA NBN review and the ACCC performance monitoring program are likely to help consumers make more informed decisions.

In addition, the differing views on the benefits of mobile versus fixed broadband technologies highlight the opportunity for telcos to further communicate their service capabilities. Further, and most significantly, the NBN must continue to focus on resolving its perceived quality issues, while also ensuring a competitive product roadmap is in place for future broadband products.

Finally, the rollout of 5G networks and fixed wireless broadband solutions in Australia will further increase consumer interest and options for wireless broadband services. Whilst we do not believe that wireless broadband services will fully replace fixed broadband services, it is clear that specific fixed broadband customer segments will be under threat.

Acknowledgements

The author would like to thank Dr Leith Campbell (Honorary Fellow, Melbourne School of Engineering) for his advice on this article.

References

ACCC [Australian Competition and Consumer Commission]. 2018a. *Communications Sector Market Study: Final report*, April. Available at https://www.accc.gov.au/system/files/Communications%20Sector%20Market%20Study%20Final%20Report%20April%202018_0.pdf

ACCC [Australian Competition and Consumer Commission]. 2018b. 'Report 3', *Measuring Broadband Australia*, November. Available at https://www.accc.gov.au/system/files/ACCC%20-%20MBA%20Report%20-%20November%202018.pdf

http://doi.org/10.18080/jtde.v7n1.178

ACMA [Australian Communications and Media Authority]. 2017a. *Migrating to the National Broadband Network – the consumer experience: Key findings from analysis of industry information*, December. Available at https://www.acma.gov.au/-/media/Consumer-Interests/Report/PDF/Migrating-to-the-NBN--The-consumer-experience--Key-findings-from-analy-pdf.pdf?la=en

ACMA [Australian Communications and Media Authority]. 2017b. 'Protecting consumers on the NBN', ACMA General Information, 20 December. Available at https://www.acma.gov.au/Industry/Telco/Infrastructure/The-NBN-and-industry/protecting-consumers-on-the-nbn

Cisco. 2017. 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021', *White Paper*, 7 February. Available at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

Switkowski, Z. 2017. 'NBN: The transition years', *CommsDay Melbourne Congress*, Melbourne, 10 October.

http://doi.org/10.18080/jtde.v7n1.178

Tunnelling the Internet

Habiba Akter
School of Electronic Engineering and Computer Science
Queen Mary, University of London, London, United Kingdom
h.akter@qmul.ac.uk

Chris Phillips
School of Electronic Engineering and Computer Science
Queen Mary, University of London, London, United Kingdom
chris.i.phillips@qmul.ac.uk

Abstract: Despite a considerable increase in Internet capacity, regional congestion is still an issue at certain times of day. Dimensioning the system to provide minimal delay under these transient conditions would be uneconomical. We therefore investigate a scheme that allows end-users to selectively exploit a sequence of mini-tunnels along a path from their origin to a chosen destination. Such tunnels can be advertised centrally through a broker, with the cooperation of the Autonomous System (AS) domain operators, similar to a driver choosing to use a toll road to avoid potential congestion. It is thus a type of loose source routing. The approach avoids the need for inter-operator cooperation, although such cooperation could enable extending tunnels across AS peers. We explore the benefit in delay reduction for a given concentration of tunnels within a portion of the Internet. We show that a relatively small number of tunnels can provide worthwhile improvements in performance. We consider both when tunnels are randomly distributed and when they are provided close to an AS domain of interest, where traffic congestion is more likely. In this latter case, even a relatively small number of tunnels can benefit a reasonable number of users across a large region.

Keywords: Internet, Autonomous System, loose source routing, tunnelling, broker.

Introduction

Although the Internet has proved to be robust and flexible, the delivery of time critical data traversing multiple Autonomous System (AS) domains remains sub-optimal due to the unwillingness of the network operators to support inter-operator signalling coupled with the control of the associated forwarding infrastructure (Schaffrarh, 2009). Mechanisms for such signalling have been proposed, with functional entities such as the ITU Resource and Admission Control Function (RACF) and the IETF Path Computation Element (PCE) (Chamania, 2012). Despite the proposal and refinement of these operator-owned control plane

http://doi.org/10.18080/jtde.v7n1.175

entities over many years (Yost, 2015; Rzym, 2016; Dasgupta, 2007), their adoption outside the academic community is no nearer.

The focus of this research is on improving the end-to-end communication performance of the Internet, driven from an end-user perspective. This work is not concerned with establishing end-to-end paths or tunnels: rather, the aim is designing a scheme where short tunnels are made available across individual ASes, and possibly between adjacent ones. These are advertised to the end-users through a "Service Broker", providing users with an opportunity to use them, for a small fee, if they wish to do so. To facilitate this, we envision an entity at the users' access point that would select the most "appropriate" path for a given data stream, depending on constraints such as the amount of money the user is ready to pay, the end-to-end delay, and the flow content, for example.

This paper is an extended version of the paper "Are Internet Tunnels Worthwhile?" presented at 28th International Telecommunication Networks and Applications Conference (ITNAC), 2018. It includes additional material examining the focused deployment of tunnels.

Motivation for Tunnels

The main motivation for tunnelling over segments or the entire end-to-end path across the Internet is to overcome limitations inherent in traditional next-hop forwarding. With next-hop forwarding the path taken by the traffic is determined by the router node at each "hop" using information held in its Forwarding Information Base (FIB). The FIB data is typically constructed based on automatically configured routing information obtained via intra- and inter-gateway routing protocols along with operator policy filtering (Farrel, 2004). This presents two key issues. First, end-users have no say in how their data is forwarded. Second, lack of traffic differentiation means that information flows along paths based on a simple "least cost" metric lead to load imbalances and "best effort" equal treatment of all traffic, irrespective of its importance to the user.

A tunnelling mechanism, e.g., a classification and label switching mechanism, can be used to address both of these issues. Tunnelling has already been implemented using various technologies (Secci, 2008). We aim to give end-users some control over choosing the path their data flows through by making the presence of these tunnels visible, advertised centrally using a broker, along with a means of steering traffic between them. Although the broker we are proposing is expected to know where the tunnels are, along with their characteristics, it does not need to know how the tunnels are established or operated. Operator security is not compromised, as the details of the technology used to provide the tunnels is hidden, and their establishment and maintenance remains fully under the control of the operator.

http://doi.org/10.18080/jtde.v7n1.175

Users can choose to use the tunnels, if they wish, for a nominal fee. The idea of charging customers for better service is not new (Doctorow, 2014). However, in our case, choosing to use tunnels is optional and it is up to the user which specific flows are directed through them. As such, some customers may be happy to selectively pay to obtain flow transport with a better Quality of Experience (QoE).

In our proposal, the end-user will be the one to decide whether specific tunnels will be used or not, knowing the "financial cost" and the expected benefits. Operators are expected to cooperate, as they receive extra revenue by providing the tunnels. However, these tunnels, at least initially, only straddle ingress to egress points of specific AS domains between AS Border Routers (ASBRs). The location, delay, cost and perhaps resilience of these tunnels (comprising an IP address of the ingress ASBR and additional information) are passed to the broker. An entity at the end-user's access point can see the information advertised by the broker and optionally decide to direct traffic flows via one or more tunnels if the perceived benefits are sufficient relative to the cost involved.

Net Neutrality

The term "net neutrality" was first used in 2003, by Tim Wu, as augmentation of the idea of "common carrier" (which transports data for any person or company with taking the responsibility of any possible loss) for telephone systems (Wu, 2003). Net neutrality is the idea stated as "all Internet traffic should be treated equally" (Honan, 2008). According to this idea, Internet Service Providers (ISPs) and the governments regulating the Internet treat all the data equally, without making any discrimination or taking different charges by user, content, website, platform, application, type of attached documents (e.g., emails, audio, video), or mode of communication (Rushe, 2017). Hence, according to this policy, the ISPs cannot prioritise any data over the others while sending it from the source to the expected destination.

Thinking generally, it can be easily stated that a few milliseconds' delay while sending an email will not bother the sender or receiver much. On the other hand, the same amount of delay in a live video streaming flow can have a noticeable negative impact on the Quality of Experience (QoE) of the user.

A motivation behind our research is that, from the point of view of an end-user, treating all the traffic in the Internet equally creates problems. There is much debate concerning how different traffic should be treated. However, our vision is not about charging users for the services, rather it gives the users the opportunity to choose if they want to pay for getting a better service and also provides some control over how their traffic moves across the Internet. Hence, in a way, we are not against net neutrality: rather, we aim to give more control to the users to decide how they want their traffic to be handled by the Internet.

http://doi.org/10.18080/jtde.v7n1.175

Example Framework

The Tunnel Framework

The basic architecture of the AS-Domain tunnelling framework is shown in Fig. 1. The tunnels shown are assumed to have been set up and maintained by the specific network operators using whatever means they wish. This could involve the use of PCE/RACF signalling; however, this is not essential. The presence of the tunnels is advertised via the Directory Service Broker (DSB). This is explained briefly in the section "Broker Function". The tunnels can be of any technology, though it is expected that many will employ Multi-Protocol Label Switching (MPLS) or be based on optical channels. These tunnels can be both intra- and inter-AS in scope, in the latter case this being achieved through operator peering. Some tunnels may offer 1+1 protection; others may exist between peering operators through Label-Switched Path (LSP) stitching. Unlike the usual traffic sending process, in a 1+1 architecture (spoken of as "One Plus One"), dual copies are sent through two routes in parallel so that, in case of any network failure, the alternate route can be chosen for receiving the packet flow . However, details of the construction mechanism are considered outside the scope of this research.

Initially, customers for this service are assumed to be Small and Medium Enterprises including financial institutions that wish to transport data quickly without having to incur the costs associated with a leased end-to-end infrastructure. They will have awareness of the sequence of AS domains that their data is passing through and possible alternatives, particularly if Border Gateway Protocol (BGP) reachability information is made available to them via the DSB Internet Map.

Their IT administration, which could be automated software that performs path selection based on cost and other requirements, may wish to choose a preferred path between their own site and a given destination, such as between Customer A and B in Fig. 1. For example, by interrogating the information in the DSB, Customer A wishes to use Tunnel T1 and T3 to hasten the delivery of data between the two sites. Having informed the DSB of this decision, for a small fee Customer A is given tickets for each of the tunnels (i.e. T1 and T3) along with their ingress IP addresses. Tickets are ephemeral so it is unlikely that users can abuse the system extensively.

http://doi.org/10.18080/jtde.v7n1.175

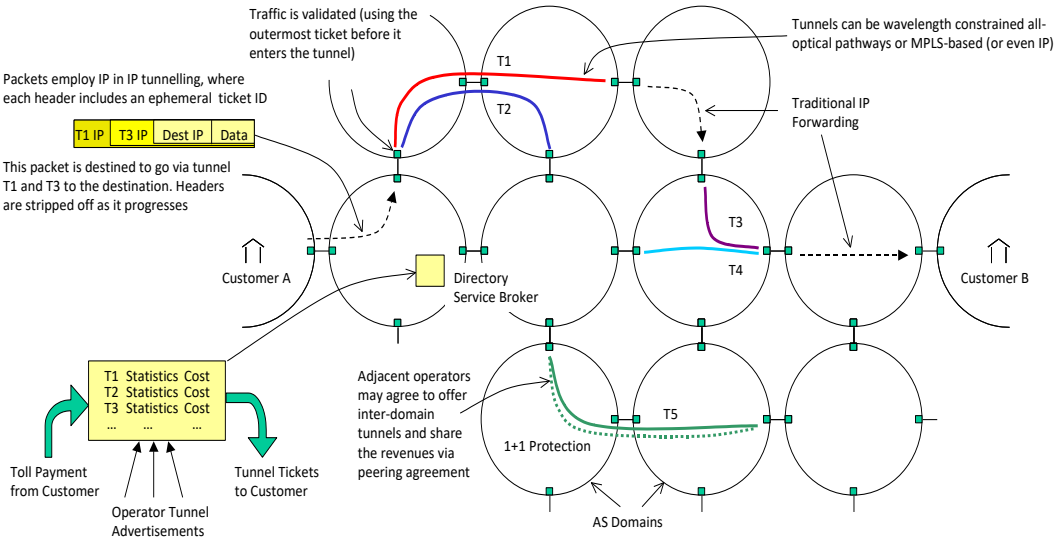

Figure 1. User-Selectable AS Domain Tunnelling Framework

Network Operator Functions

Tunnels traversing multiple domains are hampered by the unwillingness of network operators to support inter-operator signalling, coupled with the control of the associated forwarding infrastructure. However, our system does not depend on any information that the network operators will not share with the DSB due to "trust" issues. We assume that cooperative operators will let the broker advertise their available tunnels centrally, with some information such as where the tunnels are, how much the "usage charge" is, and what performance they offer to the users, typically in terms of guaranteed traversal delay relative to the no-tunnel alternative. The approach does not require the sharing of any sensitive information such as the mechanism by which the tunnels are established and maintained. However, AT&T and CAIDA already provide some information concerning dynamic network performance (Statista, n.d.; CAIDA, n.d. Huffaker, 2012).

Our system deals with the tunnels existing between Autonomous System Border Routers (ASBRs) belonging to the same AS. There is no need to know about the internal path of the tunnels. Tunnels straddling AS domains are considered optional, as they would require a peering relationship between operators. However, mechanisms for stitching together LSPs across AS domains could technically be provided if sufficient trust existed between adjacent operators.

Broker Function

The idea of implementing a service broker has already been proposed in the field of telecommunication to make offers of best service against customer requests (Plummer, 2011). In (Markakis, 2016), a tunnel broker system is discussed that minimizes the job of the tunnel

http://doi.org/10.18080/jtde.v7n1.175

server by assigning the broker server that handles the user requests and returns the prime configuration to both users and tunnel servers.

We introduce a DSB in order to provide a centralized resource for advertising the AS tunnels to the end-users, giving them the opportunity to choose to some extent their desired path across the inter-network. We assume it will have the map view of the ASes that the broker can show the end users, indicating which ASes are adjacent to each other and, in the case of cooperative ASes, information concerning their tunnels will be included. The broker presents the location of tunnels to the users superimposed on an AS view of the Internet (or a portion of it) and the users have the opportunity to choose whether their traffic is directed through one or more tunnels in a particular sequence. This provides a form of loose source routing. Furthermore, certain ASes may show information concerning their degree of congestion. This allows the end users to selectively choose to use a tunnel to detour traffic away from the congestion, or to provide preferential treatment across the congested AS.

To clarify more, the DSB does not retrieve topology maps. It generates a map view from information that is either passed to it from the ISPs or which can be obtained using "traceroute" and/or BGP update messages. We naturally assume that the operators that are willing to cooperate will also pass some information saying whether the tunnels or their default forwarding environment are busy at a particular time and this information can be made available in the proposed broker's map view. In short, the DSB provides an Internet Map showing the tunnel locations, their usage charge and some statistics regarding the performance they offer.

However, the broker does not tell the user how to get across the network. It provides a view of the topology, with the cost. The map can also include ASes present in the network that are not cooperating with the broker. In this instance, only their ASBR interconnection with other ASes will be available.

The DSB also provides a single brokerage point whereby the user can request a sequence of tunnel permits (tickets) so that traffic can use a tandem arrangement of multiple tunnels between a source and destination. The DSB is effectively the customer-facing entity where operators advertise their tunnels and the transactions that can be made.

End-User Function

The end-user would be expected to install software in his/her network. The software would obtain the visualization part of the Internet map from the DSB. It also needs to know where the tunnels are available for the users and what are the tunnels' starting and end points. The software will get some information from the user, e.g.:

http://doi.org/10.18080/jtde.v7n1.175

- The source and destination ASes for the data of the user to be sent.
- Expected service of the users, where delay and other constraints will be the measure.
- Amount of money the user wants to pay.

Knowing the preferences of the user, the software will be able to:

- Tell the least cost path using Dijkstra's Algorithm.
- Find the path with tunnels.
- Compare the constraints and the financial cost.
- Suggest the better route for the traffic.

Initially, the decision will be made depending on two factors: the benefit and the (financial) cost.

The user software will get the same visualization of the Internet map from the broker, including the location and expected service provided by the tunnels and the usage cost. However, details of this mechanism and how the financial model operates are considered beyond the scope of this paper. This paper focuses on assessing the magnitude of the benefit in terms of delay performance, if such tunnels existed.

Evaluation

Implementation

A framework has been constructed to investigate the benefits of using different percentages of tunnels present in a part of the Internet for sending data from one AS to another.

Some regional internet topologies at the AS level are generated using the topology generator PFP (Positive Feedback Preference) developed by Mondragon and Zhou in 2004 (Zhou, 2006) and used as input for the tool we have developed. The main reason for choosing PFP is that it is a phenomenological model for AS-level internet topology which can precisely reproduce a number of topological characteristics, e.g., degree distribution, rich club connectivity, maximum degree, shortest path length, short cycles, disassortative mixing and betweenness centrality (Zhou & Mondragon, 2004). The PFP model starts from a small random AS-graph and keeps growing where, at each step, new nodes are attached to old nodes and old nodes also peer with other old nodes (Zhou, 2006). The probability of a node gaining a new link, which is a function of the node degree, is calculated as 0.048 (Clegg, 2010). The more links a node has, the more is its chance to obtain further links. The developers of PFP have explained the consequence as "the rich not only get richer, but they get proportionately richer" (Zhou, 2006; Clegg, 2010).

http://doi.org/10.18080/jtde.v7n1.175

The AS topology developed from the PFP is fed into the framework developed for this research, which then produces another topology at the level of ASBRs, assuming there is a peering of border routers (formed by one from each of the connecting ASes) at the point where the two AS domains are connected to each other. We are aware that the route between the adjacent border routers of two connecting ASes does not necessarily have to be one-to-one; rather, there can be one-to-several connections. However, we currently confine ourselves to one-to-one ASBR peering.

Moreover, within a single AS, the border routers are inter-connected into a full mesh, but the connections need not necessarily be direct; rather, more than one internal hop may exist between a pair of border routers. Our system does not require this knowledge, nor do operators need to share this information. Therefore, the topology view of the broker is not necessarily a complete one. We can call it a "sanitized" or an "artificial" view of the Internet map. It just shows how the various ASes are inter-connected at the AS level. Depending on this AS view, the ASBR topology is produced.

We then use Dijkstra's Algorithm to calculate the least cost routes for traffic to be sent from any source AS to any destination. The paths include the ASBRs that the traffic needs to traverse to reach the destination. This is the no-tunnel least cost path.

For now, the cost of the routes is considered using the metric of "delay" in milliseconds. A data packet typically needs to go through 4 to 6 hops within a given AS while traversing across a number of ASes to reach the destination (Begtašević, n.d.). Hence, an intra-AS tunnel having the ingress and egress points in the same AS can reduce the delay that is experienced relative to the normal no-tunnel intra-AS links. This is particularly true if the normal pathways are congested and some form of priority is given to the tunnels, be that through the use of separate optical channels or queueing priority along shared links.

Fig. 2 illustrates a simple example of alternate no-tunnel and tunnel paths within an AS.

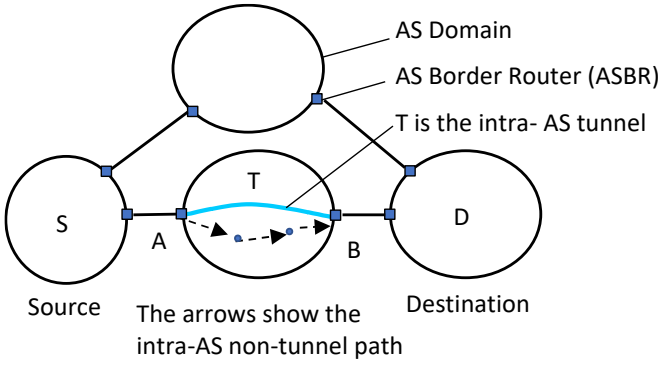

Figure 2. Example Intra-AS path with and without Tunnels

In Fig. 2, the source and destination ASes are S and D and the traffic is assumed to traverse through another AS to reach the destination, which has a tunnel T with ingress point A and

http://doi.org/10.18080/jtde.v7n1.175

egress point B. The dotted lines represent a normal intra-AS pathway including routers inside the AS.

For now, along each of the links, the associated cost is the (mean) delay in milliseconds. The four types of delay contributing to the total end-to-end delay are: transmission (Tx) delay, propagation delay, processing delay and queueing delay. The propagation delay between the ASBRs A and B will be same for the no-tunnel normal path and the tunnel. Ramaswamy (2004) shows that the processing delay matters although both processing and transmission delays are proportionately small. Hence, queueing delay is the one that typically contributes most to the delay experienced. It also confirms that processing and queueing delays are the ones that are usually considered in terms of measurements and simulations.

The amount of delay experienced via tunnels versus no-tunnel intra-AS paths and the corresponding cost ratio have been chosen carefully after doing some research on Internet delay measurements (Ramaswamy, 2004; Zeitoun, 2004; Choi, 2004; Carlsson, 2004). Keeping the hop count in mind, our experiments have been run considering the normal intra-AS path cost as *3x* milliseconds and *4x* milliseconds, where the cost for using a tunnel is *x* milliseconds. Then, for a congested traffic situation, where the queuing delay must be high, the cost for normal intra-AS path is set as *15x* milliseconds.

Our tool uses Dijkstra's Algorithm to calculate the no-tunnel least cost path depending on these allocated costs. After that, the tool generates a given percentage of tunnels in the produced AS topology. Taking the expected number of tunnels as user input, the tool places different percentages of tunnels in randomly chosen ASes and calculates the least cost path again, considering the tunnels in the chosen ASes. The least cost path includes the tunnels if and only if the delay cost of the tunnels is less than that of the no-tunnel paths. For now, we assume an AS that is selected for hosting tunnels has them arranged in a full mesh between the ASBRs of the AS.

Results

We have performed a number of simulations in order to access the benefits of using tunnels in a regional network topology. To start with, a small topology of 7 ASes is fed into the PFP model to grow it to a larger topology of 30 ASes for two different node degrees – 3 and 4 – with the probability of a node obtaining a new inter-AS link/adjacency of 0.04, to investigate the benefit for both cases.

Taking the PFP-generated AS-level topology as an input, the framework produces a topology at the ASBR level. Next, Dijksta's Algorithm calculates the least cost path from every AS to all the remaining ASes. Then, the presence of 5%, 10%, 15%, 20%, 25% and 30% tunnels is added to the topology and least cost paths are again calculated for every tunnel percentage.

http://doi.org/10.18080/jtde.v7n1.175

For now, no inter-domain tunnels have been considered and the cost of a link between the peering border routers of two adjacent ASes is set to 1 ms.

The benefit of the tunnels being present is calculated as follows:

> *Benefit from AS "A" to AS "B" for x% tunnels = [cost from A to B using no tunnels minus the cost from A to B when x% tunnels are present] ms*

The costs are automatically calculated using Dijkstra's algorithm for each least cost path and then the average and standard deviation of these differences is calculated. It should be noted that in many cases there will be no cost benefit of going via one or more tunnels when they are remote from the original no-tunnel pathway. This tunnel-placement process is repeated 10 times for a given overall AS topology and the average and standard deviation of the benefit are calculated and the results plotted.

Result for Different Topologies

Setting the average node degree to 3, five topologies each having 30 ASes and similar properties are generated by the PFP topology generator. They are then fed into our tool and tunnel placement is repeated 10 times. In each case, the ratio of the cost of a tunnel in an AS to that of a normal no-tunnel path is set at 1:3 (delays are considered in milliseconds) and the average is calculated for the average and standard deviation of the benefit for different percentages of tunnels. Table 1 summarises the results.

Table 1. Average and standard deviation of the benefit for using tunnel(s) (in milliseconds)

% of tunnels	Topology 1	Topology 2	Topology 3	Topology 4	Topology 5
	Average/ Standard Deviation	Average/ Standard Deviation	Average/ Standard Deviation	Average/ Standard Deviation	Average/ Standard Deviation
5%	0.325057/ 0.492979	0.10698/ 0.425952	0.309425/ 0.601801	0.191724/ 0.461871	0.053334/ 0.28789
10%	0.430345/ 0.647781	0.438125/ 0.736941	0.46006/ 0.790095	0.381609/ 0.74438	0.218391/ 0.574282
15%	0.822418/ 0.893881	0.59418/ 0.899783	0.657011/ 0.953498	0.498851/ 0.834226	0.558391/ 0.786062
20%	0.98318/ 1.044247	0.847816/ 1.057714	0.818391/ 1.049085	0.774713/ 1.040576	0.703908/ 0.921514
25%	1.217595/ 1.120945	0.945149/ 1.138616	0.872184/ 1.092653	0.950345/ 1.144512	0.777931/ 0.977332
30%	1.272562/ 1.134269	1.104503/ 1.230331	0.998161/ 1.173999	1.071724/ 1.144512	0.914943/ 1.028713

As expected, as the proportion of tunnels increases so does the average benefit. When the percentage of tunnels is small, the average benefit is marginal. However, from the standard

http://doi.org/10.18080/jtde.v7n1.175

deviation, we can see that even when the percentage of tunnels is low, for some users located close to the tunnels, considerable benefit is still achievable.

Of the five generated topologies, the results of one of the topologies (Topology 4 in Table 1) are now considered in detail.

Different Cost Ratio

For the same topology, different cost ratios are considered for 10 runs. While choosing the cost ratios, at first we have been conservative and considered the average delay cost for no-tunnel paths as ***3x*** milliseconds and ***4x***, where the average delay for a tunnel is ***x*** milliseconds (as explained in the Implementation section). Then we have considered a situation representing traffic congestion where the average no-tunnel link's cost is ***15x***. At certain times, the Internet can be busy, impacting on the end-to-end delay. Usually, queueing delay makes a greater contribution in such cases.

Fig. 3 presents a graph plotting the average benefit for different percentages of tunnels for Topology 4 from Table 1.

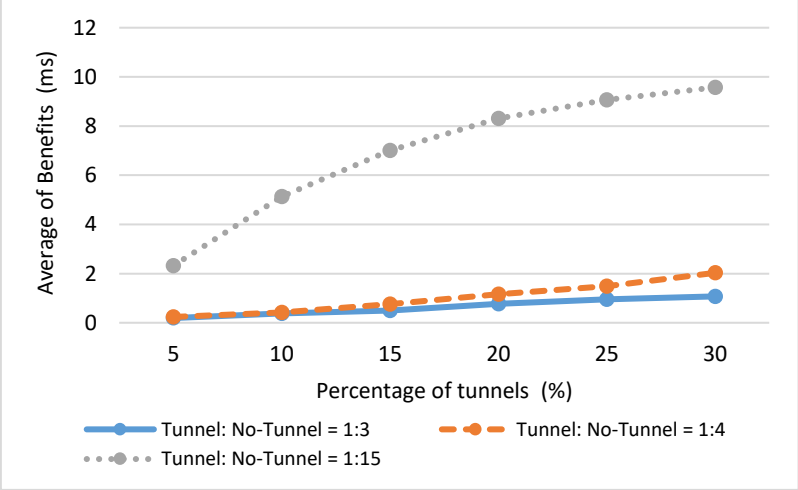

Figure 3. Average of Cost Benefit for different cost ratios

It is clear from the graph that, for all cost ratios, the benefit increases as there is an increase in the percentage of tunnels present in the Internet. With a ratio of 1:3, the average delay for sending data in topology 4 is 4.97 ms which is reduced by a minimum of 0.19 ms when 5% of ASes have tunnels in them. The average benefit gradually reaches almost 1.08 ms for 30% tunnels. For a tunnel/no-tunnel ratio set to 1:4, the average end-to-end delay without the use of tunnels is 5.97 ms. With 30% tunnels, this end-to-end delay goes down by 2.03 ms.

It can be seen that the average improvement is relatively small when the tunnel's average delay cost is one-third or one-quarter of the normal no-tunnel average delay. This is not surprising, as many paths would incur a costly diversion to reach tunnel(s), particularly when they are

http://doi.org/10.18080/jtde.v7n1.175

few in number. Even so, a decrease of almost 2 ms compared with almost 4 ms to 6 ms could still be of attraction to at least some end-users for specific application services.

Conversely, for the "busy" period, the average benefits associated with greater cost ratios are noticeably high. When we consider the cost associated with a no-tunnel link in a congested AS as 15 ms, the average end-to-end delay for the same topology is calculated as 16.97 ms. As expected, exploiting tunnels within this AS lowers the delay to a great extent, resulting in more average benefit. For 10% tunnels the average benefit is more than 5 ms and for 30% it reaches almost 9.6 ms.

The standard deviation of the benefit is plotted in Figure 4.

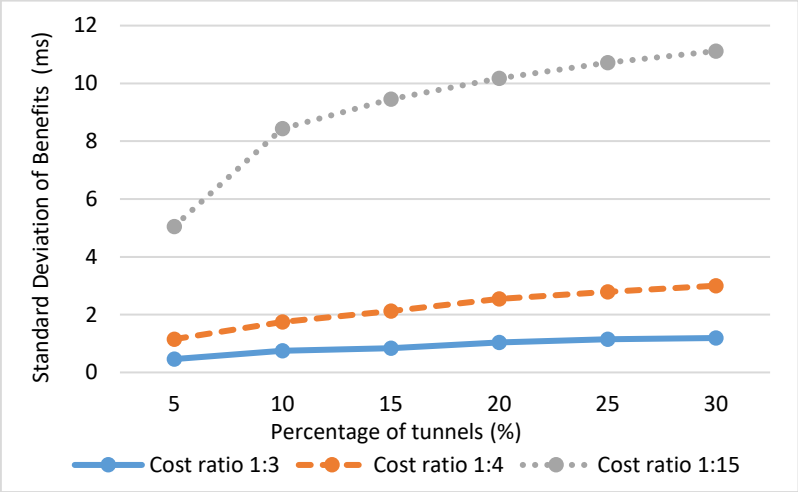

Figure 4 Standard Deviation of Cost Benefit for different cost ratios

The increasing standard deviation shows that, between a smaller number of source-destination pairs, the cost benefit can be substantial. Indeed, it is worth noting that, during peak hours or when specific high-demand events occur, the intra-AS queueing delay can be tens of milliseconds if not more. If tunnels bypass such "hot spots", the delay cost benefit could be orders of magnitude, providing end-users considerable benefit in terms of delay.

Altering the Node Degree

The PFP generator is used again to generate an AS-topology from the same initial 7-node seed graph that has been used to generate the topology used in Fig. 3 and 4. However, this time the graph evolution is altered by setting the average node degree to 4. As with the previous simulations, we have considered the use of tunnels under normal traffic conditions and during a period of localised congestion, where the ratio of the cost for tunnel to that of no-tunnel path is 1:4 and 1:15 within the specified ASes.

Then, for both cases the average of the delay cost benefit for the presence of 5%, 10%, 15%, 20%, 25% and 30% tunnels was calculated and is shown in Fig. 5.

http://doi.org/10.18080/jtde.v7n1.175

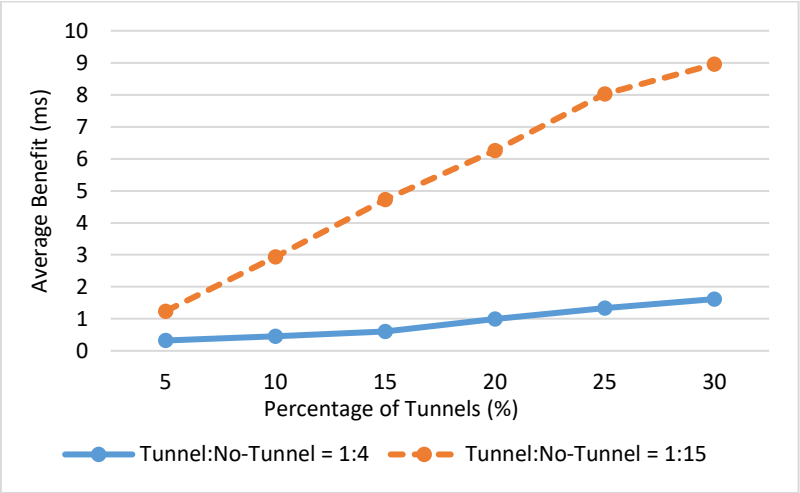

Figure 5. Average of Cost Benefit for different cost ratios

For the AS level topology, the average end-to-end delay without any tunnel is 5.97 ms, which decreases when tunnels are available to end users. If the tunnel has an average delay cost of 1/4th of the normal intra-AS link path, then it gives an average end-to-end delay benefit of 0.32 ms, which increases with the number of tunnels and, for 30% tunnels, reaches 1.62 ms.

For the busy period conditions, we assume that the tunnel will have an average delay of 1/15th of the average normal intra-AS link delay. For the no-tunnel topology, the average end-to-end delay is 14.94 ms. Clearly, the graph shows that the availability of different percentages of tunnels adds benefit by improving the average delay cost. For 15% of tunnels the average reduction in delay is 4.73 ms and for 30% it is almost double, 8.95 ms; and it is approximately 6 times more than the benefit we observed for the ratio of tunnel/no-tunnel cost of 1:4.

Hence, it is clear from the graphs that, during peak times, even the presence of a small percentage of tunnels can provide noticeable benefit to many users by decreasing the delay cost.

Considering "Hotspot" Area

In the Introduction, we mention that the lack of traffic differentiation can lead to load imbalances and "best effort" equal treatment of all traffic irrespective of its importance to the user. Keeping this situation in mind, we conducted a series of simulations for a situation where all the source ASes want to send their data traffic to a particular destination AS over the Internet. This approximates the situation where the destination AS hosts a popular server farm or data centre.

In this case, the framework is changed in such a way that, upon calculating the expected number of tunnels for a specified tunnel-percentage, it generates the tunnels in ASes adjacent to the destination AS first. If the number of expected tunnels is more than the number of adjacent ASes, then the rest of the tunnels are generated to the ASes that are one hop away,

http://doi.org/10.18080/jtde.v7n1.175

and so on. Thus, the tunnels are organised into approximately concentric rings around the destination AS.

Noting the benefits of tunnel-usage are more pronounced and meaningful for "peak time" situations, we have again run 10 simulations for the same topology with 30 ASes, as used in Figure 5 (with a node degree of 4), where the average delay cost for a tunnel is 1 ms and that of a normal path is 15 ms. Taking AS2 as the destination AS, and assuming each of the remaining 29 ASes act as the source domains, Figure 6 presents the graph of average and standard deviation of the benefit for using tunnels around a "hotspot" destination.

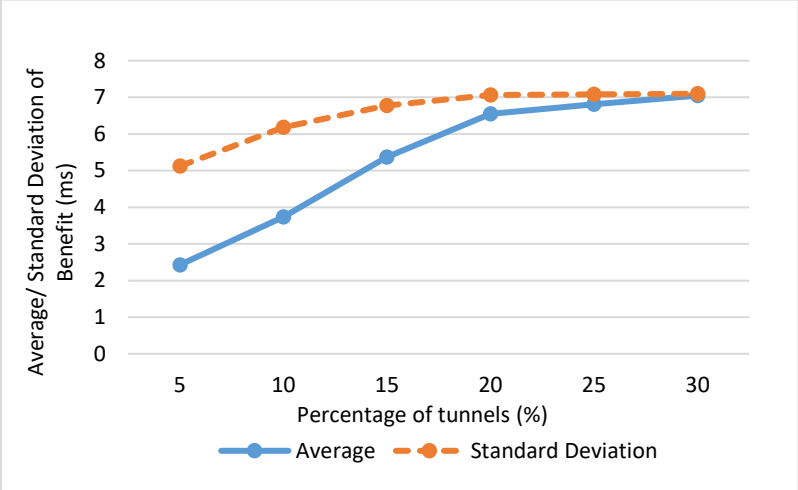

Figure 6. Average and Standard Deviation of Cost Benefit for Tunnel-No Tunnel = 1:15

The baseline average end-to-end delay for sending data to AS2 from all the other domains is calculated to be 9.5 ms. It is clearly observed that both the average and standard deviation of the delay cost benefit of employing a given percentage of tunnels is relatively high compared the ones we have observed in Figures 3 to 5, even for only 5% of tunnels near a hotspot destination in the network topology. Hence, in the case of known "hot spots" in terms of desirability and possible congestion, access to low delay tunnels becomes particularly attractive.

Discussion

Using the developed framework, we can examine the delay benefits that intra-AS tunnels might bring to the Internet. It shows that there is a benefit for even 5% tunnels in the network for some users, though this is dependent on how close the tunnel alternatives are to the default traditional pathway.

To show the variation in benefit between source-destination pairs, we provide the standard deviation. This is because the spread of values provides an indication of the percentage of customers that can obtain a certain level of benefit. For different percentages of tunnels, the average benefit is not going to be great for all the users and the standard deviation shows that

http://doi.org/10.18080/jtde.v7n1.175

at least for some customers there is substantial benefit if their desired path lies close to one or more tunnels. If they are further away, the benefit of the tunnel(s) is offset by the additional number of hops to reach them.

However, as one standard deviation only encompasses about 68% of a Normally distributed population, it is worth noting that for some users the cost benefit would be appreciable. Indeed, if the standard path experiences delays brought about by "hot-spot" congestion, then tunnel alternatives become much more attractive. Furthermore, our current investigations avoid the use of more ambitious inter-AS tunnels, and the broker function need only have access to limited information, ameliorating any security risks. The key benefit, from our perspective at least, is that it gives end-users some choice over how their data is treated by the network and it is up to the user which traffic should be directed via these tunnels.

A further aspect of user-selectable tunnels not explored in detail in this paper is their ability to partially pin down a route to circumvent "less desirable" areas of the Internet. This allows users to use one or more tunnels to "nail-up" a loose source-routed path between the source and destination. Using "heartbeat" probe messages the regular path could be monitored to a limited degree and, if an outage is detected, the traffic flows could be directed via a suitable tunnel to the destination to avoid the anticipated area of concern. This has the advantage that the action can be implemented rapidly, without waiting for BGP to announce an alternative pathway around the outage location.

Conclusions

This paper introduces a tunnelling framework allowing cooperation between end-users and transport service providers via a simple brokerage mechanism. This is done in such a way that trust issues to do with the tunnel details and AS domain internal architecture are not compromised. The paper at first takes a conservative approach to the introduction of low delay-cost tunnels in an Internet region, typically comprising about 30 AS domains. We avoid tunnels spanning ASes as this would typically require cooperation between service providers. Instead we focus on intra-AS tunnels that are added in a relatively low concentration. We show that some benefit is available, but its magnitude is dependent on the proximity of users to suitable tunnels and the delay performance ratio between the tunnel/no-tunnel intra-AS path alternatives. Not surprisingly, when the tunnels allow a user to circumvent hot spots, their benefit can be appreciable.

We have also considered an AS topology having a particular domain as a hotspot destination, representing an AS hosting a datacentre etc. As the traffic tends to concentrate as it moves towards this "hot spot", locating tunnels in the region close to this focal point provides more

http://doi.org/10.18080/jtde.v7n1.175

benefit to more users, should they choose to avail themselves of the tunnelled path alternatives.

In summary, we believe that end-user selectable access to tunnels provides a suitable degree of choice whilst avoiding the issues of "net neutrality" and would allow better management of the Internet as demands on its resources continue to grow.

References

Akter, H., & Phillips, C. (2018). Are Internet Tunnels Worthwhile? *28th International Telecommunication Networks and Applications Conference (ITNAC)*, 21-23 November.

Begtašević, F., & Van Mieghem, P. (n.d.). Measurements of the Hopcount in Internet. Available at http://circuit.ucsd.edu/~massimo/ECE158A/Handouts_files/hop-count.pdf.

CAIDA. (n.d.). Topology Research. Retrieved from: http://www.caida.org/research/topology/. Last accessed September 26, 2017.

Carlsson, P., Constantinescu, D., Popescu, A., Fiedler, M., & Nilsson, A. (2004). Delay Performance in IP Routers, *2nd International Working Conference (HET-NETs '04)*.

Chamania, M., Drogon, M., & Jukan, A. (2012). An Open-Source Path Computation Emulator: Design, Implementation, and Performance. *Journal of Lightwave Technology*, *30*(4).

Choi, B-K., Moon, S., Zhang, Z-L., Papagiannaki, K., & Diot, C. (2004). Analysis of point-to-point packet delay in an operational network. *IEEE Infocom 2004*, 7-11 March.

Clegg, R.G., Di Cairano-Gilfedder, C., & Zhou, S. (2010). A critical look at power law modelling of the Internet," *Computer Communications*, *33*(3), 259-268, February.

Dasgupta, S., De Oliveira, J.C., & Vasseur, J-P. (2007). Path-Computation-Element-Based Architecture for Interdomain MPLS/GMPLS Traffic Engineering: Overview and Performance. *IEEE Network Magazine*, *21*(4), 38-45, July-August.

Doctorow, C. (2014). Internet service providers charging for premium access hold us all to ransom. *The Guardian*, 28 April. Retrieved from: https://www.theguardian.com/technology/2014/apr/28/internet-service-providers-charging-premium-access.

Farrel, A. (2004). *The Internet and Its Protocols: A Comparative Approach*. USA: Morgan Kaufmann.

Honan, M. (2008). Inside Net Neutrality: Is your ISP filtering content? *Macworld*, 12 February. Retrieved from: https://www.macworld.com/article/1132075/web-apps/netneutrality1.html. Last accessed August 2018.

Huffaker, B., Fomenkov, M., & Claffy, C. (2012). Internet Topology Data Comparison. *Technical Report*, Cooperative Association for Internet Data Analysis (CAIDA), May.

Markakis, E., Sideris, A., Alexiou, G., Bourdena, A., Pallis, E., Mastorakis, G., & Macromoustakis, X. (2016). A virtual network functions brokering mechanism, *International Conference on Telecommunications and Multimedia (TEMU)*, IEEE, 25-27 July.

Plummer, D., Lheureux, B., Cantara, M., & Bova, T. (2011). Cloud Services Brokerage Is Dominated by Three Primary Roles. *Gartner Research Note* G00226509, 23 November.

http://doi.org/10.18080/jtde.v7n1.175

Ramaswamy, R., Weng, N., & Wolf, T. (2004). Characterising the Network Processing Delay. *IEEE Global Telecommunications Conference (GLOBECOM '04)*, 29 November-3 December.

Rushe, D. (2017). Net neutrality: Amazon among top internet firms planning day of action. *The Guardian*, 6 June. Retrieved from: https://www.theguardian.com/technology/2017/jun/06/net-neutrality-amazon-etsy-kickstarter-protest. Last accessed August 2018.

Rzym, G., Wajda, K., & Rzym, K. (2016). Analysis of PCE-based path optimization in multi-domain SDB/MPLS/BGP-LS network. *18th International Conference on Transparent Optical Networks (ICTON)*, 10-14 July.

Schaffrath, G., Werle, C., Papadimitriou, P., Feldmann, A., Bless, R., Greenhalgh, A., Wundsam, A., Kind, M., Maennel, O., & L. Mathy, L. (2009). Network virtualization architecture: proposal and initial prototype. Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 63-72 in *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*, Spain: Barcelona, August.

Secci, S., Rougier, J-L., & Pattavina, A. (2008). On the selection of optimal diverse AS-paths for inter-domain IP/(G)MPLS tunnel provisioning", *IEEE 4th International Telecommunication Networking Workshop on QoS in Multiservice IP Networks*, 13-15 February.

Statista. (n.d.). AT&T - Statistics & Facts. Retrieved from: https://www.statista.com/topics/1252/atundt/. Last accessed September 30, 2017.

W. Tim, 2003. "Net Neutrality, Broadband Discrimination", *Journal on Telecommunications And High Technology Law, Volume 2, pp 141-176.*

Yost, J.R. (2015). The Origin and Early History of the Computer Security Software Products Industry. IEEE Annals of the History of Computing, *37*(2), 46-58.

Zeitoun, A., Chuah, C-N., Bhattacharyya, S., & Diot, C. (2004). An AS-level study of Internet path delay characteristics. *IEEE Global Telecommunications Conference (GLOBECOM '04)*, 29 November-3 December.

Zhou, S. (2006). Characterising and modelling the Internet topology- The rich-club phenomenon and the PFP model. *BT Technology Journal*, *24*(3), July.

Zhou, S., & Mondragon, R. J. (2004). Accurately modelling the Internet topology. *Physical Review E, 70*(6), No. 066108, December.

http://doi.org/10.18080/jtde.v7n1.175

A Threat Computation Model using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security

Ngoc T. Le
University of Technology Sydney, Faculty of Engineering & IT

Doan B. Hoang
University of Technology Sydney, Faculty of Engineering & IT

Abstract: Securing cyber infrastructures has become critical because they are increasingly exposed to attackers while accommodating a huge number of IoT devices and supporting numerous sophisticated emerging applications. Security metrics are essential for assessing the security risks and making effective decisions concerning system security. Many security metrics rely on mathematical models, but are mainly based on empirical data, qualitative methods, or compliance checking, and this renders the outcome far from satisfactory. Computing the probability of an attack, or more precisely a threat that materialises into an attack, forms an essential basis for a quantitative security metric. This paper proposes a novel approach to compute the probability distribution of cloud security threats based on a Markov chain and Common Vulnerability Scoring System. Moreover, the paper introduces the method to estimate the probability of security attacks. The use of the new security threat model and its computation is demonstrated through their application to estimating the probabilities of cloud threats and types of attacks.

Keywords: Security threats, quantitative security metrics, cloud threats, Markov Chain, Common Vulnerability Scoring System.

Introduction

As cyber infrastructures and their interconnection are increasingly exposed to attackers while accommodating a massive number of IOT devices and provisioning numerous sophisticated emerging applications (Ghayvat et al., 2015; D. Hoang, 2015), security incidences occur more often with severe financial damages and disruption to essential services. Securing cyber systems thus becomes more critical than ever. A simplistic approach to addressing this problem would be to prevent security breaches directly or fix them if they are unavoidable. The approach appears simple and straightforward; however, the achieved solutions are far from

http://doi.org/10.18080/jtde.v7n1.181

satisfactory for several reasons. We have not developed effective predictive tools to anticipate what and where to launch preventive security actions. We may have developed a whole range of tools to deal with security breaches, but this constitutes only temporary and reactive solutions and we are still in the dark, not knowing what comes next!

We suggest a realistic and concrete approach: the goal is to determine the probability of a security threat materialised into an attack (a security breach) on a system, the cost consequences (what it hurts), and the distribution of the costs over the system's constituents or stakeholders (where it hurts) when the threat materialises. Knowing the probability that a threat materialised into an attack we are able to predict the chance that it will occur and take appropriate measures to reduce or prevent its occurrence. Knowing the consequences, we can make appropriate judgments whether the damages caused by the attack are significant enough to warrant a security response or it can be written off as one of the components of the operational costs. Knowing "where it hurts" allows us to use our security knowledge and tools to respond appropriately to the security attack. Clearly, the central issues are the probability of a threat materialised and the distribution of its consequences. In this paper, we only address the problem of determining the probability of a threat materialised into an attack.

The above discussion implies the need for a set of relevant security metrics that allows us to deal with security issues proactively and to set appropriate security goals for our systems and determine the performance of any solution for protecting the systems (both preventing potential incidences and tackling incidences head on). To ascertain the security of a system, it is necessary to develop meaningful metrics to measure appropriately the system's security level or status. Lord Kelvin stated that "when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind" (Thomson, 1889). To measure the security of a cyber space, standards organizations and researchers have proposed many security metrics. The Center for Internet Security (CIS) published a number of security metrics in management, operation, and technique (CIS, 2010). The National Institute of Standards and Technology (NIST) has developed security metrics in implementation, effectiveness, and impact (Aroms, 2012) Other metrics have been proposed for risk assessment and network security evaluation (Hu, Asghar, & Brownlee, 2017; Huang, Zhou, Tian, Tu, & Peng, 2017).

Recently, several security metrics related to the computation of probability of security threats have been developed. In (Patel & Zaveri, 2010), seven types of model-based metrics, which are created by integrating mathematical models and empirical measurements, are also used to calculate the probability of security threat. In (Almasizadeh & Azgomi, 2013), the study used a semi-Markov model to investigate the attack process to compute the transition

http://doi.org/10.18080/jtde.v7n1.181

probability between security states. Mean Failure Cost is one of the sound approaches to quantitative security metrics, taking into account various security components like stakeholders, security requirements, and security threats (Aissa, Abercrombie, Sheldon, & Mili, 2012). The probability distribution of security threats is central to this metric, but the computation is based largely on empirical or qualitative data. Several other security metrics relate to successful attacks, but they are specific to a particular type of attack and hence difficult to generalise.

With these considerations, we pose two questions: (1) how to model a security threat that involves three main security components: attackers, security vulnerabilities, and defenders? and (2) how to predict the probability that the threat materialises into an attack? Considering cloud systems, we address these challenges by proposing a security threat model based on Markov theory to calculate the probability distribution of security cloud threats. For this purpose, the Common Vulnerability Scoring System (CVSS) will be applied to compute the probability of an attack. For evaluating the proposed method, cloud security threats reported by the Cloud Security Alliance (CSA) will be investigated to calculate the probability of cloud threats materialising and the probability of various types of attack. These computation results will generate the quantitative metrics used to measure the security level of a cyber-system (Le & Hoang, 2017).

Major contributions of this paper are as follows:

1. It proposes a security threat model that takes known and major cloud security threats into account. For each security threat, security factors, like attackers, security vulnerabilities and defenders, are investigated to form attack paths for calculating the probability of security threat being materialised.
2. It proposes a method for computing the probability distribution of security threats based on a Markov chain application. The Common Vulnerability Scoring System (CVSS) is investigated to obtain the data for the computation.
3. It provides a method for determining the probability of materialised cloud threats and types of attack using relevant data for supporting security management.

The remainder of the paper is organised as follows. Section 2 provides the background related to security metrics to compute the probability of security threats and Markov theory in security metrics. Section 3 analyses the relationship between security threats and vulnerabilities. Section 4 proposes the security threat model based on a Markov chain. Section 5 describes the computation method for computing the probability distribution of security threats. Section 6 analyses the application of the proposed method in computing attack probabilities. Section 7 concludes the paper with suggestions for future work.

http://doi.org/10.18080/jtde.v7n1.181

Related work

This section discusses related work concerning security metrics related to probability of security threats, and Markov theory in security metrics.

Security metrics related to probability of security threats

For computing security threat probability based on empirical approach, Aissa *et al.* (2012) introduced a security metric named Mean Failure Cost (MFC) that measures the security of an IT system through quantifying variables including stakeholders and the loss resulting from security threats. It includes several desirable features: it identifies stakeholders and provides the cost for each as a result of a security failure; it measures the financial loss per unit of investigation time ($/h). Despite these appropriate considerations, MFC has a major drawback in that the probability distribution of security threats is based on simple empirical data, while security threats are changeable, dynamic, and specific to different IT systems. Due to the stochastic nature of threats, modelling their probability distributions has become a necessity for any security measuring and predicting system. Relevant and sound classification of threats in terms of deployed vulnerabilities, attack motivation perspectives, and likelihood of successful attacks are essential to facilitate the identification of potential security threats and the development of security countermeasures.

For computing security threat probability using a stochastic model, in (Almasizadeh & Azgomi, 2013), the authors used the attack path concept and time is used to calculate transition probabilities. The authors used probability distribution functions to define the transitions of the model for characterizing the temporal aspects of the attacker and the system behaviour. The stochastic model was recognised to be a semi-Markov chain that was analytically solved to calculate the desirable quantitative security metrics, such as mean time to security failure and steady-state security.

For Probability-Based Security Metrics related to security threat, probability-based security metrics usually express the likelihood of an adversary compromising the system or the probability that the system is secure (Ramos, Lazar, Holanda Filho, & Rodrigues, 2017). (Jha, Sheyner, & Wing, 2002) proposed the reliability metric, which represents the probability of an adversary not succeeding in an attack. This metric was obtained from a continuous time Markov chain generated from assigning transition probabilities to the edges of an attack graph. Formally, the reliability of the network is the probability that, in a sufficiently long execution time, the Markov chain will not be in a security failure state. In case not all transition probabilities are available, due to, for example, lack of data about attacks, the authors proposed a Decision Markov Process approach to compute the reliability

http://doi.org/10.18080/jtde.v7n1.181

metric. (Li, Parker, & Xu, 2011) used a renewal stochastic process to estimate the likelihood that an adversary exploits a randomly selected system vulnerability.

Markov theory in security metrics

For a Markov process, the conditional probability distribution of future states of the process (conditional on both past and present states) depends only on the present state, not on the sequence of events that preceded it. Based on this property, several studies have deployed Markov models for security metrics. (Bar, Shapira, Rokach, & Unger, 2016) used a Discrete Markov Chain Model to predict next honeypot attacks. In (Patcha & Park, 2007), to detect anomaly attacks in an intrusion detection system (IDS), the authors used a Hidden Markov Chain to model this system. (Madan, Goševa-Popstojanova, Vaidyanathan, & Trivedi, 2004) used a Semi Markov Model (SMM) to quantify the security state for an intrusion tolerant system. In this work, Discrete Time Markov Chain (DTMC) steady-state probability was applied to compute the mean time to security failure (MTTSF). Anderson *et al.* (2011) proposed a malware detection algorithm based on the analysis of graphs that represent Markov chains from dynamically collected instruction traces of the target executable. (Almasizadeh & Azgomi, 2013) used an attack path concept and time was used to calculate transition probabilities. In terms of security metrics, most research used Markov models in predicting security attacks or malware propagations. To our best knowledge, few studies consider applying Markov chains and for computing the probability distribution of security threats.

The relationship between cloud security threats and vulnerabilities

In this section, we explore the relationship between security threats and vulnerabilities to identify potential attacks.

A security threat is considered as a potential attack leading to a misuse of information or resources, and vulnerability is defined as some flaws in a cyber space (system) that can be exploited by hackers. As a result, a security threat is a potential attack that may or may not eventuate, but with a potential to cause damage. First, we clarify the cloud security threats based on the Cloud Security Alliance (CSA) report (ALLIANCE, 2016; D. B. Hoang & Farahmandian, 2017). The report released twelve critical security threats specifically related to the shared, on-demand nature of cloud computing with the highest impact on enterprise business.

1. Data Breaches (DB). These are security incidents in which confidential or protected information is released, stolen or used without permission by an attacker.

http://doi.org/10.18080/jtde.v7n1.181

2. Weak Identity, Credential and Access Management (IAM). Attacks may occur because of inadequate identity access management systems, failure to use multifactor authentication, weak password use, and a lack of continuous automated rotation of cryptographic keys, passwords, and certificates.
3. Insecure APIs (Application Programming Interfaces). The security of fundamental APIs is a vital key role in availability of cloud services. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.
4. System Vulnerabilities (SV). These are exploitable bugs in programs that attackers can use to infiltrate a computer system for stealing data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system – kernel, system libraries and application tools – put the security of all services and data at significant risk.
5. Account Hijacking (AH). It is a traditional threat with attack methods such as phishing, fraud, and exploitation of software vulnerabilities.
6. Malicious Insiders (MI). It is defined as a malicious insider threat created by people in organizations who have privileged access to the system and intentionally misuse that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information system.
7. Advanced Persistent Threats (APTs). These are parasitical-form cyber-attacks that infiltrate systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property.
8. Data Loss (DL): for reasons like the deletion by the cloud service provider or a physical catastrophe (including earthquake or a fire) leading to the permanent loss of customer data. Providers or cloud consumers have to take adequate measures to back up data, following best practice in business continuity and disaster recovery – as well as daily data backup and possibly off-site storage.
9. Insufficient Due Diligence (IDD). An organization that rushes to adopt cloud technologies and chooses cloud service providers (CSPs) without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks.
10. Abuse and Nefarious Use of Cloud Services (ANU). Poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment

http://doi.org/10.18080/jtde.v7n1.181

instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.

11. Denial of Service (DOS). DOS attacks are meant to prevent users of a service from being able to access their data or their applications by forcing the targeted cloud service to consume inordinate amounts of finite system resources so that the service cannot respond to legitimate users.
12. Shared Technology Vulnerabilities (STV). Cloud service providers deliver their services by sharing infrastructure, platforms or applications. The infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS) or multi-customer applications (SaaS). This can lead to shared technology vulnerabilities that can potentially be exploited in all delivery models.

A security threat usually exploits one or more vulnerabilities in components of a system to compromise it. The relationship between security vulnerabilities and these recognised threats is thus essential for threat modelling. Hashizume *et al.* (Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013) identified seven major security vulnerabilities in cloud computing:

1. Insecure interfaces and APIs (V1). Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON). The security of the cloud depends upon the security of these interfaces. Vulnerabilities are weak credentials, insufficient authorization checks, and insufficient input-data validation. Furthermore, cloud APIs are still immature, which means that they are frequently changed and updated. A fixed bug can introduce another security hole in the application.
2. Unlimited allocation of resources (V2). Inaccurate modelling of resource usage can lead to overbooking or over-provisioning.
3. Data-related vulnerabilities (V3). This is one of the biggest cloud challenges involving data issues. Data can be co-located with the data of unknown owners (competitors, or intruders) with a weak separation. Data may be located in different jurisdictions which have different laws. Incomplete data deletion – data cannot be completely removed. Data backup is done by untrusted third-party providers. Information about the location of the data usually is unavailable or not disclosed to users. Data is often stored, processed, and transferred in clear plain text.
4. Vulnerabilities in Virtual Machines (V4). Beside data-related issues, vulnerability in Virtual Machines is a big challenge in cloud security. It includes several aspects: possible covert channels in the colocation of VMs; unrestricted allocation and de-

http://doi.org/10.18080/jtde.v7n1.181

allocation of resources with VMs; uncontrolled migration – VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance; uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage. Uncontrolled rollback could lead to reset vulnerabilities – VMs can be backed up to a previous state for restoration, but patches applied after the previous state disappear. VMs have IP addresses that are visible to anyone within the cloud – attackers can map where the target VM is located within the cloud.

5. Vulnerabilities in Virtual Machine Images (V5). Uncontrolled placement of VM images in public repositories. VM images are not able to be patched since they are dormant artefacts.
6. Vulnerabilities in Hypervisors (V6). These vulnerabilities stem from the complexity of the hypervisor code.
7. Vulnerabilities in Virtual Networks (V7). The vulnerabilities are associated with the sharing of virtual bridges by several virtual machines.

Table 1: Relationship between security threats and vulnerabilities

	Threat	Description	Vulnerabilities	Incidents
1	DB	Data Breaches	V1, V3, V4, V5, V7	An attacker can use several attack techniques involved, like SQL, command injection, and cross-site scripting. Virtualization vulnerabilities can be exploited to extract data.
2	IAM	Weak Identity, Credential and Access Management	V1, V3	An attacker can leverage the failure to use multifactor authentication, or weak password uses.
3	API	Insecure interfaces and APIs	V1	An attacker can take advantage of weaknesses in using APIs like SOAP, HTTP protocol. Bugs in APIs can be also exploited.
4	SV	System Vulnerabilities	V4, V5, V6, V7	An attacker can attack via vulnerabilities in Virtual Machine images, in Hypervisors, and in Virtual Networks.
5	AH	Account Hijacking	V1	To get system access, attackers can use the victim's account
6	MI	Malicious Insiders	V5, V7	An attacker can generate a VM image embracing malware, then propagate it.
7	APT	Advanced Persistent Threats	V1, V4, V5, V6, V7	An attacker can use several kinds of vulnerabilities from specific virtual cloud or APIs to infect bugs permanently in the target system for mainly scavenging data.
8	DL	Data Loss	V3, V4, V7	An attacker can use data-driven attack techniques to gain confidential information from other VMs co-located in the same server; or use the risk of data backup, storing process to scavenge data.
9	IDD	Insufficient Due Diligence	V4, V6	An attacker can leverage weaknesses in complying with rules in using cloud system like configuration of VMs, data and technology shares.
10	ANU	Abuse and Nefarious Use of Cloud Services	V4	An attacker can attack, through use and share of servers, data of customers by using an anonymous account.
11	DOS	Denial of Service	V1, V2	An attacker can request more IT resources, so authorised users cannot get access to the cloud services.
12	STV	Shared Technology Vulnerabilities	V4, V6	An attacker can sniff and spoof virtual networks or exploit the flexible configuration of Virtual Machines or hypervisors.

http://doi.org/10.18080/jtde.v7n1.181

We identify and tabulate the connection between security threats and vulnerabilities in Table 1. It is seen that a security threat may have several security vulnerabilities and one vulnerability may be exploited by several security threats. For example, in terms of threat Data Breaches (DB), five vulnerabilities are involved in this security threat: Insecure interfaces and APIs (V1), Data-related vulnerabilities (V3), Vulnerability in Virtual Machines (V4), Vulnerabilities in Virtual Machine Image (V5), and Vulnerabilities in Virtual Networks (V7). Ristenpart *et al.* (Ristenpart, Tromer, Shacham, & Savage, 2009) indicated that confidential information can be extracted from VMs co-located in the same server. An attacker may use several attacks to collect data by exploiting vulnerabilities in brute-forcing, measuring cache usage, and load-based co-residence detection data processing techniques in cloud systems. Therefore, data leakage depends not only on data-related vulnerabilities but also on virtualization vulnerabilities.

Table 1 indicates that the data-related vulnerability (V3) is involved in three security threats. First, it may cause the threat Data Breaches (DB), when an attacker uses several techniques like SQL injection or cross-site scripting to attack the cloud system. Second, it may lead to the threat Weak Identity, Credential and Access Management (IAM), where an attacker may leverage the data that is often stored, processed, and transferred in clear plain text to gain access to the cloud system. Third, it may cause the threat Data Loss (DL), when an attacker exploits several related vulnerabilities like different located data, incomplete data deletion, and data backup.

Markov model for successful attacks

We introduce a Markov process to describe a cloud attack model and use the CVSS to determine the transition matrix of the proposed Markov model.

A security threat is a stochastic process. We model it as a Markov chain. The probability of transition from one state to others is based on the vulnerabilities present in the current state. An attacker exploits various vulnerabilities to arrive at a security threat state and eventually reaches the final failure state. At this stage, we mainly focus on a first level of abstraction with visible and quantifiable states and construct 3 states, namely the secure state (S), the threat state (T), and the failure state (F). Figure 1 depicts the proposed Markov model for modelling security threats and attacks with state transition probabilities, where α denotes the transient probability from state S to state T, β denotes the transient probability from T back to S, γ denotes the probability to change the state from T to F, δ denotes the transient probability from F state back to T state, ε denotes the possibility from F state back to S state. The model takes all elements of an attack mode into account, including attack, defense and recovery factors of the system. We do not present the direct transition probability from state

http://doi.org/10.18080/jtde.v7n1.181

S to state F for several reasons. First, we are investigating the impact of security threats on system failure and how an attacker takes advantage of security threats. An attacker tries to exploit vulnerabilities to change from secure state to threat state. Second, the system collapses (goes directly from S to F) mainly in the case of natural disasters or similar catastrophes. This model is simple and practical for our consideration. Even with this 3-state model, it is difficult to derive a set of data for its complete description. We refine the model in several steps of our investigation.

Figure 2 shows the attack model with the defense elements absorbed into the failure state. It means there is no transient probability from F to T or from F to S. When the process reaches F, it stays there with probability 1. This means the recovery process is not taken into account.

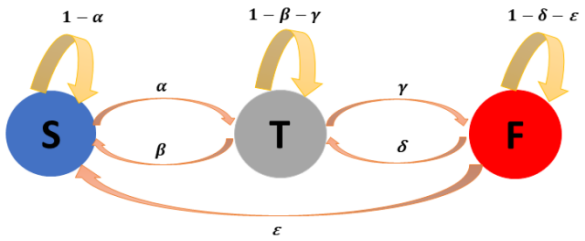

Figure 1. Diagram of attack model with defence and recovery

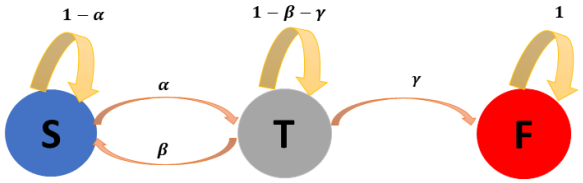

Figure 2. Diagram of attack model with defence and without recovery

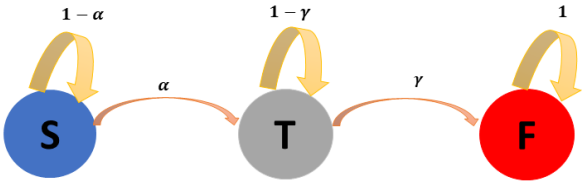

Figure 3. Diagram of attack model without defence and recovery

Figure 3 shows the attack model with the defense efforts absorbed both at the threat state and the failure state. We focus on this kind of abstraction of this model. The aim is to compute the successful chance of attacks by an attacker deploying vulnerabilities of a threat. We do not take into account the recovery element of the system at this stage of investigation, as it can be incorporated at a later stage. Furthermore, recovery efforts largely depend on the manager of the system and relevant data is not often disclosed. The probability from S to T also means the overall probability that includes the defense element that the system tries to change state from T back to S.

We are interested in finding the transition probability from state S to state F in the attack sequence. The Chapman–Kolmogorov equation (Ross, 2014) is available to find the transient

http://doi.org/10.18080/jtde.v7n1.181

probability between two states after a number of jump-steps. The transition probability can be calculated by matrix multiplication. Therefore, to derive the transition probability between two states in a number of steps, the Chapman–Kolmogorov equation can be used as follows:

$$P_{ij}^{m+n} = \sum P_{ik}^{m} P_{kj}^{n} \quad (1)$$

where P is the probability matrix of transitions in the state space. P_{ij}^{m+n} is the transition probability from state i to state j after (m + n) steps via any state k.

Distribution of security threat probabilities

To compute the distribution of security threat probabilities based on a Markov chain, 3 phases can be presented as follows: modelling security threats as a Markov chain; building a transition probability matrix; computing the transition probability from state S to state F via each threat T.

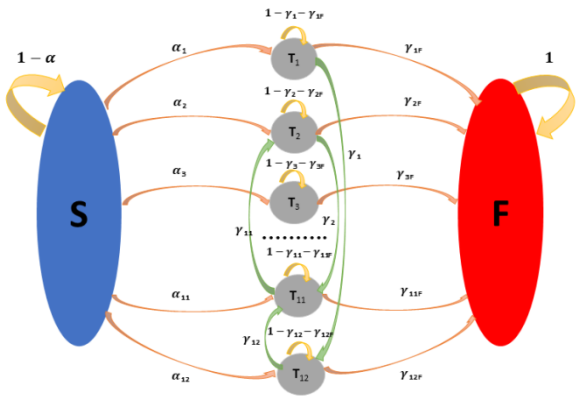

Figure 4. Security threat model with attack process

Phase 1: modelling security threats as a Markov chain. Figure 4 shows an attack model that expands the general model in Figure 3 with twelve attack paths. This is modelled as a Markov chain with fourteen states, including a security state, a failure state, and twelve threat states. The security state is defined as a state of the system that has no failure or security threats. The failure state is a state when the system fails to meet its minimum requirements. The threat state is considered as a middle state that an attacker could exploit a specific set of vulnerabilities. Attack path can be defined as a possible way that an attacker starts from security threat to reach failure state through threat states. In this model, we assume that the probability of an attack path is the overall probability that includes the defense element. This is a simplification, as it is possible that the system can move from one threat state to other determined threat states to reach the failure state.

http://doi.org/10.18080/jtde.v7n1.181

Phase 2: building transition probability matrix. The probability of each attack path is considered as the probability of changing state security to failure caused by each security threat. An attacker leverages security vulnerability of each security threat (the attack path) to attack to reach the failure state of the cloud system. From the attack model (see Figure 4) we arrive at a transition probability P_{ij} matrix with fourteen states including security, failure, and twelve threat states.

$$P = \begin{bmatrix} 1-\alpha & \alpha_1 & \cdots & \alpha_{12} & 0 \\ 0 & 1-\gamma_1-\gamma_{1F} & \cdots & \gamma_1 & \gamma_{1F} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1-\gamma_{12}-\gamma_{12F} & \gamma_{12F} \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

In this matrix, α is the sum of probability of all attack paths from S state to T states; and γ_F is the sum of the probability of all threat states to the failure state. Once the system is in the security state, it will remain in this state with probability (1-α) and, once the system is in the failure state, the probability of remaining in this state is 1 (the absorbing state). The probabilities of attack paths representing from S to T states are α_1, α_2, α_3 etc. The probabilities of attack paths representing from threat states to the failure state are γ_{1F}, γ_{2F}, γ_{3F} etc. There are also transition probabilities from one state to other states. However, for demonstration purposes, it is assumed that there is one path from one threat state to another threat state. These probabilities are presented as $\gamma_1, \gamma_2, \gamma_3$ etcetera.

Phase 3: computing the transition probability from state S to state F via threats T_i. According to attack paths theory, each attack-path represents the path that the attacker will take advantage of to reach the failure state (F) from a threat state (T) by exploiting the set of vulnerabilities (v_{ij}) of each security threat. For example, we assume that attack path 1 represents the path where the attacker exploits vulnerability of threat 1 (Data Breaches-DB). Thus, there is a distribution of probability of attack paths when attackers may choose one path to attack in the space of attack paths. To quantify this distribution, we use the concept of weight of each path. CVSS (NVD, 2018) can be used to weigh each path from S to T, from T to F, or between threats to calculate transition probabilities. The weight associated with the transition from S to T_i is determined by computing the ratio between vulnerability scores from S to T_i and all vulnerability scores from S to all threats. By using (2) below, the transition probabilities (α_i) from S to T_i can be calculated. Similarly, the transition probabilities (γ_{iF}) from T_i to F can be computed using (3). To compute the transient probability S to F via T_i, ($P(SF)_i$), (1) can be used to compute the value in any number of jump-steps. However, at this stage, for the purpose of demonstrating the threat model based on the Markov chain, we

http://doi.org/10.18080/jtde.v7n1.181

compute $P(SF)_i$ in two jump-steps using (4). In this case, the probability between threats may not be considered.

$$\alpha_i = \frac{\sum_j v_{ij}}{\sum_{k,l} v_{kl}} * \alpha \tag{2}$$

$$\gamma_{iF} = \frac{\sum_j v_{ij}}{\sum_{k,l} v_{kl}} * \gamma_F \tag{3}$$

$$P^2(SF)_i = P^2 = \alpha_i * \gamma_{iF} \tag{4}$$

In these equations, i is the index of an attack path, v_{ij} is the vulnerability score of vulnerability j associated path i, $k \epsilon P$ is the set of attack paths.

Table 2. Vulnerability scores

Vulnerability	Acronym	Exploitability score
CVE-2017-14925	V1	8
CVE-2014-4064	V2	2
CVE-2015-5255	V3	3
CVE-2015-4165	V4	5
CVE-2016-0264	V5	7
CVE-2015-1914	V6	5
CVE-2017-6710	V7	7

To calculate the probability distribution of security threats, we need to determine elements of the Markov transition matrix based on the vulnerabilities associated with a threat. From the security state S, the total probability that the system moves to one of the threat states is assumed to be α (α = 0.0318 (Jouini & Rabai, 2015)). We can determine the transition probability that the system moves from S to T_i as the ratio of the sum of vulnerability scores of threats associated with T_i over the total CVSS scores of all threats.

Table 2 shows the CVSS scores (NVD, 2018) associated with relevant vulnerabilities considered in this paper. According to CVSS, this number is a score out of ten. For example, V1 scores eight out of ten because the severity of this vulnerability is very high once it is related to cloud data breach vulnerabilities. In addition, to go to state T_1 from S, an attacker needs to exploit the certain set of vulnerabilities associated with the security threat state T_1. In this case, vulnerabilities one, three, four, five, and seven will be exploited (see Table 1). Therefore, the number of vulnerability scores for the attack path one is W1=V1+V3+V4+V5+V7=30 and the total number of all vulnerability score from S to any T_i is

http://doi.org/10.18080/jtde.v7n1.181

W=177. We can estimate the transition probability from S to T1 ($\alpha_1 = 30/177 * \alpha = 0.00539$). Similarly, other transition probabilities from S to T_i will be computed by using (2). We assume that the transition probability from state T_i to F is highly likely with probability $\gamma_{iF} = 0.95$ for any attack paths (see Figure 4). By computing α_i and γ_{iF}, the transition probability matrix P is obtained. Then by using (1) and (4), we have the probabilistic distribution of twelve security threats expressed in Table 3.

Table 3 Probability distribution of twelve security threats

	Threats	Formula	Probability ($\times 10^{-3}$)
1	DB	$\alpha_1 * \gamma_{1F}$	5.1203
2	IAM	$\alpha_2 * \gamma_{2F}$	1.8774
3	API	$\alpha_3 * \gamma_{3F}$	1.3654
4	SV	$\alpha_4 * \gamma_{4F}$	4.0962
5	AH	$\alpha_5 * \gamma_{5F}$	1.3654
6	MI	$\alpha_6 * \gamma_{6F}$	2.3894
7	APT	$\alpha_7 * \gamma_{7F}$	5.4616
8	DL	$\alpha_8 * \gamma_{8F}$	2.5601
9	IDD	$\alpha_9 * \gamma_{9F}$	1.7067
10	ANU	$\alpha_{10} * \gamma_{10F}$	0.8533
11	DOS	$\alpha_{11} * \gamma_{11F}$	1.7067
12	STV	$\alpha_{12} * \gamma_{12F}$	1.7067

As seen in Table 3, threat Advanced Persistent Threat (APT) has the highest probability (0.55%). The second highest probability is threat Data Breach with 0.51%. Threat Abuse and Nefarious Use of Cloud Services (ANU) has lowest probability with 0.08%. From the distribution of security threat probability, the highest chance for attacking the cyber system relates to threat Data Breaches (DB). In terms of security management, security experts needs to give a decision to protect data or to protect against advanced persistent attacks

Estimation of security attack probability

In this section, to compute the security attack probability, the relationship between attack types and security threats will be investigated. Then, we introduce the probabilistic method to determine the security attack probability distribution.

Relationship between attack types and security threats

A security attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorised access or permission. In other words, a security attack is an attempt to gain unauthorised access to information

http://doi.org/10.18080/jtde.v7n1.181

resources or services, or to cause harm or damage to cyber systems. It is clear that an attack type relates to security threats. An attack type can use one or several security threats and one threat can involve several attack types. We investigate the relationship between attack types and security threats (Table 4). In (Singh & Shrivastava, 2012), there are five major types of security attack in cloud computing. It is impossible that an attacker can exploit all vulnerabilities in the vulnerability space. Apparently, an attacker or a group of attackers just can exploit several determined security vulnerabilities. These vulnerabilities often are grouped into categories. These categories can be identified by different security threats. Each of these groups of attacks will have specific features that can be recognised and differentiated from other groups. Each group of attacks will fit several security threats. Five different groups of attack and their connection with security threats will be investigated as follows.

1. DOS attacks (A1)

Attackers will take advantage of the availability feature of a cloud system; they aim to overload a target server with service requests in such a way that it is unable to respond to any new request and hence resources are made unavailable to its users. This can be illustrated in several scenarios: (1) Overloading a target with a large amount of junk data, like UDP floods, ICMP floods etc.; (2) Using blank spaces in various protocols to overload target resources, like SYN floods, fragment packet attack, ping of death; (3) Initiating numerous HTTP requests so that they cannot be handled by the server in an HTTP DDOS attack or XML DDOS attack. It is clear that this attack type is related to the threat DOS (T11) and threat MI (T6), when attackers take advantage of a malicious insider to build the botnet for DDOS attacks.

2. Cloud malware injection attack (A2)

Attackers may try to inject a malicious service or even a virtual machine into a cloud system in order to hijack a user's service for their own purposes. These may include data modification, full functionality changes/reversals or blockings. Cloud malware injection attack groups tend to exploit security vulnerabilities that relate to security threats such as data breach, insecure interfaces and APIs, system vulnerabilities, malicious insider, and advanced persistent attack. This type of attack corresponds to 5 threats: DB (T1), API (T3), MI (T6), APT (T7) and DL (T8), when attackers use malicious insiders or advanced persistent threats to inject malware to take control of a cloud system, especially in database management.

3. Side-channel attacks (A3)

An attacker could attempt to compromise a cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side-channel attack. Side-channel attacks have emerged as an active type of security attack targeting system

http://doi.org/10.18080/jtde.v7n1.181

implementation of cryptographic algorithms. This type of attack has a close relationship with several threats such as: (1) AUN (Abuse and Nefarious Use of Cloud Services – T10) when an attacker attacks through using and sharing the servers so that the attacker can implement its malicious virtual machine to perform a side-channel attack; and (2) STV (Shared Technology Vulnerabilities – T12).

4. Authentication attacks (A4)

Authentication is a weak point in cloud computing services and is frequently targeted by an attacker. Today, most of the services still use simple username and password type of knowledge-based authentication. Some authentication attacks are: (1) Brute Force Attacks, where exhaustive combinations of a password are applied to break the password security. This brute force attack is generally applied to crack encrypted passwords when they are saved in a form of encrypted text. (2) Dictionary Attack: unlike the brute force attack, rather than searching all possibilities, the dictionary attack tries to match a password with most occurring words or words of daily life usage and hence it is more effective in terms of speed. (3) Shoulder Surfing: it is an alternative name for "spying" in which an attacker spies on a user's movements to gain his/her password. Here, the attacker observes the way a user enters the password, i.e. what keys of the keyboard the user has pressed. (4) Other related attacks such as Replay Attacks, Phishing Attacks, and Key Loggers. The authentication attack group is related to password attacks; hence, it is pertinent to security threats including: (1) IAM (Identity and Access Management – T2), when an attacker can take advantage from the failure to use multifactor authentication or strong passwords; (2) AH (Account Hijacking) by using a victim's account to get access to the target's resources; (3) ANU (Abuse and Nefarious Use of Cloud Services – T10), when an attacker attacks through using and sharing the servers to gain access to customers' data through an anonymous account. Therefore, A4 has a relationship with T2, T5, and T10.

5. Man-In-The-Middle Cryptographic attacks (A5)

A man-in-the-middle attack is one in which an attacker intercepts messages in the public key exchange process and then retransmits them, substituting his/her own public key for the requested one, so that the two original parties still appear to be communicating with each other. Through this process, the two original parties appear to communicate normally without being aware of the intruder. The message sender does not recognise that the receiver is an unknown attacker trying to access or modify the message before retransmitting it to the receiver. Thus, the attacker controls the entire communication. MIM attacks include: (1) Address Resolution Protocol Communication (ARP) – in the normal ARP communication, the host PC will send a packet which has the source and destination IP addresses and will

http://doi.org/10.18080/jtde.v7n1.181

broadcast the packet to all the devices connected to the network; (2) ARP Cache Poisoning, in which the attacker sniffs the network by controlling the network switch to monitor the network traffic and spoofs the ARP packets between the host and the destination PCs and then performs a MIM attack; and (3) others including DNS Spoofing or Session Hijacking. This attack group (A5) is related to several threats: (1) IAM (Weak identity, Credential and Access Management – T2), when attackers leverage the weakness in using multifactor authentication or fake information leading to loss of credentials; (2) AH (Account Hijacking – T5) by sniffing the connection to catch the cookies of victims between their PC and the web server, then using the cookies to bypass the system. So A5 has connection with T2 and T5.

Table 4. Relationship between security attack types and security threats

	Type	Description	Threats	Incident
1	A1	Denial of Service	T6, T11	Making overloaded requests to the system to stop availability of servers
2	A2	Malware Cloud Injection	T1, T3, T6, T7, T8	Injecting malicious virtual machine or service to get the victim's access to the cloud system
3	A3	Side-Channel attack	T10, T12	Using and sharing the servers
4	A4	Authentication attack	T2, T5, T10	Using weak passwords, sharing technology
5	A5	Man-in-the-middle	T2, T5	Using weakness of multifactor authentication and the cookies of users

Computing the attack type probabilities

Probability computation of an attack type is based on the probability of the set of security threats. It is can be presented mathematically as $Pr(A_i) = Pr(T_1\ and\ T_2\ or\ T_3 \ldots)$. However, in this paper, we assume that each attack path presents a security threat. There are no relations between these security threats: each threat is independent from other threats. Therefore, the probability of an attack type is the union of the probability of the attack-related security threats. It is formulated as follows:

$$P(A_i) = P\left(\bigcup_{j=1}^{N} T_j\right) = \sum_{j}^{N} P(T_j) - \sum_{1\le j<k\le N} P(T_j \cap T_k) + \sum_{1\le j<k<l\le N} P(T_j \cap T_k \cap T_l) - \sum_{1\le j<k<l<m\le N} P(T_j \cap T_k \cap T_l \cap T_m) + \cdots \quad (6)$$

This probability of the union of any number of sets can be expressed as the following steps: (1) Add the probabilities of the individual threats; (2) Subtract the probabilities of the intersections of every pair of events; (3) Add the probabilities of the intersection of every set of three events; (4) Subtract the probabilities of the intersection of every set of four events; (5) Continue this process until the last probability is the probability of the intersection of the total number of sets that we started with (Taylor, 2019). The probability of an attack type is computed by using (6). For example, to compute the probability of attack DOS (A1), we have $Pr(A_1) = \Pr(T_6\ or\ T_{11}) = \Pr(T_6) + \Pr(T_{11}) - \Pr(T6\ and\ T11) = \Pr(T_6) + \Pr(T_{11}) - \Pr(T_6) *$

http://doi.org/10.18080/jtde.v7n1.181

$\Pr(T_{11}|T_6)$. Because T_6 and T_{11} are independent, $\Pr(T_{11}|T_6) = \Pr(T_{11})$, and therefore $Pr(A_1) = \Pr(T_6) + \Pr(T_{11}) - \Pr(T_6) * \Pr(T_{11}) \approx 0.0041$. Similarly, applying the above algorithm by using (6), we will have the probability distribution of five attack types seen in Table 5.

As seen in Table 5, attack type Malware Cloud Injection (A2) has the highest probability at 1.67%. The second highest probability is attack type Denial of Service (A1) at 0.41%. The lowest probability is attack type Side-Channel Attack (A3) with 0.2%. The distribution of attack probability provides several implications. For an attack countermeasure plan, security practitioners need to care about methods to prevent malware cloud injection attacks, because the chance of this type of attack is highest. For a security manager to make a decision on security investment, it may depend on not only the probability of an attack but also the consequences of this successful attack, because, in several scenarios, the probability of an attack is very small, but the impact is very high in terms of money. As a result, the average security cost, which is the product of the probability of an attack and the consequence of this attack, is quite high. In this case, the manager can prioritise security actions against the kind of attack that makes more damage – for example, if the consequence of denial of service attacks (A1) is ten times higher than that of malware cloud injection (A2), at $1,000,000 and $100,000, respectively. In this case, using the figures from Table 5, the security cost for A1 is $1,000,000 x 0.00409=$4,092, while the security cost for A2 is $100,000 x 0.016=$1,667. Therefore, the security cost for A1 is nearly two-and-a-half times higher than the security cost for A2.

Table 5: Probability distribution of five attack type

	Attack	Description	Probability ($\times 10^{-3}$)
1	A1	Denial of Service	4.092
2	A2	Malware Cloud Injection	16.679
3	A3	Side-Channel attack	2.559
4	A4	Authentication attack	4.091
5	A5	Man-in-the-middle	3.240

Conclusion

This paper has proposed a novel security threat model to compute security threat probability as a metric to measure the security of a cyber-system. For this purpose, we applied a Markov chain model with three states to identify the attack paths through various security threats. Twelve security threats reported by the Cloud Security Alliance and seven security vulnerabilities scored by the Common Vulnerability Scoring System were investigated to quantify the parameters of the proposed security threat model and to compute the

http://doi.org/10.18080/jtde.v7n1.181

probability distribution of security threats. The probability distribution for cloud attack types also was calculated based on the security threat model. Several scenarios for using the probability distribution of security threats and attacks in cloud security management were explained. One of the limitations in the model is that the relationships between security threats have not been taken into account. Several directions are being considered for our future work: one would be to extend the proposed model to include the interrelationship among cloud security threats; another direction is to explore a new model for estimating the distribution of the consequences over the system's constituents or stakeholders once the probability of the materialised threat has been estimated. This will open up research into the area of quantitative cyber security risks.

References

Aissa, A. B., Abercrombie, R. K., Sheldon, F. T., & Mili, A. (2012). Defining and computing a value based cyber-security measure. *Information Systems and e-Business Management*, *10*(4), 433-453.

Almasizadeh, J., & Azgomi, M. A. (2013). A stochastic model of attack process for the evaluation of security metrics. *Computer Networks*, *57*(10), 2159-2180.

Anderson, B., Quist, D., Neil, J., Storlie, C., & Lane, T. (2011). Graph-based malware detection using dynamic analysis. *Journal in Computer Virology*, *7*(4), 247-258.

Aroms, E. (2012). *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30.

Bar, A., Shapira, B., Rokach, L., & Unger, M. (2016). Identifying Attack Propagation Patterns in Honeypots Using Markov Chains Modeling and Complex Networks Analysis. Paper presented at the *2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE)*.

CIS [Center for Internet Security]. (2010). The CIS security metrics. Available at http://www.itsecure.hu/library/image/CIS_Security_Metrics-Quick_Start_Guide_v1.0.0.pdf

Cloud Security Alliance. (2016). *The Treacherous Twelve - Cloud Computing Top Threats in 2016*. From https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

Ghayvat, H., Mukhopadhyay, S., Liu, J., Babu, A., Alahi, M. E. E., & Gui, X. (2015). Internet of things for smart homes and buildings. *Australian Journal of Telecommunications and the Digital Economy*, *3*(4).

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5.

Hoang, D. (2015). Software Defined Networking? Shaping up for the next disruptive step? *Australian Journal of Telecommunications and the Digital Economy*, *3*(4).

Hoang, D. B., & Farahmandian, S. (2017). Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies. In S. Y. Zhu, S. Scott-Hayward, L. Jacquin, & R. Hill (Eds.), *Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications* (pp. 3-32). Cham: Springer International Publishing.

http://doi.org/10.18080/jtde.v7n1.181

Hu, Q., Asghar, M. R., & Brownlee, N. (2017). Evaluating network intrusion detection systems for high-speed networks. Paper presented at the *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*.

Huang, K., Zhou, C., Tian, Y.-C., Tu, W., & Peng, Y. (2017). Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks. Paper presented at the *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*.

Jha, S., Sheyner, O., & Wing, J. (2002). Two formal analyses of attack graphs. *Proceedings. 15th IEEE Computer Security Foundations Workshop, 2002*.

Jouini, M., & Rabai, L. B. A. (2015). Mean Failure Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study. *Journal of Computers*, *10*(3), 184-194.

Le, N. T., & Hoang, D. B. (2017). Cloud Maturity Model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience*, *4*, 277-290.

Li, X., Parker, P., & Xu, S. (2011). A stochastic model for quantitative security analyses of networked systems. *IEEE Transactions on Dependable and Secure Computing*, *8*(1), 28-43.

Madan, B. B., Goševa-Popstojanova, K., Vaidyanathan, K., & Trivedi, K. S. (2004). A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation*, *56*(1), 167-186.

NIST. (2018). National Vulnerability Database. Available at https://nvd.nist.gov/

Patcha, A., & Park, J.-M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, *51*(12), 3448-3470. doi: https://doi.org/10.1016/j.comnet.2007.02.001

Patel, S., & Zaveri, J. (2010). A risk-assessment model for cyber attacks on information systems. *Journal of Computers*, *5*(3), 352-359.

Ramos, A., Lazar, M., Holanda Filho, R., & Rodrigues, J. J. (2017). Model-Based Quantitative Network Security Metrics: A Survey. *IEEE Communications Surveys & Tutorials*, *19*(4), 2704-2734.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM conference on Computer and communications security*.

Ross, S. M. (2014). *Introduction to probability models*. Academic press.

Singh, A., & Shrivastava, D. M. (2012). Overview of attacks on cloud computing. *International Journal of Engineering and Innovative Technology (IJEIT)*, *1*(4).

Taylor, C. (2019). Probability of the Union of Three or More Sets. Retrieved March 5, 2019, from https://www.thoughtco.com/probability-union-of-three-sets-more-3126263

Thomson, W. (1889). *Lord Kelvin: Electrical units of measurement. Popular lectures and addresses*. Macmillan, London.

How to Transition the National Broadband Network to Fibre To The Premises

Mark A Gregory
RMIT University

Abstract: NBN Co, the government business enterprise rolling out the National Broadband Network (NBN) adopted the Coalition Government's Multi-Technology Mix (MTM) plan upon receipt of a revised Statement of Expectations following the September 2013 Federal election. The MTM NBN plan included rolling out the outdated Fibre to the Node technology and remediating and upgrading the existing Telstra and Optus Hybrid Fibre Coaxial networks. This paper discusses the migration from the MTM NBN to a Fibre to the Curb or ubiquitous Fibre to the Premises (FTTP) NBN. The paper also discusses the MTM NBN cost blowout, delays and rationale for the MTM NBN to be immediately replaced with a future-proof FTTP NBN.

Keywords: Telecommunications, Wholesale, Broadband, National Broadband Network, Policy, Regulation

Introduction

In an earlier paper (Gregory, 2018) four options were identified for the future ownership of the National Broadband Network (NBN). A decision on future NBN ownership arrangements is expected by the government of the day in mid-2022, if not earlier. It is anticipated that sale arrangements, if this was the option selected by the government, would not be able to be put in place prior to 2024 due to the need for legislative and regulatory changes to reflect the new conditions upon which telecommunications infrastructure would be owned and operated nationally.

NBN Co, the company building and operating the NBN, states (NBNCO, 2019a) that it will complete the NBN rollout by mid-2020 with a "commitment to deliver access to peak wholesale download data rates of at least 25 megabits per second (Mbps) to all premises across the network, and at least 50Mbps peak wholesale download data rates to 90 per cent of the fixed-line network."

http://doi.org/10.18080/jtde.v7n1.182

NBN Co reported (NBNCO, 2019a) that monthly average revenue per user (ARPU) had risen to $45, 8.1 million premises were ready to connect, 4.7 million premises were activated on the NBN and revenue had risen to $1.3 billion for the six months ending on 31 December 2018.

NBN Co's business model remains under pressure prompting calls for a Government debt write-off post-build (Smith, 2018)(Dickinson, 2018).

The Coalition Government's MTM NBN was put to voters in 2016 with promises that the NBN rollout would be completed by 2019 with an ARPU of $51 per month making the NBN cash flow positive. However, rollout delays have caused NBN Co to adjust its targets to over 8 million homes and businesses connected by 2020 and projected ARPU of $51 per month by FY22 (NBN Co,2019b) .

A lower than expected connection rate (NBN Co,2019b) to the NBN, the threat of 5G taking a larger than expected slice of the broadband market and NBN Co's poor financials, partially brought about by the decision to rollout the effectively obsolete fibre to the node (FTTN) and to remediate the Hybrid Fibre Coaxial (HFC) network.

NBN Co has remained mute on how it expects to be able to meet demand for new applications and services that require high bandwidth, low latency, improved reliability. Publicly, NBN Co states that it can meet the demand and performance requirements forecast through to 2026, but the reality is that many consumers are frustrated by the underlying reliability and performance problems with the NBN that go far beyond the daily congestion caused by NBN Co's excessive Connection Virtual Circuit (CVC) charge (essentially a data usage charge).

To meet consumer demand and performance expectations, NBN Co is expected to replace FTTN (Gregory, 2015a) with either Fibre to the Curb (FTTC) (Gregory, 2017) or Fibre to the Premises (FTTP). This paper discusses three options and associated costings.

The NBN is not fit for purpose

In August 2014, the former NBN Co CEO Bill Morrow voiced doubts (Bender, 2014) about the Vertigan panel report that was commissioned by the former Prime Minister Malcolm Turnbull when he was Minister for Communications (Turnbull, 2013). In this report it was predicted that the median Australian household would require 15 Mbps in 2023. Mr Morrow said that he was "curious" about the prediction.

In February 2018, the Bureau of Communications and the Arts Research (BCAR) within the Department of Communications and the Arts released a working paper (BCAR, 2018) that claims that "peak bandwidth demand for the highest usage households is forecast to increase from between 11–20 megabits per second (Mbps) in 2016 to between 20–49 Mbps in 2026. 98 per cent of households are estimated to demand less than this amount of bandwidth in

http://doi.org/10.18080/jtde.v7n1.182

2026—that is, only 2 per cent of households are expected to demand more than 49 Mbps in bandwidth."

It is possible to see a trend here. The Coalition Government is guilty of using every resource at its disposal in an ongoing attempt to justify the unreliable, poor performance and fiscal irresponsibility attached to the MTM NBN.

In 2014, when the Vertigan panel report was released there was public criticism (Gregory, 2014)(Crozier, 2018) of the findings, particularly the low bandwidth demand projection that supported the earlier claims by the Coalition government (RAFC, 2016) that the NBN would provide all Australians with 25 Mbps NBN connections by 2016 for $29.5 billion and that this outcome would be satisfactory for a majority of consumers for about a decade.

Having failed to meet the commitment made during the MTM NBN policy launch in 2013, the Coalition government shifted the goal post to a target of "50 and 100 megabits per second by the end of 2019 in 90 per cent of the fixed line footprint." The 2018 BCAR report can be seen to dovetail nicely with this Coalition government commitment.

In January 2019 at the Consumer Electronics Show the focus was on 8K televisions (News, 2019). In 2020, the Tokyo Olympics organisers plan to stream the games in 8K format. The bandwidth required for a poor quality 8K stream is about 50 Mbps per channel and for an improved quality the bandwidth is 80-120 Mbps. The instantaneous bandwidth required to support fast forward, rewind and other functions can require a 50 per cent short term increase in the average bandwidth requirement (Dow, 2016)(Gregory, 2016).

In addition to many Australians not having broadband infrastructure that will support reasonable congestion free viewing of the Tokyo Olympics in 8K, there are augmented reality and virtual reality applications being developed that require more than 1 Gbps connection speeds.

In Australia, most of the over-the-top application and service providers have remained relatively mute, the reason for this silence remains a task for future research.

One streaming media provider, FoxTel has provided clear guidance on why the Coalition Government's MTM NBN is not "fit for task" today, let alone when 8K media streaming becomes the norm globally over the next couple of years.

FoxTel states online "Don't you hate it when you've maxed out your internet capacity and the speed drops faster than a Walking Dead zombie with a knife to the noggin? Say goodbye to that issue, as satellite will guarantee 4K delivery" (FoxTel, 2018).

Foxtel provides a table titled "Understanding nbn™ speeds" (FoxTel, 2019) that recommends a Plus Speed tier or a Premium Speed tier depending on household demand.

http://doi.org/10.18080/jtde.v7n1.182

The Plus Speed tier *"is ideal for use of the internet by 3-4 people at the same time, for activities like:*

- *Regular uploading & downloading of large files*
- *Online gaming*
- *Streaming in Ultra HD (4K) quality*
- *Moderate simultaneous use of several devices*
- *Included in Foxtel Broadband Unlimited plans"*

The Premium Speed "*is ideal for use of the internet by more than 5 people at the same time, for activities like:*

- *Constant uploading & downloading of large files*
- *Online gaming*
- *Streaming in Ultra HD (4K) quality*
- *Heavy simultaneous use of several devices*
- *Once you've signed up, you can check your eligibility for an upgrade to Premium speed (for an additional fee) by calling xxx xxx"*

FoxTel has provided an indication that the typical evening speed for the Plus Speed tier of 44.6 Mbps and for the Premium Speed tier of 85 Mbps "Based on Foxtel's typical busy Period download speed measurement between 7pm and 11pm, collected from 15/02/2019 - 28/02/2019. Your actual speeds on Fibre to the Basement (FTTB) and Fibre to the Node (FTTN) services will be confirmed once your home is connected."

Rather than demanding improved infrastructure, companies are now "squeezing" the connection speeds and capacity needed to make their applications and services work over FTTN and the end result is poor quality, especially for streamed media, reduced availability, congestion and a poor consumer experience.

Telecommunications is an essential service. Without adequate, reliable telecommunications, Australia's economy is negatively impacted. The introduction of the NBN is having a positive impact on the average fixed broadband connection speeds, but relative to our competitors in the global digital economy, Australia is falling further behind.

The Ookla speedtest global rankings provide a reflection on global broadband penetration and connection speeds that can be used to provide general guidance. Australia was ranked 60th in the latest global speed ranking (Ookla, 2019). Whilst Australia's NBN provides national

http://doi.org/10.18080/jtde.v7n1.182

coverage and some of the nations ranked above Australia do not do so for fixed broadband, these nations have not committed more than $51 billion to complete their broadband networks.

Are Australian taxpayers getting value for the $51 billion committed by the Australian government to the MTM NBN? In respect of most measures the MTM NBN is not fit for purpose. It is not future proof, it does not meet current nor future demand, it is unreliable and has a higher OPEX than that for a ubiquitous FTTP network. It has cost significantly more and taken significantly longer than the Coalition Government argued were prime reasons for adopting the second rate MTM NBN rather than continuing with the FTTP rollout.

Technology upgrade

A decision to carry out a technology upgrade should be based on criteria including demand, performance, CAPEX, OPEX, capital availability and the effect of the upgrade on NBN Co's business model.

In this section the options available to NBN Co are explored with the assumption that NBN Co would remain a single entity, either government owned or privatised, possibly through an amalgamation with a recently separated and listed InfraCo (Telstra's current infrastructure division) (Irving, 2018).

In New Zealand, Chorus, the largest broadband wholesale provider, carried out a comparative analysis of technologies that could be used to upgrade the existing FTTN network and selected FTTP, thereby providing the nation with a future proof, reliable, low latency broadband network.

NBN Co reports (NBNCo, 2019a) that the cost per premises (CPP) for FTTN is $2,259, HFC is $2,466, FTTC is $3,058 and FTTP is $4,403. In the text, NBN Co states that "As the deployment of this technology continues to scale, it is anticipated that cost synergies will be realised."

In 2017, NBN Co estimated that the FTTC CPP could fall to about $2,800 as the deployment to more than 700,000 premises progressed (Keisler, 2017). NBN Co's estimated CPP savings for FTTC are in line with international (Chorus, 2018) and local experience for national telecommunications rollouts.

The CPP for FTTP is anticipated to fall to about $3,800 or lower, a figure that includes the estimated $700 leasing cost payable to Telstra. In New Zealand, Chorus has reported a 44 per cent drop in the CPP for FTTP as the UFB rollout has proceeded (Gregory, 2015b).

http://doi.org/10.18080/jtde.v7n1.182

In 2018, Chorus reported (Chorus, 2018) the cost per premises as NZ$1,568 (cost per UFB1 premises passed) and NZ$1,037 (cost per UFB1 premises connected).

NBN Co's reported CPP for FTTP reflects the initial rollout costs prior to September 2015 for about 900,000 premises connected.

A search of the literature has not found any indication of a NBN Co estimate of the final or average CPP for FTTP if the FTTP rollout had continued through to the completion of the NBN.

FTTP technology improvements over the past decade have resulted in improvements in the FTTP technology available in the mass-market for network rollouts and in terms of design intelligence and experience gained through global deployments to date.

Examples of FTTP technology improvements include below ground fibre distribution pits, Figure 1, and more flexible approaches to installation of drop lines into premises, including micro-trenching, aerial and armoured fibre cable negating the need for conduit into premises.

Figure 1. Chorus UFB underground fibre distribution

NBN Co's Corporate Plan 2019-2022 (NBN Co, 2018) provides guidance that the technology split by 2020 is expected to be:

- FTTP Brownfields 1.1 million
- FTTP Greenfields 0.8 million
- FTTN/B 4.7 million
- FTTC 1.4 million
- HFC 2.5 million
- Fixed Wireless 0.6 million
- Satellite 0.4 million

In the following sections three options are provided for an upgrade program to a ubiquitous FTTP fixed access network. The costings are estimates based on figures identified in a review

http://doi.org/10.18080/jtde.v7n1.182

of statements made during Senate Estimates by members of the NBN Co senior management team, NBN Co publications, and Chorus publications.

Option 1 Upgrade by NBN Co

Option 1 is for an upgrade program carried out by NBN Co to replace the FTTN/B/C and HFC footprints with FTTP.

The average CPP to upgrade to FTTP is estimated to be:

- FTTN/B $1,500 ($7.05 billion)
- FTTC $600 ($0.84 billion)
- HFC $3,000 ($7.5 billion)

The cost projections include:

1. Layer 2 - $100 per premises
2. FTTN upgraded to Fibre Premises Passed (FPP) - $900
3. HFC upgraded to FPP - $2,400
4. Cost per Fibre Premises Connected (CFPP) - $500 (lead-in)

The total cost of this option is estimated to be $15.39 billion or with a 10 per cent variance approximately between $14 billion and $17 billion. A 10 per cent variance in costings is provided as a guide to highlight the estimated cost range.

Option 2. Upgrade by NBN Co and RSP

Option 2 is for NBN Co to upgrade FTTN/B and HFC to FPP and for RSPs to absorb the CFPP cost in the broadband plan offering.

The cost to NBN Co now becomes:

- FTTN/B $1,000 ($4.7 billion)
- FTTC $100 ($140 million)
- HFC $2,500 ($6.25 billion)

The total cost of this option is estimated to be $11.09 billion or with a 10 per cent variance approximately between $10 billion and $12.21 billion. If this option was to include a shift of the Layer 2 connection cost to the RSP then the total cost of this option is reduced by $860 million.

http://doi.org/10.18080/jtde.v7n1.182

Option 3. Upgrade by NBN Co and Consumer

Option 3 is for NBN Co to upgrade FTTN/B and HFC to FPP and for consumers to self-install the lead-in (CFPP).

The cost to NBN Co now becomes:

- FTTN/B $1,000 ($4.7 billion)
- FTTC $100 ($140 million)
- HFC $2,500 ($6.25 billion)

The total cost of this option is estimated to be $11.09 billion or with a 10 per cent variance approximately between $10 billion and $12.21 billion. For this option, NBN Co posts out a free self-install lead-in kit to consumers, however, this approach necessitates the Layer 2 connection cost.

Consumers benefit by not having the lead-in charge added to RSP broadband plans, however, consumers would be required to install the lead-in to their premises.

Self-installation is an approach that has been utilised in Europe (FastInternetBlog, 2016)(Gigaclear, 2016). A more recent trend among service providers, driven by competitive market forces, has meant that the lead-in installation costs are absorbed by the service providers and the activation cost is offered for free to consumers that select premium plans.

In Australia, self-installation of customer premises modems and devices has become commonplace, e.g. Telstra (Telstra, 2019) has utilised the self-install approach for NBN modems and Fixed Wireless devices.

Self-installation of the lead-in from pit to premises currently does not require a cabling license but may require Government to provide regulatory approval for consumer access to pits for the purpose of self-installation of the lead-in.

The provision of guides and videos, similar to those released in Europe, should be sufficient for consumers to complete the task. One option is for street parties or community days, where people work together to install the lead-ins.

Conclusions

This paper has presented options for upgrading the fixed access portion of the NBN from the MTM NBN to an all fibre NBN. The motivation for NBN Co to complete the ubiquitous FTTP fixed access network has been discussed. Of the three options, the third option provides the lowest cost to NBN Co because it does not have to complete the pit-to-premises lead-in installation.

http://doi.org/10.18080/jtde.v7n1.182

References

Bender, A. (2014). Vertigan broadband demand forecast leaves NBN Co CEO 'curious'. Computerworld. IDG. 28 August 2014. Retrieved from https://www.computerworld.com.au/article/553475/vertigan_broadband_demand_forecast_leaves_nbn_co_ceo_curious_/

BCAR. (2018). Demand for fixed-line broadband in Australia. Bureau of Communications and Arts Research. Department of Communications and the Arts. 27 February 2018. Retrieved from https://www.communications.gov.au/publications/demand-fixed-line-broadband-australia

Chorus. (2018). FY18 Full Year Result. Chorus. 27 August 2018. Retrieved from http://nzx-prod-s7fsd7f98s.s3-website-ap-southeast-2.amazonaws.com/attachments/CNU/322831/285411.pdf

Crozier, R. (2018). NBN Co chief gets frank about copper's problems. Itnews. 27 April 2018. Retrieved from https://www.itnews.com.au/news/nbn-co-chief-gets-frank-about-coppers-problems-489788

Dickinson, E. (2018). What if Telstra acquired the NBN?. ARN. IDG. 13 November 2018. Retrieved from https://www.arnnet.com.au/article/649042/what-telstra-acquired-nbn/

Dow, C. (2016). The case for 100 Mbps (or more...). Chorus. 20 June 2016. Retrieved from https://www.chorus.co.nz/blog/the-case-for-100mbps-or-more

FastInternetBlog. (2016). Gigaclear – Installation & Review. FastInternetBlog. 12 September 2016. Retrieved from https://www.fastinternetblog.uk/?p=348

FoxTel. (2018). 4K TV: Why You Should Switch to Satellite. FoxTel. 24 August 2018. Retrieved from https://www.foxtel.com.au/whats-on/foxtel-insider/foxtel/iq4k/satellite-vs-internet.html

Foxtel. (2019). Foxtel Broadband Bundles for existing customers. FoxTel. 30 March 2019. Retrieved from https://www.foxtel.com.au/shop/upgrade/broadband-bundles/bundles/nbn.html

Gigaclear. (2016). Ultrafast Fibre from Gigaclear Networks. Gigaclear. Retrieved from https://www.gigaclear.com/homebroadband

Gregory, M. (2014). Why the NBN's cost-benefit analysis is flawed on arrival. The Australian. News Corporation. 18 September 2014. Retrieved from https://www.theaustralian.com.au/business/business-spectator/why-the-nbns-costbenefit-analysis-is-flawed-on-arrival/news-story/dbc280971aec94ceb18ac44e211d18be

http://doi.org/10.18080/jtde.v7n1.182

Gregory, M.A. (2015a). "Why the NBN can do without fibre-to-the-node". *The Australian*. News Limited. 10 April 2015. Retrieved from https://www.theaustralian.com.au/business/business-spectator/why-the-nbn-can-do-without-fibretothenode--/news-story/29215a9c2b4c2d0cb904326283887f64

Gregory, M. (2015b). How much do FTTP NBN connections really cost? The Australian. News Corporation. 18 September 2015. Retrieved from https://www.theaustralian.com.au/business/business-spectator/how-much-do-fttp-nbn-connections-really-cost/news-story/74dadb937448c9efefecde5e7d6f56b2

Gregory, M. (2016). Can NBN withstand the pressure test? The Australian. News Corporation. 10 March 2016. Retrieved from https://www.theaustralian.com.au/business/business-spectator/can-nbn-withstand-the-pressure-test/news-story/8fbcb3b208f9638242784a0c0585246c

Gregory, M. (2017). Is it time for NBN Co to make fibre-to-the-curb the default option?. The Australian. News Corporation. 15 February 2017. Retrieved from https://www.theaustralian.com.au/business/technology/opinion/is-it-time-for-nbn-co-to-make-fibretothecurb-the-default-option/news-story/6c1938a6a48da2c74743ee939b5e226c

Gregory, M. (2018). Australian Wholesale Telecommunications Reforms. Journal of Telecommunications and the Digital Economy, 6(2), 1-34. https://doi.org/10.18080/jtde.v6n2.155

Irving, W. (2018). Establishing a standalone infrastructure business unit. Telstra Wholesale. Telstra Exchange. 20 June 2018. Retrieved from https://exchange.telstra.com.au/establishing-standalone-infrastructure-business/

Keisler, K. (2017). Setting the facts straight on Fibre-to-the-Node. NBN Co. 8 March 2017. Retrieved from https://www.nbnco.com.au/blog/the-nbn-project/setting-the-facts-straight-on-fibre-to-the-node

NBNCO. (2018). Corporate Plan 2019. NBN Co. August 2019. Retrieved from https://www.nbnco.com.au/corporate-information/about-nbn-co/corporate-plan/corporate-plan

NBNCO. (2019a). NBN Co half-year report FY19. NBN Co. 18 February 2019. Retrieved from https://www.nbnco.com.au/corporate-information/about-nbn-co/corporate-plan/financial-reports.html

NBN Co. (2019b). NBN Co scales towards 2020. NBN Co. 18 February 2019. Retrieved from https://www.nbnco.com.au/corporate-information/media-centre/media-statements/nbn-co-scales-towards-2020

News. (2019). 8K is here this year, but there's no rush to upgrade. News.com.au. News Corporation. 13 January 2019. Retrieved from https://www.news.com.au/technology/home-entertainment/tv/8k-is-the-new-frontier-in-tv-technology-but-you-really-dont-need-it/news-story/4d5f6f1d93ad5820bcaccfe5300c718f

Ookla. (2019). Speedtest Global Index. January 2019. Retrieved from https://www.speedtest.net/global-index

RAFC. (2016). Promise Check: Deliver minimum broadband speeds of 25 mbps by 2016 and 50 mbps to 90pc of fixed line users by 2019. RMIT ABC Fact Check. Australian Government. 8 May 2016. Retrieved from https://www.abc.net.au/news/2014-07-27/nbn-speeds-promise-check/5543512

Smith, P. (2018). NBN write-down 'inevitable': Damning S&P report. Australian Financial Review. Fairfax Media. 25 July 2018. Retrieved from https://www.afr.com/technology/web/nbn/sp-nbn-20180724-h132tf

Telstra. (2019). How To. How do I set up my devices on nbn™ Fixed Wireless? Telstra Corporation. 22 March 2019. Retrieved from https://www.telstra.com.au/support/category/broadband/nbn/how-do-i-install-my-fixed-wireless-equipment

Turnbull, M. (2013). "Panel of Experts to conduct cost-benefit analysis of broadband & review NBN regulation". Ministers for the Department of Communications and the Arts, Government of Australia. 12 December 2013. Retrieved from http://www.minister.communications.gov.au/malcolm_turnbull/news/panel_of_experts_to_conduct_cost-benefit_analysis_of_broadband_and_review_nbn_regulation#.WxIOQEiFNaQ

http://doi.org/10.18080/jtde.v7n1.182

An Artificial Immune System-Based Strategy to Enhance Reputation in MANETs

Lincy Elizebeth Jim
Melbourne Institute of Technology, Australia

Mark A Gregory
RMIT, Australia

Abstract: In Mobile Ad hoc Networks (MANETs) the nodes act as a host as well as a router, thereby forming a self-organizing network that does not rely upon fixed infrastructure, other than gateways to other networks. Security is important for MANETs and trust computation is used to improve collaboration between nodes. This paper proposes an Artificial Immune System-based reputation (AISREP) algorithm to compute trust and thereby provide a resilient reputation mechanism. In this paper, the presence of selfish nodes are considered. Selfish nodes are known to enhance the reputation of their selfish peers which in turn causes packet loss. In the event of the packet being routed using the AISREP algorithm, even though the number of selfish nodes increases, this algorithm identifies the selfish nodes and avoids using the selfish nodes from the routing path thereby improving the overall performance of the network.

Keywords: MANET, Artificial Immune System, Reputation, Selfish, PAMP

Introduction

The efficiency of Mobile Ad hoc Networks (MANETs) relies on cooperation amongst the nodes to route and forward packets (Murthy & Garcia-Luna-Aceves, 1996). Therefore, it is vital to maintain effective collaboration amongst the nodes. Trust computation is used to identify the malicious or selfish nodes from the good nodes. In order to establish trust, the nodes have to be constantly monitored so that trustworthy nodes can be found to participate when routing messages. Maintaining trust between nodes in the network provides benefits to the overall network efficiency (Shaikh *et al.*, 2009). When nodes are seeking a routing path that does not have malicious, selfish or faulty nodes the computed trust values provide an important input. Trust augments traditional security by verifying that only authentic nodes are participating when routing traffic.

http://doi.org/10.18080/jtde.v7n1.176

There have been various definitions of trust proposed in the literature. The term trust has been qualitatively and quantitatively substantiated in a range of approaches based on Quality of Service (QoS), risk and other measures. Trust can also be computed using various functions such as the reputation function, by calculating direct trust and calculating trust based on recommendation. In Xiong & Liu (2003), a trust model is proposed based on filtering the badly behaving nodes from the remaining nodes in the network. The misbehaving nodes can yield a deceptive recommendation when queried and this, in turn, can lead to a variety of attacks like bad mouthing and collusion, which can hamper the trust framework. Mei *et al.* (2014) proposed a trust approach where recommendations are considered valid if a majority of nodes provide the recommendation. This is a potentially successful approach, but there is also the possibility that the majority of nodes could be colluding to launch an attack on the remaining nodes. In Buchegger & Le Boudec (2005), a trust model is proposed where trust is computed based on the prior experience of the trustee node with the node to be evaluated. This results in the use of scepticism to compute trust and circumstances may occur where the trustee node does not have prior experience with the node to be evaluated. In this paper a trust model is computed based on direct trust and indirect trust.

Background

Selfish Attacks

Safeguarding a network against attack is considered to be an important challenge today, as the potential for attack has increased significantly. Research has been carried out into packet forwarding security attacks, such as black hole (Sharma & Sharma, 2012), wormhole (Gupta & Singh, 2016), and gray hole (Sen *et al.*, 2007). It is also worth noting that trust attacks are carried out in the form of deceptive recommendations from corrupted or selfish nodes. There are other forms of attack that utilize this deceptive recommendation. The following types of attacks can be carried out:

- Bad Mouthing Attack: In this attack the selfish nodes give negative feedback about good nodes in order to tarnish their reputation. This falsified information leaves the trust management framework in a state of jeopardy (McCoy, Sicker, & Grunwald, 2007).
- Ballot Stuffing Attack: In this attack the selfish nodes collude and propagate a falsified rating to genuine nodes (Tan *et al.*, 2017).
- Incorrect Traffic Generation. This attack consists of sending false control messages. The false control messages can be sent on behalf of another node or the control messages may contain falsified routing information (Raffo, 2005).

http://doi.org/10.18080/jtde.v7n1.176

- Intelligent Misbehaviour Attack. Nodes launch intelligent attacks against the trust architecture. When the misbehaviour is insignificant to notice, it can be persistent; this attack will not be detected by traditional trust computation methods (Ishmanov & Kim, 2011).
- Time Dependent Attacks. The selfish node drops data packets at some predetermined time and behaves normally during other instances (Saha *et al.*, 2013).
- Information Disclosure. A selfish node may reveal confidential information to unauthorized nodes in the network (Basagni *et al.*, 2004).
- Eclipse Attack. In this attack the selfish node poisons the routing table of the well behaved nodes as the routing tables would contain links to a conspiracy of malicious nodes (Yih-Chun & Perrig, 2004; Schütte, 2006).

This paper considers the Ballot Stuffing Attack and Bad Mouthing Attack to evaluate the performance of the proposed approach in the midst of selfish nodes.

Artificial Immune System and Human Immune System

The immune system is a key to the defence against foreign objects or pathogens. It is necessary for the proper functioning of the immune system to maintain host well-being. The cells that play a fundamental role in this defence process are known as Dendritic Cells (DCs).

Research has been carried out into the Human Immune System (HIS) due to its distinctive ability to solve complex issues. The HIS present in the human body provides a robust defence against pathogens. The ability of the HIS to distinguish between self cells and foreign cells is noteworthy. The most important job of the HIS is to safeguard the body against pathogens. The cells, organs and tissues present in the body work in collaboration to launch a series of steps, known as an immune response, to keep the body healthy and ward off disease causing microbes.

Considerable research is being carried out in the HIS field and this knowledge is being translated into current Artificial Immune Systems (AIS) research. AISs are inspired by theoretical immunology and observed immune functions, which in turn are used to solve problems in complex domains (Abdelhaq, Hassan & Alsaqour, 2011). The evolution of AIS based research since 1990 has seen it gain prominence as a branch of computational intelligence. The four major algorithms which form the basis of AIS research are 1) Artificial Immune Networks (AIN); 2) Negative Selection Algorithm (NSA); 3) Clonal Selection (CS); and 4) Danger Theory (DT) and the Dendritic Cell Algorithm (DCA). AIS research amalgamates the principles of immunology, engineering and computer science to solve

http://doi.org/10.18080/jtde.v7n1.176

complex problems. Some of the attributes of AIS are learning, memory and pattern recognition.

The AIS based DCA is widely known for its large number of applications and well established in the literature. DT suggests that unfamiliar pathogens, which are threatening, will induce the generation of cellular molecules (danger signals) by instigating cellular stress or cellular death. These molecules are in turn perceived by Antigen Presenting Cells (APCs), critical cells that instigate an immune response.

The NSA proposed by Forrest *et al.* (1994) differentiated self cells from non-self cells based on the generation of T cells. This principle was applied to the detection of computer viruses. Since then, variations of NSA have evolved whilst keeping the original NSA principles intact.

AIS borrows its principles from HIS to solve problems in data mining, computer security, robotics and so on. DCs are antigen-presenting cells present in the HIS, where they present the antigen to the T cells, which in turn kill invaders. The features of the DCs as APCs were identified by Steinman & Cohn (1973). The state of DC is changed (Twycross & Aickelin, 2005) upon recognition of signals, such as the Pathogen Associated Molecular Pattern (PAMP) and Danger Signal (DS).

The role of the PAMP signal is noteworthy as it triggers the immune response. The DSs are released when tissue damage is suspected but they are of a lower priority than PAMP.

The DCA proposed by Greensmith & Aickelin (2008) is based on the function of DCs to investigate the state of the environment after combining various signals like DS and PAMP. The DT proposed by Matzinger (2001) forms the basis of the DCA. The DT is based on the principle that stressed cells release a DS in order to launch the immune response. The drawbacks of DT in Aickelin & Cayzer (2008) suggest the presence of an APC is fundamental for launching an immune response and the DS does not need to relate to threatening scenarios.

Proposed Reputation Model

By taking into account the trust based on a node's behaviour, there is the opportunity to consider both the direct trust and indirect trust. In direct trust, a node has to earn its reputation based on its behaviour with its immediate neighbours; and in indirect trust, the node's behaviour is calculated based on nodes other than immediate neighbours with which it would have gained reputational knowledge while routing packets for other nodes. In the same region of the MANETs, the node's behaviour is not only spatially correlated but also temporally correlated. In other words, the node's behaviour not only relates to its own history, it is also relates to other nodes in the same region. The behavioural change regularity

http://doi.org/10.18080/jtde.v7n1.176

of the node's behaviour has certain statistical characteristics that can be identified and evaluated. Based on this behaviour the direct and indirect trust value is collected by the nodes from the same region, thereby reducing data exchange among the other nodes in the network.

Computation of Trust and Reputation

In this paper, a model based on the AIS principle of DT is utilized to propose the AIS-based Reputation Algorithm (AISREP) wherein each node is modelled as a DC. Selfish nodes are detected by the DC nodes prompting the need to identify the danger by sending a DS to intermediate nodes, whereupon further action is initiated including a PAMP message. The DC nodes monitor the activity occurring in the MANET to report malicious, selfish or malfunctioning nodes. The PAMP signal is utilized here to signify the presence of a malicious, selfish or malfunctioning node in the network. Based on the aforementioned concepts a mathematical model is built.

Reputation is the quality or behaviour as seen by other nodes. Reputation is important in a MANET because the performance of the MANET depends on good behaviour by all of the nodes. Reputation is crucial because MANET functionality is not dependent on a single node. As a result, it is vital to have good reputation for all nodes and for the nodes to participate with honesty in the routing process in order to earn the good will of neighbouring nodes and, in turn, to improve network functionality and performance. A MANET with nodes that maintain a good reputation functions as expected and with improved message transmission performance. Therefore, reputation in MANETs is an interconnected system. As a result, a good reputation is able to mitigate bad mouthing by other nodes. The commendation from a reputed node is taken into consideration. The commendation from a reputed node has a higher rank based on its reputation. The node with a high reputation is given priority during trust calculations.

The concern about trustable nodes in the routing path is important as a measure of packet forwarding success. Consider the reputation for *Node a* as given in Equation (1):

$$REP_a = \frac{1}{DT}\left[\sum_{a=1}^{n-1} \frac{T_{a,n}(N_{a,n}^{S} - N_{a,n}^{PAMP})W}{N_{a,n}^{TOTAL}}\right] \quad (1)$$

where $T_{a,n}$ is the sum of direct and indirect trust, DT is trust deviation, W is the weight of the PAMP signal obtained using statistical analysis, $N_{a,n}^{S}$is the number of successful interactions between nodes a and n, $N_{a,n}^{PAMP}$is the number of times PAMP had to be sent when nodes a and n interact, $N_{a,n}^{TOTAL}$ is total number of interactions between nodes a and n.

http://doi.org/10.18080/jtde.v7n1.176

The AIS based Trust Computation model uses direct and indirect trust. Direct Trust ($T_{a,b}^{D}$) is calculated as:

$$T_{a,b}^{D} = \left(\frac{P_{a,b}}{P_{a,b} + N_{a,b}}\right) * \left(\frac{1}{N_{a,b}^{DS} + N_{a,b}^{PAMP}}\right) \quad (2)$$

Indirect Trust ($T_{a,n}^{IND}$) is calculated as:

$$T_{a,n}^{IND} = \sum_{a=1}^{n-1} \left(\frac{P_{a,n}}{P_{a,n} + N_{a,n}}\right) * \left(\frac{1}{N_{a,n}^{DS} + N_{a,n}^{PAMP}}\right) \quad (3)$$

In Equations (2) and (3), $P_{a,n}$ is the count of positive experiences (number of successful data-ack transmissions) between node *a* and node *n*, where node *n* is not an immediate neighbour of node *a;* $N_{a,n}$ is the count of the negative experiences (unsuccessful data–ack transmissions) between node *a* and node *n;* $N_{a,b}^{DS}$ is the number of times node *a* had to send a danger signal to the source due to node *b* not sending an acknowledgement; and $N_{a,b}^{PAMP}$ is the number of times PAMP had to be used during interactions between node *a* and node *b*.

Filtering AISREP Algorithm for Authentic Commendation

In this approach each node takes a role like the DCs in the HIS. In the scenario where there are no attackers, a source node sends a packet to the destination node and the intermediate nodes route traffic. As seen in Figure 1, *Node A* is the source node, *Node E* is the destination node and the intermediate nodes are *B*, *C* and *D*. The intermediate nodes respond with a Data Ack to the respective Data Send. If *Node D* is a malicious node, *D* would receive the data sent to it and might not acknowledge receipt of data causing a path disruption. The destination *Node E* would not receive the packet in this scenario or might receive a corrupt packet.

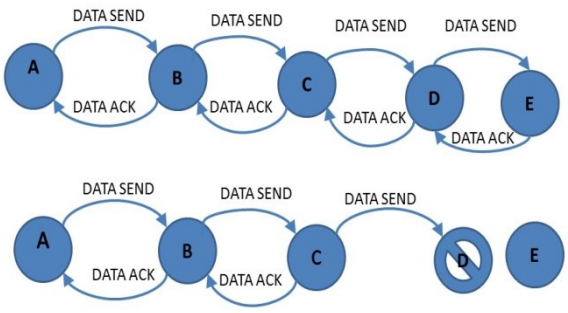

Figure 1. Routing in normal and attacker scenario

http://doi.org/10.18080/jtde.v7n1.176

In the event of the malicious *Node D* not sending a Data Ack the immediate neighbour *Node C* sends "Danger Signal (N_D)" to *Node B* in order to inform the source about the presence of a problem in the transmission path. *Node B* in turn relays this "Danger Signal (N_D)" to the source *Node A*. Once the source is informed of the presence of a problem with *Node D*, the source sends "PAMP Send (N_D)" as can be observed in Figure 2 to *Node D* and *Node D* responds with a "PAMP Ack (N_D)". PAMP is a high priority signal and it triggers an immune response; therefore, it overwrites the node buffer of the corrupted *Node D* and *Node D* is forced to acknowledge the PAMP signal. Once the presence of a defective node is identified, the routing path via this node would be avoided.

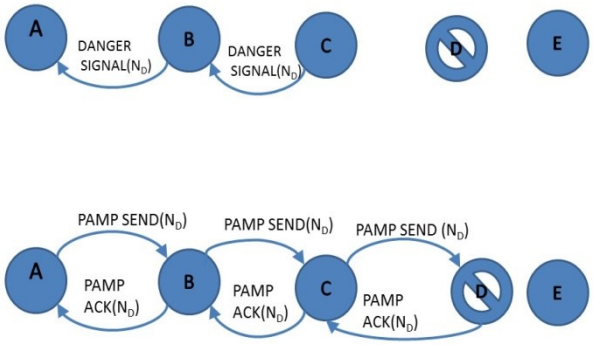

Figure 2. PAMP to confirm attacker

Simulation and Results

The Ns-3.23 simulator was used to simulate the proposed AIS based reputation mechanism (Henderson *et al.*, 2008). The pseudo-code used in the simulation is given in Table 1 and the simulation parameters are listed in Table 2.

Table 1. AISREP Pseudo Code

1. *Source node ($Node_{src}$) broadcasts Route request*
   (a) $Node_{src}$ sends data packet.
   (b)Intermediate node ($Node_{intermed}$) acknowledges data.
2. *For each intermediate set of nodes, Compute Trust (Number of DS, Number of PAMP)*
   (a) $Node_{src}$ computes Trust of $Node_{intermed}$
   (b) $Node_{src}$ sends packet to neighbor node($Node_{ngbr}$)
   (c) $Node_{ngbr}$ sends packet to the next $Node_{intermed}$
   (d) $Node_{ngbr}$ does not receive Ack
3. *$Node_{ngbr}$ sends DS to source*
4. *When $Node_{src}$ receives DS*
   (a) $Node_{src}$ sends PAMP.
   (b) $Node_{intermed}$ acknowledges PAMP.
   (c) The presence of a selfish node is detected.
5. *Compute Reputation based on the trust computed in step 2.*
6. *Isolate the selfish node.*

http://doi.org/10.18080/jtde.v7n1.176

Table 2. Simulation Parameters

Simulator	Ns-3.23
Mobility Model	Random Waypoint
Simulation Time	1000s
Number of Nodes	10-90
Routing Protocols	AODV, AISREP
Traffic Type	UDP
Network Area	300 * 1500
Mobility	6 m/s
Pause Time	0-800 s
Transmission Range	50 m

In Figure 3, the relationship between Trust and Reputation can be observed. As the Trust value, which is the combination of direct and indirect trust gathered from DC nodes, increases the reputation of the DC nodes also increases. This in turn creates an improved trust framework that can be used to identify traffic paths via the DC nodes.

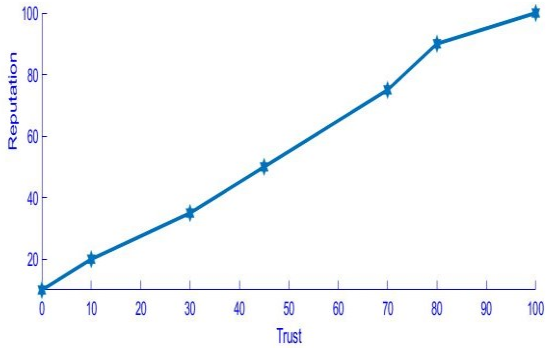

Figure 3. Reputation versus Trust

Ad hoc On-Distance Vector (AODV) (Perkins, Belding-Royer, & Das, 2003) is a reactive routing protocol for Mobile ad hoc networks. In routing protocols like AODV (Jhaveri, Patel & Jinwala, 2012) security has not been addressed and nodes are considered to be cooperative and trustworthy. The proposed approach has been compared with AODV using the performance metrics including packet delivery ratio, throughput and end-to-end delay.

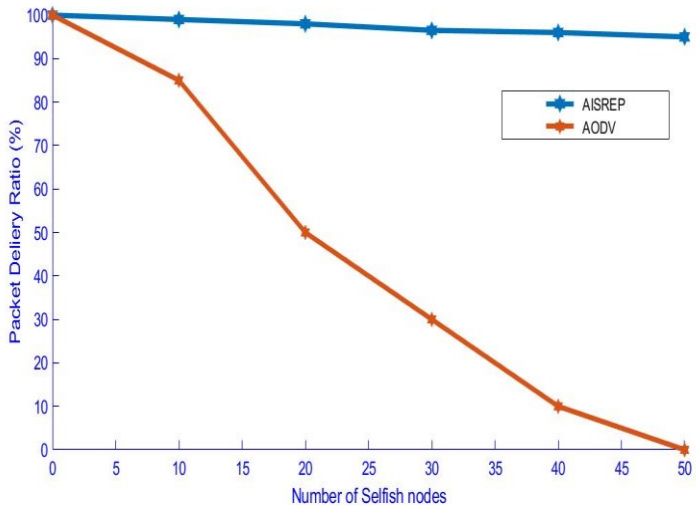

Figure 4. Packet Delivery versus Number of Selfish Nodes

http://doi.org/10.18080/jtde.v7n1.176

In Figure 4, the reputation in the presence of selfish nodes is studied. For a network that consists of non-DC nodes, it is seen that the reputation decreases for AODV nodes as they fall prey to the selfish or corrupted nodes. In the proposed AISREP, the node reputation increases in the presence of selfish nodes due to the utilization of the PAMP signal to identify and reset the selfish nodes.

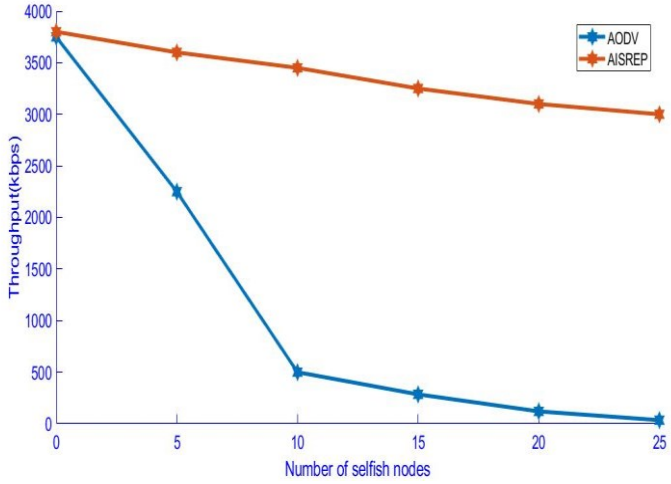

Figure 5. Throughput versus Selfish Nodes

Throughput is defined as the total number of packets delivered over the total simulation time. In Figure.5, the throughout comparison is done for AODV and the proposed AIS-based algorithm AISREP. As the number of selfish nodes increases the throughput for AODV decreases as the selfish nodes hinder the packets from reaching the destination; the selfish nodes do not facilitate the routing of packets. However, in the case of AISREP, as the number of selfish nodes increases the throughput is not drastically reduced due to the efficiency of the AISREP algorithm.

The average time taken by a data packet to reach the destination node is known as the end-to-end delay. This would include all delays that the packet encounters, such as route discovery delay and queueing delay. This metric is obtained by calculating the difference between the time *t* at which the packet was first transmitted by the source and the time *t* at which the same packet arrived at the destination.

In Figure 6, the comparison of end-to-end delay with respect to AODV and the AIS-based algorithm AISREP can be observed. As the number of selfish nodes increases, the packets sent by a source will take greater time to reach the destination node, as the selfish nodes do not allow the packet to reach the destination; whenever a packet happens to be routed by a selfish node it would take further time to reach the destination node.

http://doi.org/10.18080/jtde.v7n1.176

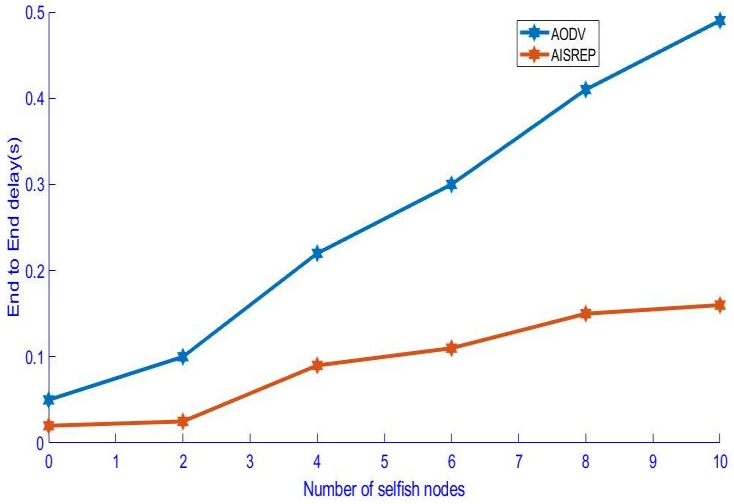

Figure 6. End-to-End delay versus Selfish Nodes

In the event of the packet being routed by nodes using the AISREP algorithm, even though the number of selfish nodes increases, this algorithm identifies the selfish nodes and avoids using the selfish nodes from the routing path. There will be delay to identify the selfish nodes but the packets eventually reach the destination with a lesser delay when compared to AODV.

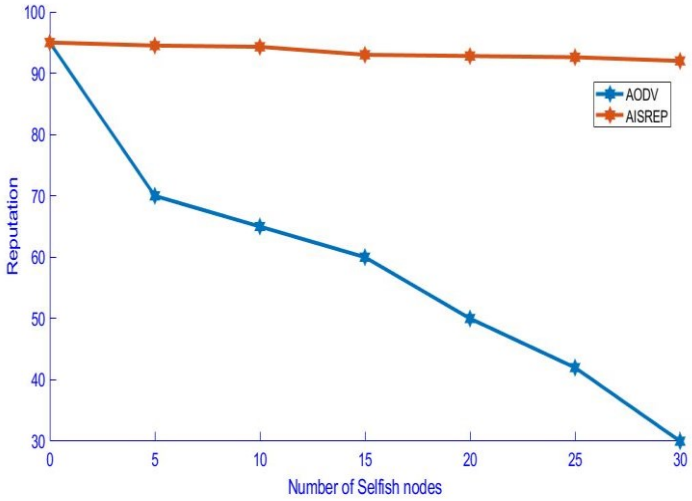

Figure 7. Reputation in Bad Mouthing attack scenario

In Figure 7, the reputation of the good nodes is considered in the Bad Mouthing attack scenario. As the number of selfish nodes increases the reputation of the good nodes goes down for AODV .This is due to the selfish nodes propagating false information. During the AISREP approach, the reputation of the good nodes is as per the expected value even in the presence of increasing selfish nodes.

http://doi.org/10.18080/jtde.v7n1.176

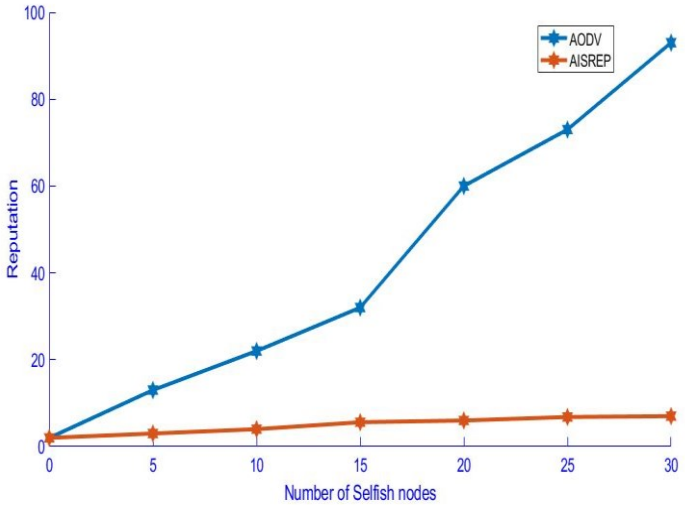

Figure 8. Reputation in Ballot Stuffing attack scenario

In Figure 8, the reputation of nodes in the Ballot Stuffing attack scenario is considered. In the scenario where AODV is used, the selfish nodes propagate false ratings about other selfish nodes, hence, as can be observed in Figure 8, the reputation value goes higher for other selfish nodes as their count increases in the network. However, in the AISREP approach, this misleading information propagated by the selfish nodes is curbed and thus the falsified information is mitigated.

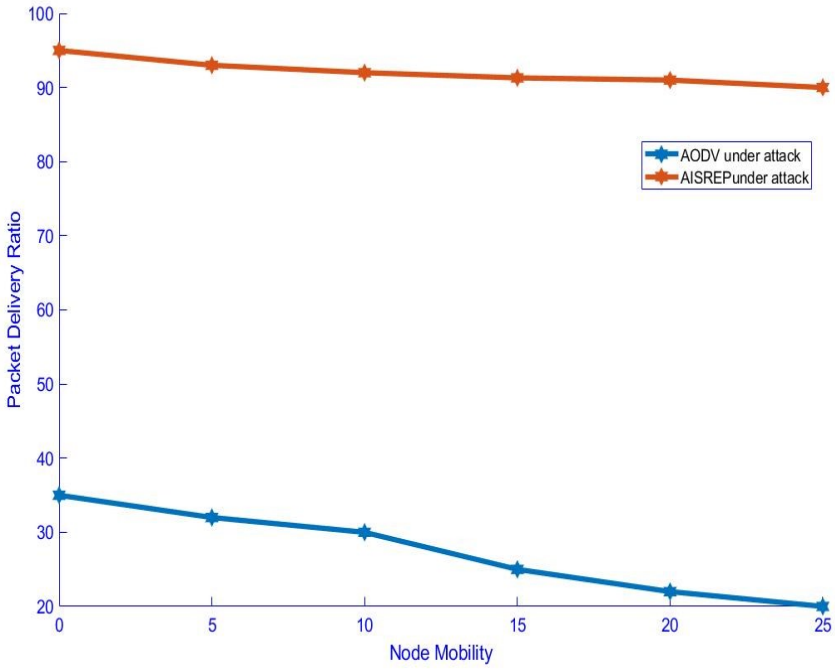

Figure 9. Packet Delivery vs Node mobility

In Figure 9, the packet delivery ratio for AODV under attack tends to decrease with increase in node mobility, whereas, for the AISREP algorithm, the packet delivery ratio increases with

http://doi.org/10.18080/jtde.v7n1.176

node mobility, as only the nodes with good reputation are chosen with the help of PAMP signals.

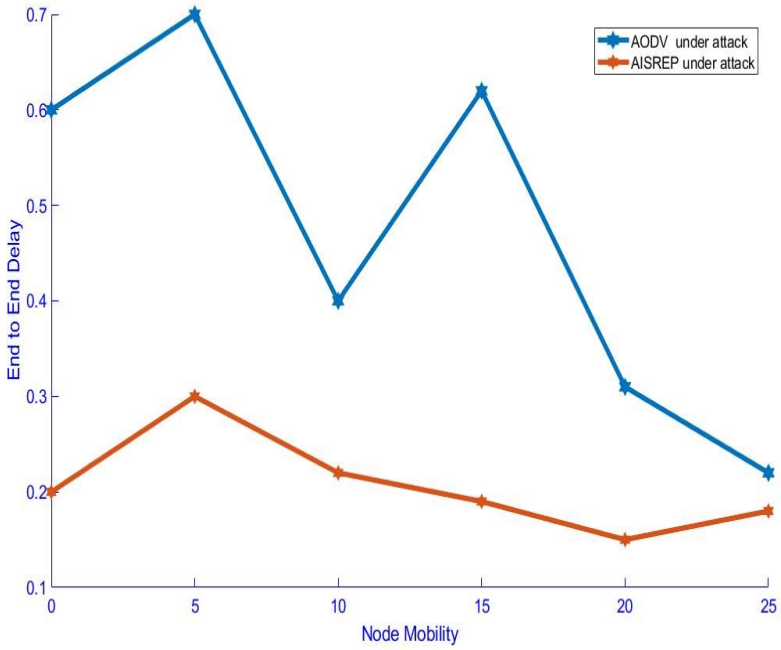

Figure 10. End-to-End Delay vs Node Mobility

In Figure 10, end-to-end delay gradually increases with increase in mobility for AODV as the corrupt nodes can cause intentional delay by not choosing to forward packets, whereas, in the AISREP algorithm due to the presence of reputed nodes, the delay encountered will be less with increase in node mobility.

Conclusion

In this paper, an AIS-based reputation mechanism is presented and the results have been analysed with the Ns-3.23 simulator. The presence of corrupt or selfish nodes is considered and the reputation mechanism depends on the direct and indirect trust commendation from the nodes in the network. The solution proposed is robust and uses AIS principles, thereby protecting the network from corrupt or selfish nodes.

This paper also considers the Bad Mouthing attack and the Ballot Stuffing attack and studies their effects on the reputation of the nodes in the network. During the Bad Mouthing attack, the selfish nodes propagate false information about good nodes but, with AISREP, the effect of false information is mitigated.

Similarly, in the case of the Ballot Stuffing attack, the selfish nodes propagate false information about other selfish nodes, claiming that they are good. In the AISREP approach, the effect of selfish nodes providing high reputations about other selfish counterparts is curbed. In some cases, the node may not be able to send an acknowledgement due to broken

http://doi.org/10.18080/jtde.v7n1.176

links through corrupt or malfunctioning nodes: therefore, there would be a situation where the commendation received from other nodes about the behaviour may not be accurate. In order to deal with this issue, a filtering algorithm is applied to aid in gaining the reputation of genuine nodes.

The simulation results obtained highlight the potential for the proposed approach as a trust framework. The AISREP approach provides improved packet delivery in the presence of selfish or corrupt nodes. In future, the AIS NSA could be utilized to enhance the trust and reputation calculations.

References

Abdelhaq, M., Hassan, R., & Alsaqour, R. (2011). Using dendritic cell algorithm to detect the resource consumption attack over MANET. Paper presented at the *International Conference on Software Engineering and Computer Systems*. https://link.springer.com/chapter/10.1007/978-3-642-22203-0_38

Aickelin, U., & Cayzer, S. (2008). The danger theory and its application to artificial immune systems. arXiv preprint arXiv:0801.3549. https://arxiv.org/abs/0801.3549

Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (2013). *Mobile ad hoc networking*. Hoboken: John Wiley & Sons. doi: 10.1002/0471656895

Buchegger, S., & Le Boudec, J.-Y. (2005). Self-policing mobile ad hoc networks by reputation systems. *IEEE Communications Magazine*, *43*(7), 101-107. https://ieeexplore.ieee.org/abstract/document/1470831

Forrest, S., Perelson, A. S., Allen, L., & Cherukuri, R. (1994). Self-nonself discrimination in a computer. *Research in Security and Privacy, 1994. Proceedings, 1994 IEEE Computer Society Symposium*. https://www.cs.unm.edu/~immsec/publications/virus.pdf

Greensmith, J., & Aickelin, U. (2008). The deterministic dendritic cell algorithm. Paper presented at the *International Conference on Artificial Immune Systems*. https://dl.acm.org/citation.cfm?id=1428224

Gupta, N., & Singh, S. N. (2016). Wormhole attacks in MANET. Paper presented at the *Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference*. https://ieeexplore.ieee.org/abstract/document/7508120

Henderson, T. R., Lacage, M., Riley, G. F., Dowell, C., & Kopena, J. (2008). Network simulations with the ns-3 simulator. *SIGCOMM demonstration*, *14*(14), 527. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.415.6550&rep=rep1&type=pdf

Ishmanov, F., & Kim, S. W. (2011). A secure trust establishment in wireless sensor networks. Paper presented at the *Electrical Engineering and Informatics (ICEEI), 2011 International Conference*. https://ieeexplore.ieee.org/abstract/document/6021517

Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). Improving route discovery for AODV to prevent blackhole and grayhole attacks in MANETs. *INFOCOMP, 11*(1), 1-12. http://www.dcc.ufla.br/infocomp/index.php/INFOCOMP/article/view/362/346

Matzinger, P. (2001). Essay 1: the Danger model in its historical context. *Scandinavian journal of immunology*, *54*(1-2),4-9. https://onlinelibrary.wiley.com/doi/full/10.1046/j.1365-3083.2001.00974.x

McCoy, D., Sicker, D., & Grunwald, D. (2007). A mechanism for detecting and responding to misbehaving nodes in wireless networks. Paper presented at the *Networking Technologies for Software Define Radio Networks, 2007 2nd IEEE Workshop*. https://ieeexplore.ieee.org/abstract/document/4348973

Mei, J.-P., Yu, H., Liu, Y., Shen, Z., & Miao, C. (2014). A social trust model considering trustees' influence. Paper presented at the International Conference on Principles and Practice of Multi-Agent Systems. https://link.springer.com/chapter/10.1007/978-3-319-13191-7_29

Murthy, S., & Garcia-Luna-Aceves, J. J. (1996). An efficient routing protocol for wireless networks. *Mobile Networks and Applications*, *1*(2), 183-197. https://link.springer.com/article/10.1007/BF01193336

Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (2070-1721). IETF RFC 3561. https://www.ietf.org/rfc/rfc3561.txt

Raffo, D. (2005). Security schemes for the OLSR protocol for ad hoc networks. *Université Pierre et Marie Curie*-Paris VI. https://tel.archives-ouvertes.fr/tel-00010678/

Saha, H. N., Bhattacharyya, D., Banerjee, B., Mukherjee, S., Singh, R., & Ghosh, D. (2013). A review on attacks and secure routing protocols in MANET. *International Journal of Innovative Research and Review*, *1*(2), 12-36. https://www.researchgate.net/profile/Himadri_Saha2/publication/289510067_A_REVIEW_ON_ATTACKS_AND_SECURE_ROUTING_PROTOCOLS_IN_MANET/links/568d817808aef987e56601aa.pdf

Schütte, M. (2006). Detecting selfish and malicious nodes in MANETs. Paper presented at the Seminar: *sicherheit in selbstorganisierenden netzen*, hpi/universität potsdam, sommersemester. https://pdfs.semanticscholar.org/e733/fc17534542315559f6b47906c2d2cf73390c4.pdf

Sen, J., Chandra, M. G., Harihara, S., Reddy, H., & Balamuralidhar, P. (2007). A mechanism for detection of gray hole attack in mobile Ad Hoc networks. Paper presented at the *Information, Communications & Signal Processing, 2007 6th International Conference*. https://ieeexplore.ieee.org/abstract/document/4449664

Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y.-J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *20*(11), 1698-1712. https://ieeexplore.ieee.org/abstract/document/4721432

Sharma, N., & Sharma, A. (2012). The black-hole node attack in MANET. Paper presented at the *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference*. https://ieeexplore.ieee.org/abstract/document/6168430

Steinman, R. M., & Cohn, Z. A. (1973). Identification of a novel cell type in peripheral lymphoid organs of mice: I. Morphology, quantitation, tissue distribution. *Journal of Experimental Medicine, 137*(5), 1142-1162. https://www.ncbi.nlm.nih.gov/pubmed/4573839

Tan, H. C., Ma, M., Labiod, H., Chong, P. H. J., & Zhang, J. (2017). A non-biased trust model for wireless mesh networks. *International Journal of Communication Systems*, *30*(9), e3200. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3200

Twycross, J., & Aickelin, U. (2005). Towards a conceptual framework for innate immunity. Paper presented at the *International Conference on Artificial Immune Systems*. https://dl.acm.org/citation.cfm?id=2156125

Xiong, L., & Liu, L. (2003). A reputation-based trust model for peer-to-peer ecommerce communities. *Proceedings of the 4th ACM conference on Electronic commerce*. https://dl.acm.org/citation.cfm?id=779972

http://doi.org/10.18080/jtde.v7n1.176

Yih-Chun, H., & Perrig, A. (2004). A survey of secure wireless ad hoc routing. *IEEE Security & Privacy*, *2*(3), 28-39. https://dl.acm.org/citation.cfm?id=1009287

http://doi.org/10.18080/jtde.v7n1.176

The Eucla Recorder (1898 –1900)

Community journalism on a remote telegraph station

Denis Cryle
Central Queensland University

Abstract: The rise of Eucla in the late nineteenth-century as a border telegraph station, located on Western Australia's southern maritime border with South Australia, has been celebrated by Moyal (1984) for the cohesion and resilience of its skilled workforce. This article further explores the Eucla story, offering a vivid snapshot of the community's preoccupations and challenges at the end of the 19th century through the pages of its monthly newspaper, the *Eucla Recorder* (1898 – 1900). Little if any attention has been paid to its community journalism, despite the *Eucla Recorder*'s unusual setting and distinctive mode of production. The following case study documents the life of the *Eucla Recorder*, extending its scope to the social and political attitudes of the telegraph staff which produced it.

Keywords: Telecommunications, History, Telegraph Station, Newspaper, Eucla

Introduction

Despite its remoteness and the belated construction of the great east-west telegraph line linking Western Australia to the eastern colonies, the Eucla telegraph station has attracted considerable attention from telecommunication historians, most notably from Ann Moyal (1984) who recognised its strategic yet remote position as comparable with that of the Alice Springs station at the heart of the Overland Telegraph Line. Both remote stations were strategically chosen for the retransmission of messages over vast distances across the Australian continent. But if Alice Springs, situated at the centre of the north-south telegraph was better known than Eucla on the east-west line, the rise of Eucla, symbolised by its own newspaper, was arguably more rapid. One of the key roles of the community newspaper was to promote the local interest and the *Eucla Recorder* was no exception in this respect. In so doing, it provides a closer assessment of the environmental and psychological challenges faced by the settlers and telegraph workers who moved into the area.

http://doi.org/10.18080/jtde.v7n1.177

Yet it will be also shown that the *Eucla Recorder* and its editors did not confine themselves to reporting local issues. For while tracking the movements of staff throughout the telegraph station network, the monthly paper editorialised on the great issues of the day, such as the advent of Federation, the campaign to enfranchise women and the dramatic events of the Boer War in which Australian telegraphists were destined to play a part. The diversity of the *Eucla Recorder*'s coverage owed something to Eucla's status as a border station, distinct from Alice Springs. As such, it comprised a wider microcosm of colonial society drawn from not one, but several Australian colonies.

Genesis of the newspaper

Community journalism was a feature of 19th century Australian newspapers (Cryle, 2017; Manion, 1982), occurring in different formats and a range of different circumstances. In colonial Australia, community journalism arose in the range of circumstances, starting with newspapers printed on immigrant ships bound for Australia, and continuing in embryonic settlements, often distant from the larger towns and ports of the colonies. In Australia as in America, newspapers acted as 'parish pumps,' promoting local progress and improved communication with the outside world (Kirkpatrick, 1984). In this respect, the *Eucla Recorder* perpetuated similar colonial values, albeit with a decidedly different outlook. For while newspapers, which began with limited circulation, thrived in regional mining and agricultural centres, the *Eucla Recorder* operated in a more remote environment, dominated by civil service employees, and without the usual spur of private enterprise to sustain it.

Arguably this experiment undertaken on a remote telegraph station at the end of the 19th century was unique, operating as it did in a remote locality on Western Australia's maritime border with South Australia.

The *Eucla Recorder*, a voluntary monthly enterprise which first appeared on 15 October 1898, was printed and published by the combined telegraph staff working at the station. The initiative for the paper came from the Western Australians, following a meeting in their dining room to establish a printing press syndicate (Eucla Recorder, 1898). Shares were taken out on a printing press, and a committee was appointed by nomination and election to edit the enterprise. Unsurprisingly the first editor, W J Simmons was a Western Australian (Eucla Recorder 26 May 1900), and Western Australia's Postmaster General, R A Sholl praised the initiative when it began circulating throughout the telegraph fraternity of that colony.

The appearance of the *Eucla Recorder* corresponded with other positive developments at the station, including the construction of new stone quarters in place of wooden cabins and tents, in September 1898, and the declaration of Eucla as a township and a port (Saunders 2005, p.10). For despite its remote coastal location on the edge of the Nullarbor plain, Eucla had

http://doi.org/10.18080/jtde.v7n1.177

grown by the turn of the century into an important communication hub for the East-West telegraph line and become one of the busiest stations outside the Australian capital cities (Moyal 1984, p.66). As Ann Moyal (1984) demonstrates in her epic account, *Clear Across Australia*, the telegraph line followed mineral discoveries, most notably of gold which was booming at Kalgoorlie and Coolgardie in Western Australia at a time when the economies of the eastern colonies had fallen into depression (Blainey 1993).

Figure 1. Eucla New Station 1902

Drawing upon the reminiscences of Eucla telegraphists like Frederick Simmons, Moyal (1987, p.80) affirms the camaraderie and fellowship of the operators, despite the tough and primitive environment in which they worked and lived. This was in part inspired by the growth of Eucla as 'wives joined the growing settlement of telegraphists … breeding large families (and) carefully conserving their stores' before 'the visits of sailing ships and steamers with supplies' (Moyal 1984, p.110). Photographs of the telegraph station community, carefully documented by itinerant photographers, confirm the formal dress conventions of the Eucla operators as a new status group with the colonial society, one which nevertheless made 'few concessions to comfort' throughout their rotating eight hour work shifts. Valuable as such photos undoubtedly are, an examination of the printed record in the *Eucla Recorder* enables a deeper understanding of the collective attitudes which helped bind this remote community together,

http://doi.org/10.18080/jtde.v7n1.177

not only the attitudes of its workforce, but also its social and political interests, extending to issues of gender and the approach of federation in 1901.

Figure 2. Map of the Eyre Highway showing central position of Eucla between Perth and Adelaide

Estimates of the local population, some of it transient, vary from fifty to as many as one hundred (*Eucla Recorder* 6 January 1900; Bursil 1898, p.91), some of which can be explained by the changing nature of telegraph work around that time. From humble beginnings, with a simplex (single) wire and only four operators, Eucla station was, by 1898, employing 26 operators recruited from both the Western Australian and South Australian colonies to work the recently installed and more sophisticated duplex and quadruplex systems (*Eucla Recorder* 12 November 1898).

Consequently, at the time of the paper's appearance, a proud *Eucla Recorder* editor could declare its station to be a notable exception. For, as a border telegraph station and a 'halfway house' with a large number of telegraph staff, Eucla outstripped any other along the Great Australian Bight in size and importance. As one famous photo of the Eucla operating room shows (Figure 2), the two rows of telegraphists from adjacent colonies, worked opposite one another along a partition the length of the room. Each passed incoming hand-written messages to their opposite number, working on the other side of the partition, who in turn translated them, using a Morse code alphabet distinctive to his own colony. Such a physical working arrangements prevailed, even when neighbouring colonial governments, unlike Western Australia and South Australia, employed the same Morse alphabet.

Community Content

One regular item of interest featured in the *Eucla Recorder* was the arrival of the mail. The mail came overland from South Australia on a monthly basis and, in the case of Western

http://doi.org/10.18080/jtde.v7n1.177

Australia, by steamer from Albany (*Eucla Recorder* 15 October 1898; Bursil 1898, p.92). In view of the poor soil and low rainfall at Eucla, food and vegetables had to be imported, while water supplies, always limited, had to be extracted locally and carefully managed (Fuller 1971, p.88). Because letter writing was an important activity for many Eucla residents, the mail brought vital information as well as newspapers, albeit with stale news by the time of receipt. Despite the isolated location, the *Eucla Recorder* and its workforce, which rotated in and out every three to five years, remained deeply interested in communicating with the outside world and in tracking the movements of former staff, some of whom went on to serve on even more remote stations such as Broome or Darwin on the Overland Telegraph Line.

Figure 3. Eucla telegraph room: South Australian operators at work 1902

From its inception, the *Eucla Recorder* was committed to the memory of its predecessors at the station, updating readers on the movements of former Western Australian staff; one was working on a north-western sheep station; a second was now in Darwin; another living in Perth and still manipulating 'the keys at headquarters;' yet another had forsaken telegraph work altogether for an accountant's position in Melbourne (*Eucla Recorder* 15 October 1898). It was the status and education of the telegraph workforce that made such geographical and professional mobility possible. Conscious that 'hundreds of telegraph office workers were scattered across the continent,' the *Eucla Recorder* also kept its readers abreast of current staff changes in and out of the settlement; to Mount Gambier in the case of one long-serving South

http://doi.org/10.18080/jtde.v7n1.177

Australian; or to Perth in the case of the *Eucla Recorder's* own editor in May 1900. Such notices were usually accompanied by generous tributes to those departing, whether it be for their 'athleticism, companionship or untiring perseverance' as fellow workers (*Eucla Recorder* 1 April 1899 and 31 March 1900). In tracking their movements and subsequent working lives, *Eucla Recorder* editorials fostered a wider sense of community and encouraged telegraphic 'esprit de corps' among colleagues, past and present.

Travel journalism was also featured in the paper, including accounts by staff of their return journeys to the station from Port Lincoln along the coast, this, despite the fact that 'no human being (was) to be seen' along that barren stretch of South Australia (*Eucla Recorder* 10 December 1898). To alleviate such long and hazardous journeys, the *Eucla Recorder* editor envisaged the construction of a railway, linking South Australia and Western Australia at Eucla on the border, and called for a survey to be undertaken for this purpose (*Eucla Recorder* 6 March 1899). His commendation corresponded with the beginnings of agitation in Western Australia for a transcontinental railway, a project destined to become a bargaining chip in the complex politics surrounding Federation.

In addition to recruiting an able editor, the *Eucla Recorder* appointed a sports writer to help encourage much-needed relaxation from the demands of the operations room and line maintenance. He covered cricket and racing on a regular basis, while angling, shooting and cycling were also part of staff leisure activities. At the same time, the paper was keen to promote indoor activities such as music, singing and reading. The *Eucla Recorder* published its own regular fictional column which it attributed, rightly or otherwise, to a local contributor (*Eucla Recorder* 15 October 1898). Previously a literary society created at the station had lapsed; but with the welcome addition of a substantial library, local reading increased and it was this improvement, more than any other, which had given rise to the idea of a newspaper. It was to remain the only production of its kind on an Australian telegraph station.

The marked gender imbalance at Eucla in favour of young males was in keeping with colonial society throughout nineteenth century Australia. In this instance, the *Eucla Recorder*, which was conscious that many young men on the staff were socially disadvantaged, assumed a paternal role as their comforter. At key moments during the year, it sought to lift spirits on the station, especially around Christmas and the New Year, when family members were conspicuously absent. Christmas concerts, organised for the event, were deemed essential by the paper for restoring flagging morale among local and community workers. After a succession of bad seasons and hot summer weather, the editor acknowledged, in one December leader of 1898, that his readers were prone to 'the blues' (*Eucla Recorder* 24 June 1899). In the same issue, he warned them against the carefree lifestyle of stockmen and drovers, claiming that the latter were too fond of drinking their wages. If 1890s bush writers

http://doi.org/10.18080/jtde.v7n1.177

like Patterson and Lawson were extolling the virtues of outback living in poetry and prose, the *Eucla Recorder* begged to differ in exhorting its young men to a regular combination of physical and mental activity (*Eucla Recorder* 10 December 1898).

Figure 4. Eucla Residents 1905

Another special event designed to interest and inspire readers was its coverage of a local wedding in December 1899, the first at Eucla in the 22 years of its existence (*Eucla Recorder* 9 December 1899). Such unions, including another at Israelite Bay and a double wedding at Esperance (*Eucla Recorder* 26 May 1900) - both telegraph stations on the Western Australian side of the great east-west line - were regarded as highly newsworthy. In a community where the editor estimated that males outnumbered women and children by 6 to 1 (*Eucla Recorder* 6 January 1900), it was perhaps inevitable that the prospect of literary friendships with women would be deemed highly desirable by *Eucla Recorder* readers, with the prospect of further marital unions. In one 1899 issue, the paper published, alongside conventional advertisements one such matrimonial expression of interest inserted by a member of staff in search of a female correspondent (*Eucla Recorder* 3 March 1899). The author, a traditionalist, stipulated his terms in detail, requesting that his correspondent be 'prepossessing in appearance,' 'docile' in manner and 'able to make bread.' Yet his optimism may have been misplaced. For the times were changing and the pages of the *Eucla Recorder* confirmed that community awareness was beginning to change with it.

http://doi.org/10.18080/jtde.v7n1.177

Tackling big issues of the day: the franchise, Federation, the Boer War and the environment

In Western Australia, women's suffrage had become, in the words of the editor, 'the burning question of the year' (*Eucla Recorder* 10 December 1998). Indeed, the *Eucla Recorder* helped stimulate local discussion at the outset by publishing a letter on the rights of women in one of its early issues and asking whether the female franchise should be introduced. Voting for women and the suffrage were widely debated throughout Australia on the verge of Federation. South Australia had led the way among the Australian colonies by granting women the vote in 1895 (Australian Electoral Commission 2018). On a still more progressive note, the same colony had also granted women the right to stand for parliament, a concession well ahead of other colonies, including Western Australia, which did not endorse it until 1920.

In a border community where workers from both colonies were represented, there were bound to be considerable differences of opinion on the issue. If there were those at Eucla in favour of extending voting rights to 'the great sisterhood of mankind,' (*Eucla Recorder* 12 November 1898) as one writer put it, a majority presumably from Western Australia, where the issue was still undecided, opposed granting women voting rights on the grounds that they were 'not educated enough in politics'. Another opponent debunked their entry into politics on the grounds that it might 'breed a class of women devoid of all charm' (*Eucla Recorder* 10 December 1898). This negative viewpoint, out-of-step with general feeling in both colonies, reflected in part the dominant position of men as operators on telegraph stations, in spite of the inroads which colonial women had made as employees on telephone exchanges (Moyal 1984).

Closely related to the question of voting rights for women was the impending proclamation of Federation in 1901. Conscious of the public's limited knowledge about the machinery of federal government, the *Eucla Recorder* editor set out to explain changes to the bicameral system under the Commonwealth, including the roles of the Senate, the constitution and governing bodies like the public service into which the various colonial postal and telegraph departments would soon be merged as a single entity (*Eucla Recorder* 1 April 1899). As late as 1899, after a succession of federation conferences had canvassed these and related issues, it was clear that the colony of Western Australia, removed from the rivalries of the East Coast, was still divided, with its goldfields districts supporting a Yes vote, while other towns and districts in the populated South-West were urging a No vote (*Eucla Recorder* 9 December 1899).

Proud of their elevated status and occupation, the Eucla workforce had been trained to think beyond individual colonies, as part of a brotherhood playing an important unifying role and 'proud of the trust reposed in them by the governments and publics of their respective colonies'

http://doi.org/10.18080/jtde.v7n1.177

(*Eucla Recorder* 12 November 1899). Yet if they were nationalistic in maintaining professional networks and telegraph lines across the continent, the Eucla telegraphists were also more imperialistic than the mining community or outback workers in canvassing imperial federation and representation for Australia in the English parliament as a viable alternative to going it alone as a separate nation (*Eucla Recorder* 19 August 1899).

There was no better example of such nostalgia and imperial feeling than the newspaper's commentary on the Boer War, in which British and Australian troops became involved over this period (1899–1902). The *Eucla Recorder* consistently reported on the dramatic conflict, to which both South Australian and Western Australian telegraphists were dispatched, applauding 'the brave defenders of Ladysmith,' and adopting a strongly pro-British stance throughout. In this spirit, the editor urged local staff to 'sing the national anthem' and 'raise (their) glasses to their distant colleagues' (*Eucla Recorder* 18 August 1899), after an additional twenty telegraphists were sent to South Africa in February 1900 (*Eucla Recorder* 3 March 1900; Cryle 2017, p.231). In this way, the paper reflected the mood of the times when Australian nationalism was becoming a more potent force.

In editorialising on a series of important current issues, the *Eucla Recorder* was more likely to espouse the views of Western Australians rather than the South Australians working at the station. No doubt this reflected the editor's own background, but also Eucla's geography, situated as it was to the west of the southern border. Yet if it were true that the *Eucla Recorder* remained a Western Australian experiment, it was also prepared to advocate precedents set by South Australia on more than one occasion. The impending arrival of a rabbit plague during 1898-99 (Munday 2017) was one notable instance of its attempt to stir the Western Australian government to action. As rabbits spread relentlessly westwards along the coast, they began to destroy the fragile vegetation, compounding declining morale at the station and threatening to aggravate the drought on surrounding pastoral settlers (*Eucla Recorder* 12 November 1898 and 4 February 1899). With competing local fauna and the kangaroo skin industry in decline, growing numbers of rabbits became a reliable source of meat for wild dogs which in turn preyed on stock. The eventual introduction of cats into the neighbourhood from South Australia, provided ineffective protection against the swarming rabbits which, in time, would threaten the stability of Eucla station itself by burrowing under the dunes on which it was located and exposing the sandy fringe to the full impact of the coastal winds (Fuller 1971, pp.94-99).

Even before the arrival of rabbits, environmental issues loomed large for the paper as well as for its residents. One of the *Eucla Recorder's* consistent preoccupations was with water conservation. For although the resources of the Great Artesian Basin had been discovered as early as 1878 in Australia, this subterranean water resource did not extend beneath the

http://doi.org/10.18080/jtde.v7n1.177

Nullarbor Plain or to parts of the arid southern coastline upon which Eucla was located (Western Australian Government 2018). With the onset of the Great Drought and the withering of existing mallee vegetation, this became an urgent theme in the *Eucla Recorder*, along with the relentless search for underground water sources (*Eucla Recorder* 28 June 1900). The *Eucla Recorder*, in a bid to increase coastal population and secure the progress of the district, urged the government of Western Australia to follow the example set by neighbouring South Australia (*Eucla Recorder* 24 June 1899) which had taken the precaution of sinking 30,000 gallon wells near the station in the earlier years. A subsequent South Australian decision to further expand its network of wells east of the border in response to the drought drew repeated praise from the *Eucla Recorder (Eucla Recorder* 11 November 1899). At a time when water was still scarce on the western side of the border and the overland stock route to the goldfields was proving a hazardous one for local drovers, the editor persisted in calls, largely unheeded, for Western Australia to follow South Australia's more enlightened example (*Eucla Recorder* 31 March 1900).

Conclusions

How long did the *Eucla Recorder* continue, and why did the local newspaper cease? By September of 1900, now two years into its existence and several months after the departure of its first editor, W J Simmons, there were growing signs that the energy of the staff behind the paper was dwindling. Indeed, most small colonial publications of this kind were not destined to survive for much more than two years, relying as they often did on the drive of a single individual (Cryle 1987, p.1). Newspapers of any kind are generally reluctant to divulge such adverse developments. But several years of continuous monthly publication clearly generated increasing tension between the literary staff and the printing press shareholders (*Eucla Recorder* 14 October 1899). Open criticism began to appear in its columns accusing the shareholders of showing too little appreciation of the efforts of staff. Committee meetings were unattended and suggestions to the editor's letterbox dwindled away. Yet the eventual decision to close must have created a vacuum for those who had read the *Eucla Recorder*, sustained it and recognized it for the brave and unique experiment that it was.

References

Agriculture and Water Resources. Western Australia. (2018). 'Great Artesian Basin.' 20 August 2018, Retrieved from https: australianfoodtimeline.com.au/great-artesian-basin/

Australian Electoral Commission. (2018). 'Women and the right to vote in Australia.' 22 June 2018. Retrieved from https://www.aec.gov.au

Blainey, G. (1993). *The Golden Mile*, Sydney: Allen and Unwin.

http://doi.org/10.18080/jtde.v7n1.177

Bursil, H. O. (1898). *Souvenir of the postal, telegraph and telephone departments of Western Australia*, Perth: General Post Office.

Commonwealth of Australia. (2013). 'Eyre Highway'. 24 January 2019. Retrieved from https://en.wikipedia.org/wiki/Eyre_Highway

Cryle, D. (1987). *The Press in Colonial Queensland. A social and political history*, St Lucia: University of Queensland Press.

Cryle, D. (2017). *Behind the Legend: the Many Worlds of Charles Todd*, Melbourne: Australian Scholarly Publishing.

Eucla Recorder. (1898). Eucla Station. October 15, 1898 – September 15, 1900.

Eucla photographic collection (1905). 1902–1905. Adelaide: State Library of South Australia.

Fuller, B. (1971). *The Nullarbor Story*, London: Robert Hale and Company.

Institution of Engineers. Australia, (2001). *Nomination of the East-West Telegraph for a national engineering landmark*, IEA: South Australia and Western Australia divisions, 2 June.

Kirkpatrick, R. (1984). *Sworn to No Master. a history of the provincial press in Queensland to 1930*, Toowoomba: DDIAE Press.

Manion, James. (1982). *Paper Power in North Queensland*, Townsville: North Queensland Newspaper Company Ltd.

Moyal, Ann. (1987). 'The most perfect invention': the arrival of the telegraph in Australia. *Australian Heritage*. pp. 76–81.

Moyal, Ann. (1984). *Clear across Australia: a history of telecommunications*, Melbourne: Nelson.

Munday, Bruce. (2017). *Those Wild Rabbits*, Adelaide: Wakefield Press.

Saunders, B.A. (2005). *Spirit of the Desert: the story of Eucla after the east – west telegraph era*, Kalgoorlie, Western Australia: Eucla history project.

http://doi.org/10.18080/jtde.v7n1.177