ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics and Information Engineering

Vol. 3, No. 1 (Sept. 2015)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

Editor-in-Chief

Publishing Editors

Board of Editors

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 3, No. 1 (Sept. 1, 2015)

Network Neutrality: Developing Business Model and Evidence Based Net Neutrality Regulation

Anurag Rana

Department of Computer Science and Engineering, Arni University, India
(Email: anuragrana.anu@gmail.com)

(Received Apr. 20, 2014; revised and accepted July 5, 2014)

Abstract

This analytical study provides background on the debate over network neutrality, including the implications for business models going forward that have been attempted and that are currently in play. This article explains for a global policy audience what the regulatory and governance problems and potential solutions are for the issue referred to as 'network neutrality', unpacking its 'lite' and 'heavy' elements. Eschewing technical, economic or legalistic explanations previously tackled elsewhere, it explains that increasing Internet Service Provider (ISP) control over content risks not just differentiated pricing and speed on the Internet. It explains that a co-regulatory regime may ensure regulatory oversight and remove obvious abuses by fixed and mobile ISPs, without preventing innovation, while guarding against government abuse of the censorship opportunities provided by new technologies.

Keywords: Internet Provider; Net Neutrality; Non-Discrimination; QoS.

1 Introduction

Over the past ten years, the debate over "network neutrality" has remained one of the central debates in Internet policy. Governments all over the world have been investigating whether legislative or regulatory action is needed to limit the ability of providers of Internet access services to interfere with the applications, content and services on their networks. Net neutrality' comprises two separate non-discrimination commitments. Backward-looking 'net neutrality lite' claims that Internet users should not be disadvantaged due to opaque and invidious practices by their current Internet Service Provider (ISP). Forward-looking 'positive net neutrality' is a principle whereby higher Quality of Service (QoS) for higher prices should be offered on fair, reasonable and non-discriminatory (FRAND) terms to all-comers. Neither extreme in the debate is an optimum solution. There is too much at stake to expect government to supplant the market in providing higher-speed connections, or for the market to continue to deliver without basic policy and regulatory backstops to ensure continued openness. Permitting content discrimination on the Internet will permit much more granular knowledge of what an ISP's customers are doing on the Internet. A co-regulatory regime will ensure oversight and remove the most obvious abuses by fixed and mobile ISPs. Beyond rules that forbid network providers from blocking applications, content and services, non-discrimination rules are a key component of any network neutrality regime.

What constitutes network neutrality? Several definitions are in current use:

- The ability of all Internet users to access the content or applications of their choice.
- Assurance that all traffic on the Internet is treated equally, whatever its source, content or destination.
- Absence of unreasonable discrimination on the part of network operators in transmitting Internet traffic [4].

These definitional differences are not a mere matter of semantics. They differ in (1) the degree of focus on access, versus the quality of access, versus the price of accessing content and applications; and (2) whether one should be concerned with all forms of differentiation, or only with those that are anticompetitive, discriminatory, or otherwise unreasonable. It is worth noting at this point that the concern here is not only with traditional text and audiovisual content, but also with services such as search engines (such as Yahoo, Google, and Bing) and voice over IP (such as Skype and Viber). The use of various forms of quality differentiation for Internet traffic has been routine for decades. Departures from network neutrality (i.e. unreasonable discrimination) could raise a number of quite distinct potential issues of societal welfare, among them:

Anticompetitive behavior: Is there a risk that a network operator with significant market power (SMP) might project its market power into upstream or downstream market segments that would otherwise be competitive?

Innovation: Might a network operator (especially a vertically integrated network operator that possesses some form of market power) act as a gatekeeper, inhibiting the ability of content providers or application service providers with which it competes from offering new, innovative products or services?

Freedom of expression: Might a network operator interfere with the ability of its customers to express views with which the network operator disagrees?

Consumer awareness: Do consumers understand the service that is being offered to them, and are they receiving the service that has been committed?

Privacy: To the extent that a network operator treats some Internet traffic differently from other traffic, does this necessarily imply that the network operator is delving more deeply than it should into the user's personal affairs (e.g. by means of Deep Packet Inspection [DPI])?

2 Developing Business Models

2.1 An Emergence of the Two-Lane Model

Initially, the net neutrality discussions focused on the different treatment of traffic flows in the public Internet. The public Internet is a global system of interconnected networks that use the IP protocol to transport data between the connected end points. The adjective "public" in public internet emphasis that ends users can access all information and applications on the global Internet from their own end point. This information and the applications are offered, either for free or in exchange for payment, by content providers that are connected to an Internet end point themselves as well. The role of the public Internet is essentially that of a transport network that connects users and applications providers across the globe. In principle, the Internet can support all IP-based services and applications by transporting IP traffic between application or content providers and users worldwide. Broadband ISPs play an important role in the public Internet, as they provide the Internet Access Service: the part of the Internet transport chain between the home network or mobile terminal of the user and the larger ISPs that collectively comprise the Internet core. In general, the Internet access service is a best-effort service, e.g., there are no guarantees that IP packets sent over the network reach their destination end point within a certain time. This type of best-effort Internet access services matches the best-effort characteristics of the Internet core. Providers of Internet Access Services increasingly provide other IP-based services in parallel with the Internet access service over same infrastructure. Two well-known examples here are IPTV and IP telephony services provided by a range of European ISPs over their DSL, cable and fiber access networks. Although these services are delivered over the same network infrastructure as the Internet Access Service, they can in a number of respects be distinct from the Internet Access Service. Often, they are offered as "managed services". Other terms that are used are "managed or specialized services" [3] or "additional, differentiated online services". The adjective "managed" can be slightly misleading here, as it does not provide a clear demarcation between these newer forms and the traditional public Internet access service. Although the Internet access service and the Internet core are both characterized as best effort, they are both subject to various types of management to ensure their efficient and reliable operation. Apart from this, application and service providers on the Internet actively monitor and manage their web servers, application stores and other resources. Nonetheless, the degree of management and guarantees for managed services is typically higher than that for the best-effort public Internet. The co-existence of (services and applications) over the public Internet and managed services leads to emergence of the so-called two-lane model [1]. In the two-lane model, the broadband access connection of an end user is used to provide him both with the Internet Access Service and a number of managed services.

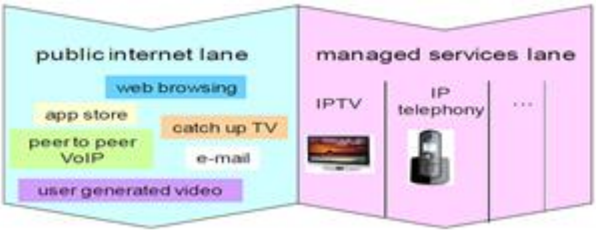


Figure 1: Two lanes model over a single broadband access

In the public Internet lane, the ISP provides an Internet Access Service to the end user. Through this access service, the user gains access to the information and applications on the public Internet. Thus, the user has access to a very large variety of information and applications on the Internet, while he only buys the Internet Access Service from his ISP. In a number of cases, the end user is likely to enter into an agreement or contract with a content provider on the public Internet. These agreements do not involve the ISP and also do not require any action from the ISP. In the managed services lane, the ISP has an agreement with the end user to provide him specific services. There can be a single agreement, made directly between the ISP and the end user. There can also be multiple, interrelated agreements, e.g. one agreement between the end user and a content provider, in combination with a second, related agreement between the content provider and the ISP. Each specific service that an end user buys in the managed services lane requires, in principle, an action by the ISP. Typically, part of this action consists of taking measures to guarantee the quality of the service, for example through the reservation of dedicated bandwidth. In the public Internet lane, no measures are taken to guarantee the quality of specific services.

Table 1 summarizes the characteristics of the public Internet lane and the managed services lane. It is seen that there are substantial differences between the two lanes in two areas that are crucial to net neutrality discussion: openness and quality guarantees.

- Public Internet lane offers more openness.

As discussed earlier, an end user can access all information and buy services from all content providers on the global public Internet via a single Internet access service. In addition to this openness from the end user perspective, there is also openness from the content provider perspective: a content provider connected to the public Internet can reach and provide services to all end users on the global public Internet. The openness in the public Internet lane is obtained through a combination of access and interconnection. The managed service lane, in contrast, has a limited openness. Typically, an end user can only choose among the managed services offered by his own ISP. Also, from the content provider perspective, the openness can be limited: the content provider is heavily dependent on the end user's ISP to provide the service to a particular end user over the managed services lane.

Table 1: Characteristics of the public Internet lane and the managed services lane

	Public Internet Lane	**Managed services Lane**
Services provided by ISP	Single service: access to the global public Internet	Specific service, e.g, IPTV, IP, telephony, etc.
Services provided by other providers	All services on the public Internet ("Over the top services")	Specific services, subject to agreement between other provider and ISP
Agreements between ISP and end user	Single agreement covering Internet access service.	Individual agreements per service
Quality	Best effort (good but no guarantees)	Typically with statistically guaranteed quality for each service.

- The managed services lane offers more quality guarantees.

In the managed services lane, ISPs can, for example, guarantee the availability of bandwidth for specific services or guarantee a small delay of the IP packets. In the public Internet lane, ISPs cannot in general guarantee the quality for specific services, because they handle all traffic using the same best-effort approach. They typically aim to achieve a good quality for the total of the best-effort traffic they transport, within the technical and economic constraints they have, but the performance cannot be guaranteed.

2.2 Openness in the Public Internet Lane

One of the attractive and much valued properties of the public Internet lane is its openness. This section analyses the combination of access and interconnection through which this openness is achieved.

- Through the availability of access at the IP layer (see Figure 2, top right), a content provider can benefit from the IP routing and transport capabilities of the ISP. In essence, the access provides the content provider with a path or connection to the end user he wants to reach. With the access to one ISP network, a content provider can reach all customers of the particular ISP that he is connected to himself.

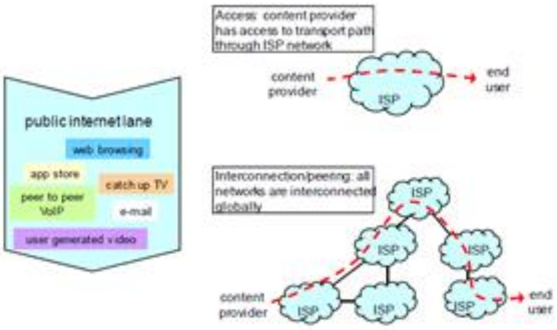


Figure 2: The role of access and interconnection in the public Internet lane

- Because ISP networks are all typically directly or indirectly interconnected through IP peering and IP transit agreements, a content provider can not only reach end users connected to his own ISP's network, but also end users connected to other ISP networks (Figure 2 bottom right). Because of the extensive interconnection of today's ISP networks, a content provider can in principle reach every end user over the global public Internet.

Thus, the current degree of openness in the public Internet lane requires both access and interconnection. With access only, a content provider can reach only a limited group of end users. If the content provider's end users are distributed over multiple ISP networks, which is a typical situation, it would need to connect its service and application platforms to each of these networks, which is difficult and expensive in practice. It is only with interconnection of networks that a large group of customers can be reached, without the need to know the specific IP connectivity arrangements of individual end users.

2.3 Quality Guarantees in the Managed Services Lane

An attractive feature of the managed services lane is the ability to guarantee the quality of the service and applications that are delivered. Since the ISP has detailed knowledge of the services that it has agreed to deliver to the end users, it can apply traffic management measures tailored to the specific services involved. This is typically done by combining the IP QoS mechanisms with bandwidth reservations at the layers below the IP layer. The technology to provide QoS assurance on an end to end basis through the entire Internet has been reasonably implementable for perhaps a dozen years, yet there is hardly any actual implementation between ISPs, even though QoS is commonly implemented within an ISP. There are technical challenges, to be sure, notably including a lack of standardization of QoS levels [10]; however, the absence of QoS aware interconnection has much more to do with economic and business factors than with technical ones [8]. Among the practical challenges are:

- Limited demonstrated consumer willingness to pay for QoS, presumably because performance in the absence of guarantees is nonetheless sufficient for most purposes.

- Network effects and the initial adoption hump: QoS-aware interconnection has little value until and unless critical masses of ISPs implement it.

- Challenges in verifying that the other network has in fact delivered the service that it has committed: This difficulty is compounded by the understandable reluctance of network operators to make the internal performance of their networks visible to their competitors.

- Challenges with the business model: A basic model for assessing different wholesale charges based on (1) the volume of traffic in conjunction with (2) the class of service requested and delivered has been fairly clear for some time[5]. Actual implementation would have to address not only the measurement issues noted previously, but also possible financial penalties for failing to meet performance level commitments (Service Level Agreements).

If bandwidth reservations in the access network are used to obtain quality guarantees in the managed services layer, then this can also affect the quality of the services delivered through the public Internet lane. Since both lanes are typically provided over a single broadband access connection, they share the network capacity in this part of the transport chain. As a result, bandwidth reservations that are beneficial for service delivery in the managed services lane can lead to a lower quality for services delivered through the public Internet lane.

3 Future Business Models Combining Quality Guarantees and Openness

There is, of course, no certainty as to how business models will evolve in the future. In order to clarify possible directions for future evolution, and their relative impact on consumers, we have attempted to identify a number of possible outcomes or scenarios, each based on considerations of a two lane (or multiple lane) Internet. They differ chiefly among three dimensions:

- The quality and bandwidth available to the public lane, in comparison to that available to the managed services lane. Will the public lane offer sufficient bandwidth for over-the-top (OTT) providers? How is the relative balance of bandwidth likely to evolve over time?
- What new services and applications are likely to emerge that might function better with better-then-best-efforts quality? Might the evolution of other sectors (health, energy, transport) drive such applications?
- What market players will have access to the best-efforts lane, and to the managed services lane?

3.1 Possible Scenarios for the Future Evolution of the Sector Include

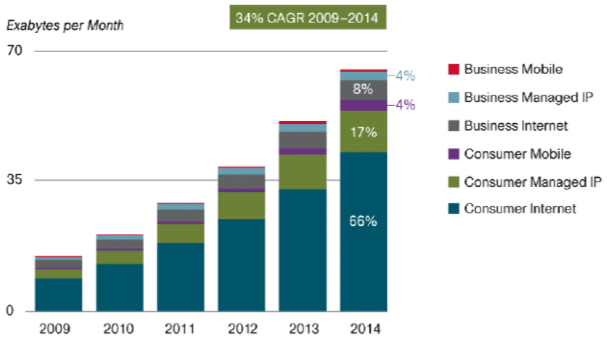
One of the attractive and much valued properties of the public Internet lane is its openness. This section analyses the combination of access and interconnection through which this openness is achieved.

- **Little change from today:** A two lane Internet has been technically feasible for at least ten years. That it has appeared to only a very limited extent may mean that consumers do not want it, or at least that commercial incentives are not strong enough to drive the evolution. This is a rather likely option. The managed services lane already exists, but it is used mainly for the TV and telephony components of triple play. These two components compete to only a limited degree with services delivered over the public Internet lane.
- **Continuation and further expansion of two-lane model:** If traffic over the managed services lane were to substantially increase, either due to new applications or due to increased use of the managed services lane for forms of video that today are in the public lane, might they tend to crowd out services in the public Internet lane? This scenario assumes that access remedies remain relative to traditional service, but that the managed services lane is used exclusively by the facilities based ISP for its own “walled garden” of services.
- **ISPs open up the managed services lane to other providers:** In this scenario, not only does the managed services lane expand, but it is made available to competitors of the facilities-based network operators. Capacity planning potentially becomes more complex than it is today.
- **End-to-end service guarantees become possible in the public Internet:** QoS aware interconnection has been technically feasible for many years, but is hardly ever implemented. If it were possible to surmount the quite substantial practical obstacles, new uses of the Internet might be enabled.

In the remainder of this section, we assess these four scenarios in terms of their relative likelihood, and in terms of their implications for competition, innovation, freedom of expression, consumer awareness, and privacy.

3.2 Relative Likelihood

Given the relative slow pace of change over the past ten to fifteen years in regard to implementation of QoS, it would seem that the most likely scenario reflects only gradual change to the status quo. On the other hand, increasing traffic volumes might drive a more rapid evolution. As part of Cisco Systems’ annual review of likely trends in Internet traffic (based largely on a review of likely take-up of VoIP, video, and sectoral applications), they project a gradual but substantial increase in the scope of the managed services lane for both consumer and business traffic [2]. I find their projections plausible.



Source: Cisco VNI, 2010.[61]

Figure 3: Cisco VNI global overall Internet traffic forecast

This would seem to suggest a steady growth in the importance of the managed services lane, but not necessarily to the point of crowding out services based on the public lane – at least, not for quite some time. We would also caution against simply extrapolating the growth in managed services beyond the period that they have projected – often, there are natural limits to the growth of new services, resulting in S-shaped growth curves that “top out” rather than growing exponentially without limit. The idea that ISPs might open their managed service lane to competitors is perhaps not as far-fetched as it might seem at first blush, even though we are aware of no instance of commercial application today. Several NRAs have considered imposing QoS constraints, with different price levels for different mixes of average delay, jitter, and packet loss. One of our interviewees also indicated that they have a QoS-aware wholesale offer, but no actual take-up. End-to-end guarantees and QoS-aware interconnection pose perhaps the greatest challenges. It is notoriously difficult to bring services over the initial adoption hump in a case like this, which is characterized by strong network effects, long value chains, and high transaction costs (many ISPs that have to somehow find agreement) [7]. For either the “opening the managed services lane” of the “end-to-end guarantees” scenarios, it would be important to arrive at agreed standards on how to interpret QoS. Promising work has been done in this area [10], but much remains to be done.

3.3 Competition

In terms of competition, “little or no change” is familiar and would appear to be acceptable. Further expansion of a two-lane model as a series of broadband ISP-specific “walled gardens” would seem to be a somewhat less attractive model, to the extent that it implies that the broadband ISP’s own services become increasingly important, and that third parties might not be able to offer competitive alternatives that depend on special QoS capabilities. This would effectively confer a certain degree of market power on the broadband ISP, even in cases where competitors using LLU, shared access and/or bit stream access were effective. This is already the case today, but it might take on increasing significance if QoS-sensitive applications were to gain in importance. This form of market power would appear likely to enhance the ability of a facilities-based ISP to extract payments from the other side of the market, to the extent that there are applications that depend on better-than-best-efforts service. This is arguably a negative consequence. There might also be some risk in that scenario of the broadband ISP choosing to permit the public Internet lane to be crowded out in order to make its own manages services lane more attractive in comparison to the offers of competitors; however, NRAs in the EU seem to have adequate tools to deal with this in the form of the minimum QoS authority provided by the 2009 amendments to the regulatory framework. If facilities-based operators were to open their QoS-aware managed service lane to third parties, and if the opening (and other elements of existing regulation) were effective, then one could expect competition to be in good shape. The effect that QoS-aware interconnection would have on competition is heavily dependent on how it is implemented, and by which market players.

3.4 Innovation

Innovation is not just a matter of physical network access. In the complicated and potentially multi-sided market of the Internet, gateways of bottlenecks could serve to inhibit the creation of applications. For example, it is impossible to determine which applications might have been developed, but were not, due to the lack of QoS guarantees in the Internet. It is also possible for the threat of gate keeping activity to inhibit innovation. From the perspective of innovation, scenarios where there is no gatekeeper will tend to preferable to those where there are bottlenecks, other things being equal. Some have argued that, in the absence of additional payments from content providers to broadband ISPs, the latter will not be motivated to build or maintain their networks. We find this argument unpersuasive; however, from a twosided market perspective, such payments are not necessarily objectionable. In general, differentiation can help bring to market new goods and services whose QoS requirements exceed or differ from the market's least common denominator.

3.5 Freedom of Expression

The scenarios that entail a gatekeeper will also tend to be less attractive from the perspective of maintaining freedom of expression; however, National policymakers are unlikely to tolerate limits to freedom of expression, and will find tools to deal with it should problems arise. Examples of network neutrality deviations as a means of interference with freedom of expression have been rare in any case. As a possible example, consider the case of a large US broadband provider that was alleged in 2004 to have systematically filtered all email messages to its subscribers whose content contained the URL of a coalition of activists who opposed the war in Iraq [6].

3.6 Consumer Awareness

In the communications transparent communication of QoS parameters and network management practices has been a recurrent theme. We think that there may be scope for continued technical and policy research on better (more meaningful, more easily grasped, more repeatable) Internet performance metrics. This is independent of scenario that the sector ultimately follows. The scenarios that entail end-to-end QoS assurance, or where the managed lane becomes available to competitors, might be slightly superior from this perspective. They tend to depend on a degree of standardization of QoS, which is likely to be more readily grasped by consumers.

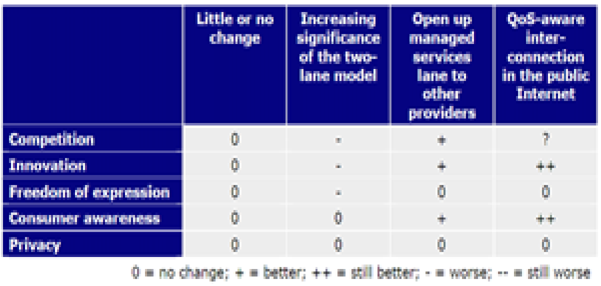
3.7 Privacy

The intersection between network neutrality and privacy is rather limited. The primary concern is that managed services could be implemented by means of Deep Packet Inspection, and that DPI potentially makes a great deal of individual data available to the ISP. The key questions still relate to how the data is used, and how and for how long it is retained. These are still addressed by the e-Privacy Directive. Given that DPI can be used in any of the scenarios (including the “little or no change” scenario), this is not a reason to prefer one scenario over another.

3.8 Comparative Assessment

Table 2 provides a rough assessment of the relative merits of the alternative evolutionary scenarios. As with any table of this type, it should be interpreted with some care. QoS-aware interconnection is in some ways the most promising of the scenarios, but it is also the least likely to emerge.

Table 2: Relative merits of different Internet evolutionary scenarios.



	Little or no change	Increasing significance of the two-lane model	Open up managed services lane to other providers	QoS-aware inter-connection in the public Internet
Competition	0	-	+	?
Innovation	0	-	+	++
Freedom of expression	0	-	0	0
Consumer awareness	0	0	+	++
Privacy	0	0	0	0

0 = no change; + = better; ++ = still better; - = worse; -- = still worse

4 Evidence-Based Net Neutrality Regulation

The Internet’s evolution is dynamic and complex. The availability and design of a suitable regulatory response must reflect this dynamism, and also the responsiveness of regulators and market players to each other. Therefore, national legislation should be future proof and avoid being overly prescriptive, to avoid a premature response to the emerging environment. Regulators expecting a ‘smoking gun’ to present itself should be advised against such a reactive approach. A more proactive approach to monitoring and researching non-neutral behaviors will make network operators much more cognizant of their duties and obligations. The pace of change in the relation between architecture and content on the Internet requires continuous improvement in the regulator’s research and technological training. This is in part a reflection of the complexity of the issue set, including security and Internet peering issues, as well as more traditional telecoms and content issues. Regulators can monitor both commercial transactions and traffic shaping by ISPs to detect potentially abusive discrimination. No matter what theoretical powers may exist, their usage in practice and the issue of forensic gathering of evidence may ultimately be more important. An ex ante requirement to demonstrate internal network metrics to content provider customers and consumers may be a practical solution. Should packet discrimination be introduced, the types of harmful discrimination that can result may be undetectable by consumers and regulators. Blocking is relatively easy to spot, but 'throttling' or choking bandwidth may be more difficult. A solution may be to require network operators to provide their Service Level Agreements both to content providers and more transparently to the end-user via a regulatory or co-regulatory reporting requirement. Strong arguments remain for ensuring that ISPs inform consumers when they reach a monthly download limit or 'cap', ensuring no return to the rationed per-minute or per-byte Internet use. As the law and practice stand today, it seems that most customers do not know when they have been targeted as over-strenuous users of the Internet, only that their connection has slowed. Once targeted, customers generally cannot prove their 'innocence' – they have to accept the Terms of Use of the ISP without appeal (except theoretically via courts for breach of contract, or regulator for infringement of their consumer rights). The number of alternative ISPs is shrinking – not only is the ISP business expensive, leading to concentration in the industry, but the costs of renting backhaul from dominant operators is sufficiently high that no ISP would want to offer service to a suspected 'bandwidth hog'. We may expect to see more protest behavior by 'netizens' who do not agree with these policies, especially where ISPs are seen to have failed to inform end-users fully about the implications of policy changes. Regulators and politicians are challenged publicly by such problems, particularly given the ubiquity of email, Twitter and social media protests against censorship. Regulators will need to ensure that the network operators report more fully and publicly the levels of connectivity that they provide between themselves as well as to end-users. Internet architecture experts have explained that discrimination is most likely to occur at this level as it is close to undetectable by those not in the two networks concerned in the handover of content. A reporting requirement will need to be imposed if voluntary agreement is not possible. As this information is routinely collected by the network operators for internal purposes, it should not impose a substantial burden. Regulators should be wary of imposing costs on ISPs that are disproportionate. Very high entry barrier co-regulation and self-regulation can curb market entry. Onerous regulation (including self-regulation) leads towards closed and concentrated structures, for three reasons:

1) Larger companies are better able to bear compliance costs;

2) Larger companies have the lobbying power to seek to influence regulation;

3) Dominant and entrenched market actors in regulated 'bottlenecks' play games with regulators in order to increase the sunk costs of market entry for other actors, and can pass through costs to consumers and innovators in non-competitive markets.

Therefore, any solution needs to take note of the potential for larger companies to 'game' a co-regulatory scheme and create additional compliance costs for smaller companies (whether content or network operators and the combination of sectors makes this a particularly complex regulatory 'game'). The need for greater research towards understanding the nature of congestion problems on the Internet and their effect on content and innovation is clear [9, 11].

5 Conclusions

There have been scattered complaints, some of them credible, of (1) mobile network operators (MNOs) blocking or charging excessive prices for VoIP, and of (2) blocking or throttling of traffic such as file sharing. Despite all of this, possible concerns for the future remain.This are a policy area with no perfect solutions. Of course the Internet should be open to all, but private investment is the critical component in building a faster Internet. Of course universal service should be supported, and there must be some minimum access to the open Internet for all, whether they use a mobile 3G connection or a fast IPTV-enabled premium service. In light of the current state of play, we think that it is important to avoid inappropriate, disproportionate, or premature action. Based on the findings noted in the previous section, our key recommendations are:

- Do not impose any further network neutrality obligations until there is sufficient experience with the obligations already imposed through the 2009 amendments to the regulatory framework to make a reasoned judgment about their effectiveness;
- Support both technical and policy research to enhance the effectiveness of the consumer transparency obligations, and to ensure that the minimum QoS obligations can be effectively imposed should they prove to be needed;
- Continue to study the aspects of network neutrality where complaints may have some basis, including (1) charges and conditions that mobile operators impose on providers of Voice over IP (VoIP), and (2) impairment of peer-to-peer traffic.

I am happier limiting my conclusions to emphasize the complexity of the problem than trying to claim a one-sizefits-all solution.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC 95-2416-H-159-003. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] BEREC (Body of European Regulators for Electronic Communications): Response to the European commission's consultation on the open Internet and net neutrality in Europe, BoR (10) 42, 30 September 2010. (http://www.erg.eu.int/doc/berec/bor_10_42.pdf)

[2] Cisco VNI: Hyper connectivity and the Approaching Zetta byte Era, 2 June 2010.

[3] FCC (Federal Communications Commission): In the Matter of Preserving the Open Internet, Broadband Industry Practices, GN Docket No. 09-191, WC Docket No. 07-52, October 22, 2009. (http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.doc)

[4] FCC (Federal Communications Commission): In the Matter of Preserving the Open Internet; Broadband Industry Practices; GN Docket No. 09-191, WC Docket No. 07-52, 23 December 2010.

[5] J. J. Laffont, J. S. Marcus, P. Rey, and J. Tirole, "IDE-I, Toulouse: Internet interconnection and the off-net-cost pricing principle", *RAND Journal of Economics*, vol. 34, no. 2, 2003. (http://www.rje.org/abstracts/abstracts/ 2003/rje.sum03.Laffont.pdf)

[6] K. R. Carter, J. S. Marcus, C. Wernick, "Network Neutrality: Implications for Europe", WIK, Diskussionsbeitrag, Nr 314, 2008.

[7] J. S. Marcus, "Evolving core capabilities of the internet", Journal on Telecommunications and High Technology Law, 2004. (http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=921903)

[8] J. S. Marcus, "Framework for interconnection of IP-based networks – Accounting systems and interconnection regimes in the USA and the UK", 27 March 2006. (http://www.bundesnetzagentur.de/media/ archive/6201.pdf)

[9] C. Marsden, S. Simmons, I. Brown, L. Woods, A. Peake, N. Robinson, "Options for and effectiveness of internet selfand co-regulation Phase 2: Case study report', Prepared for European Commission DG Information Society & Media, 2008. (http://ssrn.com/abstract=1281374)

[10] MIT QoS WG: Inter-provider Quality of Service, White paper draft 1.1, 17 November 2006. (http://cfp.mit.edu/publications/CFP_Papers/Interprovi er%20QoS%20MIT_CFP_WP_9_14_06.pdf)

[11] J. Zittrain, The Future of the Internet and How to Stop It. New Haven, CT: Yale University Press, 2008.

Anurag Rana is currently employed as Assistant Professor in Arni University. He acquired M..Tech. Computer Science and Engineering from Arni School of Technology (HP). Author M.Tech. Thesis has published in GRIN Journal Germany. Research Field: Soft Computing (Artificial Neural Network) Specialization Subject: Network Programming, Soft Computing, Object oriented.

M. Tech. CSE with first division from Arni University, HP.

Scored 68 percentile in C-DAC exam organized by C-DAC, Mumbai in January 2009.

Straddling the Next Cyber Frontier: The Empirical Analysis on Network Security, Exploits, and Vulnerabilities

Emmanuel U Opara[1], Oredola A. Soluade[2]
(Corresponding author: Emmanuel U Opara)

College of Business, Prairie View A&M University, Prairie View, Texas U.S.A. [1]
P.O. Box 519, MS 2310, Prairie View A&M University, Prairie View, Texas 77446
Iona College, Hagan School of Business, New Rochelle - New York [2]
(Email: euopara@pvamu.edu)

(Received Apr. 20, 2014; revised and accepted July 5, 2014)

Abstract

Network crime is rising at an exponential level because the world is so interconnected and the internet knows no borders. The magnitude of network breaches and attacks have changed in sophistication as incidents have increased significantly over the past few years. Security defenses at this present time are failing because, security teams are implementing outdated defensive arsenal. These experts are using legacy platforms that leverage technology that are dependent on signatures. However, in today's sophisticated network-attacks that occur across multiple vectors and stages, legacy platforms will not stand a chance to defend a network. This study will create threat awareness; identify who the network threat actors are, find out their capabilities, motivations and objective and identify best practices.

Keywords: Breaches, Exploits, Network Security, Threats, Vulnerabilities

1 Introduction

As enterprise systems evolve, Information Technology [IT] security needs to evolve even faster. Today's competitive platform presents an awkward conundrum. To maintain competitiveness in global market, organizations are under scrutiny to streamline operations and safeguard assets while keeping up with new technologies and maintaining usability of assets for employees, partners, vendors, investors etc. The need to balance speed with demand for security become paramount. In order for enterprise systems to build stronger customer relationship with their clients, they opened up their networks to remote employees, business partners and third parties. This resulting porosity of the network perimeter created security vulnerabilities and exploits in various systems, resulting in breaches and threats.

Network security threats as witnessed in 2013 exploded exponentially as security experts seek for solutions to undermine the potential threats. A number of new attacks in today's increasingly sophisticated toolkits include zero day attacks, Distributed Denial of Service (DDoS), and server-based botnets and encrypted layer attacks. These are just a few of the new attacks challenging organizations. Since 2012, these attacks have been continuous against U.S. financial institutions. This problem continues to be one of the most pressing challenges facing chief information security officers in the global systems. The new network breed of hackers are a new group with a potential or social agenda as noted by a recent study in [1]. This breed as the study will identify, implore sophisticated methods that uses evolving technologies that target network infrastructures. A recent breach was the "Target Corporation" incident. These criminals' capabilities of extracting value and intellectual properties from computers or networks of unsuspecting companies and governmental agencies have become a big business. Enterprise systems can no-longer ignore these threats.

No matter the size of these organizations, network security should be a top priority concern for all organizations. Enterprise networks are more vulnerable than ever due to the inherent risk of facilitating remote access in conjunction with the volume of traffic and the speed at which that traffic is flowing. As organizations migrate from gigabytes to terabytes capacity etc., managing, updating various applications, and closing loopholes at back-end systems becomes a monumental challenge.

Most foreign entities have identified that the four highest priority risk faced by most governments are those arising from international terrorism, network-attacks, international military crises and major accidents or natural hazards. Of this group, network-attacks ranked highest among the four high-priority risks. In recent year, study did show evidence in a series of highly advanced persistent attacks (APT) posed by organized crime and state-level entities, with attacks against enterprises like Google, Coca-Cola, NASA and Lockheed Martin as reported in [2].

The potential impact of network-risk to a governmental entity, states, individuals and organizations, are very high. Some of these risks include, financial loss from theft or fraud, loss of invaluable customer information or intellectual property, possible fines from legal and regulatory bodies, loss of reputation through 'word of mouth', adverse press coverage and survival of the enterprise systems itself.

Other new attacks in today's increasingly sophisticated toolkits include Web exploits that target Java, mobile malware that target Android devices, server-based botnets and encrypted layer attacks. These are just a few of the new attack tools challenging organizations. Most recently, these tactics were leveraged by perpetrators in the attacks against U.S. financial institutions that have been ongoing since September 2012.

Our goal is to provide actionable intelligence to ensure organizations can better detect and mitigate threats that plague their network infrastructure,

As this study will indicate, network threat anecdotes or solutions have become routine within various organization, however, the barrage of alarms has not significantly raised survey respondents' understanding of who these network adversaries are, or what they target and how they operate.

Most of corporate executives have neither adequate knowledge of who the most serious threat actors are, nor do they have a network-security strategy to defend against them.

The key in this study is to create threat awareness; identify who the network threat actors are, find out their capabilities, motivations and objective. With this information, this study will recommend and develop an adequate network security strategy by providing the contextual background against which organizations can identify key assets that will likely be of interest to network adversaries. Such awareness and our result findings will help streamline methodologies for assessment of vulnerabilities to network-attacks which will come from potential network threat actors.

As the authors survey questions 12-15 [appendix 1] revealed, participants were asked, who the top network-threat actors are, that are menacing their organization. This question was raised because, most members of security teams, do not agree on what constitutes the most significant network-threat to their systems. The result of the survey will point us to a direction.

Also in questions 16-24 [appendix 1], survey respondents were asked to respond to the types of proactive tools used to counter Advanced Persistent Threat [APT]. These are commonly use terms to define remote attacks employed by sophisticated threats actors. These actors could be nation states or their intelligence services etc. Some of the intelligence services are classified as:

- Malware
- TCP/IP based network support tools
- Rogue device
- Network subnetting as geolocation of IP Traffic
- Distribution intrusion detection systems (DIDS)
- Deep Packet Inspection [DPI]

The survey results will point us to a direction. The findings from this study, will articulate the current network security measures enterprise systems will have to deploy to counter vulnerabilities, potential breaches and threats.

2 Literature Review

Steinbart, Raschke, Graham William [4] in their study noted that millions of pieces of malware and thousands of malicious hacker-gangs roam today's online world preying on easy unsuspecting exploits. These hackers as cited are seeking for backdoors and vulnerabilities in an un-suspected network so as to steal valuable data.

Vijayan [5], Goldman [6], Javelin [7], among others, cited that companies that have become more reliant on external internet connectivity for daily business operations are susceptible to financial loss if the network is compromised. Distributed denial of service (DDoS) attacks or worm outbreaks that affect a given network infrastructure can have devastating effect on that business as reported in [8].

Lockhart [9], in their report noted that enterprises and government agencies are under virtually constant attack on a daily basis. The report further cited that significant breaches at RSA, Global Payments, Automatic Data Processing, Symantec, International Monetary Fund, and a number of other organizations have made headlines—and undoubtedly thousands more have occurred that have not been reported.

According to report in [2], Government infrastructure has come under attack from network espionage. This report summarized that several cases involving human errors indicated that the governmental agencies need to be more proactive when it comes to protecting critical infrastructures, intellectual property, economic data, employee records and sensitive information [2].

A recent study found that hacking incidences "represent more than one-quarter of the total recorded data breaches for 2013[3]. This according to the study was followed by Subcontractor (third party involvement) at 14.3% and Data on the Move at 13%. Insider Theft was identified in 11.7% of the breaches, Employee Error/Negligence accounted for 9.3% followed by accidental exposure at 7.5%" [3].

In another report by Lockhart [9], it was stated that more that 95% of all attacks tied to state-affiliated espionage employed phishing as a means of establishing a foothold in their intended victim's systems.

Early studies as reported by [7], [10], [11], showed that yesterday's workforce was monolithic. That means that workers were working within tightly controlled corporate perimeters, using computer terminals with limited capabilities and with restricted access to data. The average employee as a result was not a significant security risk to the enterprise system. Later studies by [6], [9], [12], [13], summarized that the rise of new technology has fragmented the monolith. This means that employees now use high-powered pocket-sized gadgets to access and manipulate a wealth of data, most of which is stored in the cloud. As a result, a mobile, fragmented working population that was made possible by combinations of cloud and mobile computing technologies created more opportunities for data breaches and network crimes.

More earlier studies by Skoudis [15], [16], [17], among others noted that "Advanced Exploit Development for Penetration Testers" teaches the skills required to reverse engineering 32-bit and 64-bit applications, performing remote user application and kernel debugging, analyze patches for 1-day exploits, and writing complex exploits, such as use-after-free attacks, against modern software and operating systems. These, will help security experts pinpoint vulnerabilities and develop fixes before damages are done to enterprise data.

Later studies by Lockhart [9], also summarized that to combat the ever-escalating danger posed by network security threats by enterprise systems, forward-thinking organizations have two options. These are to invest significantly in the people, processes and technology required to maintain world-class, 24/7 network security operations, or outsource the function to the growing number of highly effective managed security services providers (MSSPs).

3 Methodology

In order to pilot-test the network-security concerns, the authors constructed, distributed and collected responses from survey questionnaires at a network-security business professional conference in May 2013 at San Antonio Texas.

```
NONPAR CORR
  /VARIABLES=Var005 Var006 Var009 Var018 Var019
with Var001 Var002
  /PRINT=KENDALL TWOTAIL NOSIG
  /MISSING=PAIRWISE.
```

The survey population comprises of professionals who publish research findings and work in their respective fields. These are experts with extensive history in teaching and in the business world. Survey data was distributed to senior IT professionals from midmarket (100 to 999 employees) and enterprise-class (1000 employees or more] organizations. The survey questionnaires were distributed to 320 attendees. The number completed and returned was 202. Overall, we consider these as an equitable representative random population. Most of the survey items were Likert scale types, yes/no responses or categorical, ordinal items, gender, ranks of personnel, etc.

The study conducted a survey of 23 questions covering a range of security issues that are of importance and of concern to IT and security administrators in small and medium size businesses [SMBs]. The questions were designed and conducted to obtain a snapshot of the state of security issues in SMBs and to confirm issues that have been raised in other security studies.

4 Findings/Results

A non-parametric correlation analysis was done to determine the extent of collinearity among all the variables. It was discovered that there was significant correlation between Investment in network security and the use of rogue device scanning when broken down by gender. There was also a significant correlation between the respondent's perception of Downtime as the most effective network security in their organization, or perceiving security issues as the most effective network security tool, or whether geolocation and IP traffic pose the greatest threat to their organization, when it is broken down by the status of the respondent.

Table 1: Non-parametric Correlation

Correlations

			Var001: Gender	Var002: Executive or Senior IT Administrator?
Kendall's tau_b	Var005: Do you agree that investment in cybersecurity in 2013-2014....will provide the best systems solutions to thwart cyberattacks?	Correlation Coefficient	.153*	.017
		Sig. (2-tailed)	**.020**	.792
		N	200	200
	Var006: Downtime is the greatest IT concern of my organization	Correlation Coefficient	-.044	.136
		Sig. (2-tailed)	.536	**.050**
		N	200	200
	Var009: Security Issues is the greatest IT concern of my organization	Correlation Coefficient	.122	.160*
		Sig. (2-tailed)	.079	**.021**
		N	200	200
	Var018: Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to your organization	Correlation Coefficient	-.138	.127
		Sig. (2-tailed)	**.050**	.072
		N	200	200
	Var019: Analysis & Geolocation of IP Traffic is the most proactive activity/technique used to counter persistent threats to your organization	Correlation Coefficient	-.052	.178*
		Sig. (2-tailed)	.459	**.011**
		N	200	200

*. Correlation is significant at the 0.05 level (2-tailed).

One basic question that required further investigation is the degree to which the responses between male and female respondents differed, regarding what they considered to be the greatest network security threat to their organization. The hypothesis is as follows:

H0: There is no significant difference in perspective between male and female respondents regarding whether Investment in network security in 2013 -2014 would increase with private software companies and system integrators and provide the best systems solutions to thwart network attacks.

H1: There is a significant difference in perspective

between male and female respondents regarding whether Investment in network security in 2013 -2014 would increase with private software companies and system integrators and provide the best systems solutions to thwart network attacks.

The test statistic was found to be t n-2 = 0.073. It can therefore be concluded that at the 5% significance level, there is not sufficient evidence that there is a significant difference in perspective between male and female respondents regarding whether Investment in network security in 2013 -2014 would increase with private software companies and system integrators and provide the best systems solutions to thwart network attacks.

Table 2: T-Test on Investment in Cybersecurity

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var005: Investment in Cybersecurity	Equal variances assumed	.001	.977	-1.802	198	.073	-.314	.174	-.658	.030
	Equal variances not assumed			-1.798	191.025	.074	-.314	.175	-.658	.030

The second hypothesis that was tested was to determine if there is any difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

H0: There is no significant difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

H1: There is a significant difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

The test statistic was found to be t n-2 = 0.050. It can therefore be concluded that at the 5% significance level, there is sufficient evidence that there is a significant difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

The SPSS syntax for these tests is shown below:

```
T-TEST GROUPS=Var001(1 2)
/MISSING=ANALYSIS
/VARIABLES=Var005 Var018
/CRITERIA=CI(.95)
```

Table 3: T-Test for Rogue Device Scanning as the most proactive

Independent Samples Test										
		Levine's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Var018:Rogue Device Scanning is the most proactive	Equal variances assumed	16.113	.000	1.964	198	.051	.125	.064	-.001	.251
	Equal variances not assumed			1.986	197.907	.048	.125	.063	.001	.250

A third hypothesis was tested to determine if there is any difference in perspective between Senior IT Executives and Administrators in terms of how they Rate their company's IT concerns with regard to Downtime.

H0: There is no significant difference in perspective between Senior IT and Admin. Respondents in terms of

how they Rate their company's IT concerns with regard to Downtime.

H1: There is a significant difference in perspective between Senior IT and Admin. respondents regarding how they Rate their company's IT concerns with regard to Downtime.

At the 5% significance level, there is sufficient evidence to conclude that there is a significant difference in perspective between Senior. IT Executives and Admin. respondents in terms of how they Rate their company's IT concerns with regard to Downtime. The test statistic was t n-2 = 0.050.

A fourth hypotheses was tested to determine if there is any difference in perspective between Senior IT Executives

and Administrators in terms of how they Rate their company's IT concerns with regard to Security Issues.

H0: There is no significant difference in perspective between senior IT and Admin. respondents regarding how they Rate their company's IT concerns with regard to Security Issues.

H1: There is a significant difference in perspective between senior IT and Admin. respondents regarding how they Rate their company's IT concerns with regard to Security Issues.

Table 4: T-Test on Downtime as greatest IT concern

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var006: Downtime is the greatest IT concern	Equal variances assumed	22.862	.000	-1.926	198	.050	-.158	.082	-.319	.004
	Equal variances not assumed			-2.480	56.250	.016	-.158	.064	-.285	-.030

Table 5: T-Test on Security Issues as greatest IT concern

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var009: Security Issues is the greatest IT concern	Equal variances assumed	20.432	.000	-2.375	198	.019	-.271	.114	-.496	-.046
	Equal variances not assumed			-3.029	55.420	.004	-.271	.090	-.451	-.092

At the 5% significance level, there is sufficient evidence to conclude that there is a significant difference in perspective between Senior. IT and Admin. respondents regarding how they Rate your company's IT concerns with regard to Security Issues.

The test statistic was t n-2=0.019 or 0.004; which justifies the conclusion that there is a significant difference between the two groups. A fifth hypotheses was tested to determine if there is any difference in perspective between Senior IT Executives and Administrators in terms of whether geolocation and IP traffic poses the greatest network security threat to their organization.

H0: There is no significant difference in perspective between Senior IT and Admin. respondents in terms of whether geolocation and IP traffic poses the greatest network security threat to their organization.

H1: There is a significant difference in perspective between Senior IT and Admin. respondents in terms of whether geolocation and IP traffic poses the greatest network security threat to their organization.

The SPSS syntax for these tests is shown below:

```
T-TEST GROUPS=Var002(1 2)
  /MISSING=ANALYSIS
  /VARIABLES=Var006 Var009 Var019
  /CRITERIA=CI(.95).
```

Table 6: T-Test on Geolocation of IP Traffic

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var019: Analysis & Geolocation of IP Traffic	Equal variances assumed	35.230	.000	-2.483	198	.014	-.240	.097	-.431	-.049
	Equal variances not assumed			-4.607	139.546	.000	-.240	.052	-.343	-.137

Overall Conclusion

Quite a number of tests were run comparing responses of male versus female respondents, as well as between Senior IT Executives and Administrators. The results presented here are the ones that indicated a significant difference between the two groups. In addition, the correlation coefficients among all the variables are low– so the assumption of a t-test based on independent samples is validated. All these results were based only on the assumption of homogeneity of variance or homoscedasticity.

5 Implication for Practitioners and Researchers

Exposure to securities litigation following the disclosure of a network-security breach should be a concern to management. Also the impact such an announcement would have on the stock prices of compromised companies should also be a concern. However, announcements of network breaches, in 2013 by Facebook and Apple did not affect the companies' share prices. Despite the high-profile disclosures, these companies were not hit with securities lawsuits about the breaches, either. More studies will be devoted to this concern.

6 Challenges

National state agencies and enterprise systems depend on digital processes, data and a network system to function effectively. This makes them increasingly vulnerable to being manipulated. Network security is about ensuring that enterprise network is resilient to prevent fraud, breaches, theft of sensitive data or business disruption, and the severe risks to reputation that comes with it. Having an Incident Response policy and plan in place is a crucial first step to ensuring that organization has the information and processes needed to respond to a security breach. However, most organizations lack the expertise and resources to perform incident and penetration testing that could disprove a false positive breach result.

7 Summary and Conclusion

The study has shown that continuous monitoring of network infrastructure with proper penetration, detection testing and analyses of the results, will remedy security exploits and vulnerabilities. Also understanding that most modern networks rely on the TCP/IP protocol suite. Network security implications must be considered before proceeding with TCP/IP network designs. Since subnetting separates a network into multiple logically defined segments or subsets, each subnet's traffic must be separated from each other subnet's traffic to harden the network topology.

This study concludes that breach prevention strategies should include adequate risk assessment, mitigation, compliance, breach preparedness etc. Risk assessment should examine all the risk factors an organization encountered during a data breach. A penetration testing and analyses should provide a detailed assessment and remedies for mitigating an exploit. Mitigation and compliance methodology should ensure that an organization enforces the rules, regulations and laws that will help provide extensive regulatory assessments. Also organizations should strive to identify and create the right policies, an efficient incident workflow, establish a network-incident response team' (CIRT). Breach preparedness help create a customized data breach response plan that minimizes the impact of an incidence.

References

[1] Anderson, Kerry A.; “A Case for a Partnership between Information Security and Records Information Management,” ISACA Journal, vol. 2, 2012, www.isaca.org/archives

[2] Rapid7 Report (2012): “Data Breaches in the Government Sector.” Rapid7. September 6, 2012. http://www.rapid7.com.

[3] Steinbart, Paul John; Robyn L. Raschke; Graham Gal; William N. Dilla; “Information Security Professionals’ Perceptions about the Relationship between the Information Security and Internal Audit Functions,” forthcoming in the *Journal of Information Systems*, 2013.

[4] Steinbart, Paul John; Robyn L. Raschke; Graham Gal; William N. Dilla; “The Influence of Internal Audit on Information Security Effectiveness: Perceptions of Internal Auditors,” working paper, 2013

[5] Vijayan, J. (2006), “Possible S&P Security Holes Reveal Risks of E-Commerce,” Computerworld, 34(22), May, 29 6.

[6] Goldman, C. FreeWave Technologies. www.elp.com/articles/powergrid_international/print/volume-17/, 2012.

[7] Javelin, "2009 Identity Fraud Survey Report Consumer Version (2009)," Javelin Strategy and Research, February 2009.

[8] Rob, M., & Opara, E. (2003), “Online Credit Card Processing Models: Critical Issues to Consider by Small Merchants,’’ Human Systems Management, 22(3), 133-142.

[9] Lockhart, B. and Gohn, B. Utility Network security: Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond. Pike Research. 2011.

[10] Alhazmi et al., (2006). “Measuring, analyzing and predicting security vulnerabilities in software systems”, Computers & Security (2006), doi:10.1016/j.cose.2006.10.002.

[11] Holz, T, Gorecki, C Rieck, K and Freiling. F. (2008), “Measuring and detecting fast-flux service networks”. In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS 08) NDSS.

[12] Baldor, Lolita C. (2013), ““US Ready to Strike Back against China Cyberattacks,” Yahoo News, 19 February 2013, http://news.yahoo.com/us-ready-strike-back-against-china-cyberattacks-225730552--finance.html.

[13] Ashford, Warwick; (2013), “Why Has DLP Never Taken Off?,” Computer Weekly, 22 January 2013, www.computerweekly.com/news/2240176414/Why-has-DLP-never-taken-off.

[14] Scholtz, T. (2004), “The Benefits of an Information Security Architecture,” Meta Group, December.

[15] Skoudis, E. (2005), “Five Malicious Code Myths and How to Protect Yourself in 2005,”SearchSecurity.com, Retrieved January 4, from, (http://searchsecurity.techtarget.com/tip/1,289483,sid14_gcu041736,00.html)

[16] Antonopoulos. A, (2008) “Georgia network war overblown”. *Network World*, August 19, 2008 (http://www.pcworld.com/businesscenter/article/150021/georgia_networkwar_overblown.html).

[17] Endeavor, et.al [2009]. Conference for Homeland Security 2009 (CATCH ’09), Network security Applications and Technology, March 3–4, 2009. The IEEE proceedings of this conference include relevant papers on detection and mitigation of botnets, as well as correlation and collaboration in cross-domain attacks, from the University of Michigan and Georgia Tech. *Network & Distributed System Security (NDSS) Symposium,* February 2008.

Dr. Emmanuel U Opara is an Associate Professor of Management Information Systems at the College of Business, Prairie View A&M University. He teaches Networking, Cyber Securities, E-Commerce Technologies, and Strategic IT Management, Information Systems, and Fundamentals of MIS.

He has interest in Integrated Network Systems Securities, Biometrics Technology, Data Communication, Strategic IT Management and Decision Making, SAP-ERP, HANA Technology.

His passion is in computer forensics, vulnerability and exploits discovery, intrusion detection/prevention analysis, incident response and penetration testing while deploying python programming.

Prior to joining the Texas A&M Systems, at Prairie View, he worked for Chevron Corporation as a Systems Analyst. He also worked in the upstream division.

Dr. Opara received commendations for his contributions in the field of Information technology and cyber security.

Dr. Oredola A. Soluade is currently an Associate Professor of Information Systems at Iona College, where he teaches, among other courses, Information Systems, Production & Operations Management, Statistics, and Quantitative Tools for Management.

Prior to joining Iona College, Dr. Soluade taught for several years in the field of mechanical engineering, specializing in Thermodynamics and Heat Transfer.

His current research interests include: Quality Assurance in an Interactive Voice Response System, as well as Statistical

Analysis of the automobile industry. Dr. Soluade is the author of an Operations Management book published by McGraw-Hill.

Dr. Soluade has served as guest editor of an International Journal of Business Continuity and Risk Management, and

has contributed chapters to a book on Risk Management. He is a Cisco Certified Network Associate, and a member of the Editorial Board of the International Information Management Association.

Dr. Soluade holds a bachelor's degree in mechanical engineering, a master's degree in mechanical engineering, a master's degree in Operations Research, and a doctorate in Operations Research.

Appendix 1: Network-Security Survey Questionnaire

1	**Select Gender Male = 1; Female = 2**					
2	**Are you an executive or a senior IT administrator? Yes = 1 No = 2**					
3	**How secured do you think your company network is?**					
4	**How strongly do you agree to the effectiveness of the Network security systems of your organization?**					
5	Do you agree that investment in networksecurity in 2013 -2014 that would increase with private software companies and system integrators will provide the best systems solutions to thwart network-attacks [Extremely agree, Moderately agree, Agree, disagree, Don't know]					
On a scale of 1 [least] to 5 [most], rate your company's daily IT concerns						
6	**Downtime**	1	2	3	4	5
7	**Compliance**	1	2	3	4	5
8	**eDiscovery**	1	2	3	4	5
9	**Security Issues**	1	2	3	4	5
10	**Network Growth**	1	2	3	4	5
11	**User support**	1	2	3	4	5
On a scale of 1 [least] to 5 [most], rate the groups that poses the greatest networksecurity threat to your organization						
12	Hackers	1	2	3	4	5
13	Current and former employees	1	2	3	4	5
14	Foreign nation-states examples China, Russia, North Korea,	1	2	3	4	5
15	Organized crime	1	2	3	4	5
On a scale of 1 [least] to 5 [most], rate the following proactive activities and techniques that your organization uses to counter advance persistent threats to your organization?						
16	Malware analysis	1	2	3	4	5
17	Inspection of outbound traffic	1	2	3	4	5
18	Rogue device scanning	1	2	3	4	5
19	Analysis and relocation of IP traffics	1	2	3	4	5
20	Subscription services	1	2	3	4	5
21	Deep packet inspection	1	2	3	4	5
22	Examining external footprint	1	2	3	4	5
23	Don't know; not sure	1	2	3	4	5
24	Document watermarking/tagging	1	2	3	4	5

Subliminal-free Variant of Schnorr Signature with Provable Security

Yinghui Zhang[1,2], Hui Li[3], Xiaoqing Li[3], and Hui Zhu[3]
(Corresponding author: Yinghui Zhang)

National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications[1]
No.1 Weiguo Road, Chang'an District, Xi'an 710121, P.R. China
State Key Laboratory of Information Security, Institute of Information Engineering[2]
Chinese Academy of Sciences, Beijing 100093, P.R. China
State Key Laboratory of Integrated Service Networks (ISN), Xidian University[3]
No.2 South Taibai Road, Xi'an 710071, P.R. China
(Email: yhzhaang@163.com)

(Received Apr. 20, 2014; revised and accepted July 5, 2014)

Abstract

Subliminal channels still exist in Schnorr signature, which presents a severe challenge to information security. In this paper, we formalize the notion and security model of subliminal-free signature, and propose a subliminal-free construction of Schnorr signature. In the proposed scheme, an honest-but-curious warden is introduced to help the signer to generate a signature on a given message, but it is disallowed to sign messages independently. Hence, the signing rights of the signer are guaranteed. In particular, our scheme can completely close the subliminal channels existing in the random session keys of Schnorr signature scheme under the intractability assumption of the discrete logarithm problem. Also, the proposed scheme is proved to be existentially unforgeable under the computational Diffie-Hellman assumption in the random oracle model. Performance experiments indicate that the proposed scheme is efficient and practical.

Keywords: Digital Signature; Information Hiding; Subliminal Channel; Subliminal-Freeness.

1 Introduction

Subliminal channels in digital signature schemes were first constructed by Simmons [1]. Simmons proposed a prison model in which authenticated messages are transmitted between two prisoners and are known to a warden. The term of “subliminal” means that the sender can hide a message in the authentication scheme, and the warden cannot detect or read the hidden message. Simmons discovered that a secret message can be hidden inside the authentication scheme and he called this “hidden” communication channel as the subliminal channel. The “hidden” information is known as subliminal information. Therefore, as a communication channel, a subliminal channel allows a sender to transmit additional secret messages to authorized receivers. To achieve this goal, subliminal receivers often share a subliminal key with the sender to protect the subliminal message, which cannot be detected by any unauthorized receivers without additional information. Subliminal channels can be used not only to transmit secret information, but also to hide a communication fact, which is a severe challenge to information security.

As a main part of information hiding techniques [2-6], subliminal channels have been widely studied and applied. To the best the authors' knowledge, subliminal channels still exist in Schnorr signature [7], which presents a severe challenge to information security.

1.1 Our Contribution

Our contributions are two-folds:

(1) We formalize the notion and security model of subliminal-free signature schemes. Then, we propose a subliminal-free variant of Schnorr signature scheme, in which an honest-but-curious warden is introduced to help the signer to generate a signature on a given message, but it is disallowed to sign messages independently. In addition, the signer cannot control outputs of the signature algorithm. To be specific, the sender has to cooperate with the warden to sign a given message.

An extended abstract of of this paper appears in the international conference ICT-EurAsia 2013, March 25-29, Yogyakarta, Indonesia. This version includes consistency analysis of the proposed scheme, a detailed security proof, experimental results based on OPENSSL library, and performance analysis.

(2) We prove that the proposed scheme is secure under the presented models. To be specific, in the random oracle model, our scheme is provably secure and can completely close the subliminal channels existing in the random session keys in Schnorr signature scheme. Also, the proposed scheme can be used as a signature scheme which introduces a warden to examine the messages and approve generation of a signature. Finally, performance experiments indicate that the proposed scheme is efficient and practical.

1.2 Related Work

It has been shown that subliminal channels exist in various kinds of algorithms, such as digital signature and asymmetric key generation. These subliminal channels traditionally exploit parameter randomness in the algorithms and redundancies in plaintexts. Plenty of researches have been done on both the construction of subliminal channels and the design of subliminal-free protocols [8-14]. Since the introduction of subliminal channels, Simmons [15] also presented several narrow-band subliminal channels that do not require the receiver to share the sender's secret key. Subsequently, Simmons [13] proposed a broad-band subliminal channel that requires the receiver to share the sender's secret key. For the purpose of information security, Simmons then proposed a protocol [16] to close the subliminal channels in the DSA digital signature scheme. However, Desmedt [10] showed that the subliminal channels in the DSA signature scheme cannot be completely closed using the protocol in [16]. Accordingly, Simmons adopted the cut-and-choose method to reduce the capacity of the subliminal channels in the DSA digital signature algorithm [17]. However, the complete subliminal-freeness still has not been realized. To be specific, the computation and communication costs significantly increase with the reduction of the subliminal capacity. On the other hand, subliminal channels in the NTRU cryptosystem and the corresponding subliminal-free methods [18] were proposed. As far as the authors know, the latest research is mainly concentrated on the construction [8, 12, 14] of subliminal channels and their applications [9].

In a zero knowledge proof system, a user is able to prove that a statement is true without revealing any other information [19]. It is noted that, zero knowledge proof systems are usually interactive in that the prover and verifier have to communicate with each other before the verifier determines whether to accept a given proof. Certain applications, however, require these proofs to be non-interactive. In this case, the prover must generate a proof such that any other user can verify it just based on the proof and some public parameters. Blum et al. [20] first introduced the notion of non-interactive zero knowledge (NIZK) proof systems. However, the original NIZK proof systems [20, 21] losses practicality due to bad efficiency and just can serve as theoretical research. Recently, general NIZK proof systems with more desirable efficient have been proposed [22]. Note that, NIZK proof systems can be used to individual privacy protection applications and have attracted an enormous amount of research [23, 24]. Portions of the work presented in this paper have previously appeared as an extended abstract [25]. We revise the paper a lot and add more technical details as compared to the extended abstract. First, in order to understand the proposed scheme at a high level, we add Section 4.1. Second, for the subliminal-free construction, we provide detailed formal security proofs in Section 5.2, which is lacking in [25]. Third, we do intensive experiments in Section 5.4 to show that the proposed scheme is suitable for real-world applications.

1.3. Outline of the Paper

The remaining of this paper is organized as follows. In Section 2, we introduce some notations, complexity assumptions, and zero knowledge proof, and then discuss subliminal channels in probabilistic digital signature. In Section 3, we lay out the abstract subliminal-free signature specification and give the formal security model. The proposed provably secure and subliminal-free variant of Schnorr signature scheme is described in Section 4. Some security considerations and efficiency-related issues are discussed in Section 5. Finally, we conclude the work in Section 6.

2 Preliminaries

2.1 Notations

Throughout this paper, we use the notations, listed in Table 1, to present our construction.

Table 1: Meaning of notations in the proposed scheme

Notation	Meaning
$s \in_R \mathbb{S}$	s is an element randomly chosen from a set $\mathbb{S}$.
l_s	The bit length of the binary representation of s.
$s_1 \parallel s_2$	The concatenation of bit strings s_1 and s_2.
$\gcd(a, b)$	The greatest common divisor of two integers a and b.
x^{-1}	The modular inverse of x modulo q such that $x^{-1}x = 1 \mod q$, where x and q are relatively prime, i.e., $\gcd(x, q) = 1$.
$\mathbb{G}_{g,p}$	A cyclic group with order q and a generator g, where q is a large prime factor of $p - 1$ and p is a large prime. That is, $\mathbb{G}_{g,p} = \{g^0, g^1, \cdots, g^{q-1}\} =< g >$ $< g >$, which is a subgroup in multiplicative group $GF^*(p)$ of the finite field $GF(p)$.

2.2 Complexity Assumptions

- **Discrete Logarithm Problem (DLP):** Let $\mathbb{G}$ be a group, given two elements g and h, to find an integer x, such that $h = g^x$ whenever such an integer exists.
- **Intractability Assumption of DLP:** In group $\mathbb{G}$, it is computationally infeasible to determine x from g and h.
- **Computation Diffie-Hellman (CDH) Problem:** Given a 3-tuple $(g, g^a, g^b) \in \mathbb{G}^3$, compute $g^{ab} \in \mathbb{G}$. An algorithm $\mathcal{A}$ is said to have advantage ϵ in solving the CDH problem in $\mathbb{G}$ if $\Pr\left[\mathcal{A}(g, g^a, g^b) = g^{ab}\right] \geq \epsilon$, where the probability is over the random choice of g in $\mathbb{G}$, the random choice of a and b in $\mathbb{Z}_q^*$, and the random bits used by $\mathcal{A}$.
- **CDH Assumption:** We say that the (t, ϵ)-CDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the CDH problem in $\mathbb{G}$.

2.3 Schnorr Signature Scheme

The Schnorr signature scheme [26] was derived from the Schnorr identification scheme via the Fiat-Shamir transform [27]. The concrete signature is generated as follows:

- **Setup:** Let $\mathbb{G}$ be a cyclic group of prime order p and $g \in \mathbb{G}$ be a generator. Also, let $H : \{0,1\}^* \longrightarrow \mathbb{Z}_p$ be a secure hash function.
- **KeyGen:** It returns $x \in_R \mathbb{Z}_p$ as a secret key and the corresponding public key is $y = g^x \mod p$.
- **Sign:** The signer chooses $r \in_R \mathbb{Z}_p$ and computes $R = g^r$. Then the signer computes $c = H(R \parallel M)$ and $y = r + x \cdot c \mod p$. Finally, the signature of M is output as $\sigma = (c, y)$.
- **Verify:** After receiving the signature message (M, σ) , the verifier parses σ as (c, y) and computes $c' = H(y^{-c}g^y \parallel M)$. The verifier returns 1 if and only if $c = c'$.

2.4 Zero Knowledge Proof

In a zero knowledge proof system, a user is able to prove that a statement is true without revealing any other information. Non-interactive zero knowledge proof systems further require that the prover generate a proof such that any other user can verify it just based on the proof and some public parameters. In the proposed construction, NIZK proofs for the following equality of discrete logarithms are required.

Let g_1 and g_2 be two generators of the group $\mathbb{G}$ of prime order p. Let $H : \{0,1\}^* \rightarrow \{0,1\}^k$ be a secure hash function. Suppose that a prover with possession of a secret number $x \in \mathbb{Z}_p$ wants to prove that $x = \log_{g_1} u_1 = \log_{g_2} u_2$ without exposing x, which is denoted as $DL_{g_1}(u_1) = DL_{g_2}(u_2)$. Chaum and Pedersen [28] firstly proposed an efficient proof as follows: The prover chooses a number $\rho \in_R \mathbb{Z}_p$, and then sends the verifier $h = H(g_1, g_2, u_1, u_2, g_1^\rho, g_2^\rho)$, and $\lambda = \rho - hx \mod p$. The verifier accepts the proof if and only if $h = H(g_1, g_2, u_1, u_2, g_1^\lambda u_1^h, g_2^\lambda u_2^h)$. The above NIZK proof technique will be used in our construction of subliminal-free signatures.

2.5 Subliminal Channels in Probabilistic Digital Signature

Probabilistic digital signature can serve as the host of subliminal channels. In fact, the subliminal sender can embed some information into a subliminal channel by controlling the generation of the session keys. After verifying a given signature, the subliminal receiver uses an extraction algorithm to extract the embedded information. Note that the extraction algorithm is only possessed by the authorized subliminal receiver. Hence, anyone else cannot learn whether there exists subliminal information in the signature [29], not to mention extraction of the embedded information.

In a probabilistic digital signature scheme, the session key can be chosen randomly, and hence one message may correspond to several signatures. More specifically, if different session keys are used to sign the same message, different digital signatures can be generated. This means that redundant information exists in probabilistic digital signature schemes, which creates a condition for subliminal channels. The subliminal receiver can use these different digital signatures to obtain the subliminal information whose existence can hardly be learnt by the others. In particular, there exist subliminal channels in a typical probabilistic digital signature scheme, that is, Schnorr Signature [26].

3 Definition and Security Model

3.1 Specification of Subliminal-free Signature Scheme

A subliminal-free signature scheme consists of three polynomial-time algorithms **Setup**, **KeyGen**, an interactive protocol **Subliminal-Free Sign** and **Verify** below. Based on a subliminal-free signature scheme, a sender A performs an interactive protocol with a warden W. And, W generates the final signature σ and transmits it to a receiver B. Note that W is *honest-but-curious*. That is, W will honestly execute the tasks assigned by the related algorithm. However, it would like to learn secret information as much as possible.

- **Setup:** It takes as input a security parameter λ and outputs system public parameters $Params$.
- **KeyGen:** It takes as input a security parameter λ, system public parameters $Params$ and returns a signing-verification key pair (sk, pk).
- **Subliminal-Free Sign:** An interactive protocol between the sender and the warden. Given a message M, a signature σ is returned.
- **Verify:** It takes as input system public parameters $Params$, a public key pk and a signature message (M, σ). It returns 1 if and only if σ is a valid signature on message M.

These algorithms must satisfy the standard consistency constraint of signature, namely when the secret keys sk is generated by the algorithm **KeyGen** and the corresponding public key is pk, then $\forall M \in \mathcal{M}$, we have $\textbf{Verify}(Params, pk, M, \sigma) = 1$, where

$$\sigma = \textbf{Subliminal-Free Sign}(Params, sk, M).$$

3.2 Security Model

We take the unforgeability of the signature into consideration. For general signature schemes, since only the signer and the verifier participate in the generation of a signature, there is no difference between the ability of the verifier and any third party to forge a signature, and the adversary is just any third party. In the proposed scheme, the warden participates in the generating signature. Hence the ability of the warden to forge a signature is enhanced. We regard the warden as the adversary. Based on the above considerations, we regard the warden as the adversary, which is the main difference between our security model and general security models. After series of hash queries and signature queries, if the adversary can forge a valid signature on a new message with a non-negligible probability, he is successful. To ensure a smooth implement of the protocol, it is necessary for the adversary to interact with the sender according to the protocol. The formal definition of existential unforgeability against adaptively chosen messages attacks (**EUF-CMA**) is based on the following **EUF-CMA** game involving a simulator $\mathcal{S}$ and a forger $\mathcal{F}$:

- **Setup:** $\mathcal{S}$ takes as input a security parameter λ, and runs the **Setup** algorithm. It sends the public parameters to $\mathcal{F}$.
- **Query:** In addition to hash queries, $\mathcal{F}$ issues a polynomially bounded number of queries to the following oracles:
  - ✧ *Key generation oracle* $\mathcal{O}_{KeyGen}$: Upon receiving a key generation request, the simulator $\mathcal{S}$ returns a signing key.
  - ✧ *Signing oracle* $\mathcal{O}_{Sign}$: $\mathcal{F}$ submits a message M, and $\mathcal{S}$ gives $\mathcal{F}$ a signature σ.

- **Forgery:** Finally, $\mathcal{F}$ attempts to output a valid forgery (M, σ) on some new message M, i.e., a message on which $\mathcal{F}$ has not requested a signature. $\mathcal{F}$ wins the game if σ is valid.

The advantage of $\mathcal{F}$ in the **EUF-CMA** game, denoted by $\mathsf{Adv}(\mathcal{F})$, is defined as the probability that it wins.

Definition 1. (Existential Unforgeability) A probabilistic algorithm $\mathcal{F}$ is said to (t, q_H, q_S, ϵ)-break a subliminal-free signature scheme if $\mathcal{F}$ achieves the advantage $\mathsf{Adv}(\mathcal{F}) \geq \epsilon$, when running in at most t steps, making at most q_H adaptive queries to the hash function oracle H, and requesting signatures on at most q_S adaptively chosen messages. A subliminal-free signature scheme is (t, q_H, q_S, ϵ)-secure if no forger can (t, q_H, q_S, ϵ)-break it.

4 Subliminal-Free Variant of Schnorr Signature

4.1 Main Idea

The previous subliminal-free schemes such as the one for the DSA digital signature scheme, which applies the cut-and-choose technique [17], cannot obtain complete subliminal-freeness. In fact, the reason is that the outputs of the signature algorithm are controlled only by the sender and received by the receiver. In addition, they are not modified by anyone else in the signature generation process. In other words, the signature is finally accomplished only by the sender.

In our scheme, the main idea to realize complete subliminal-freeness is to introduce an *honest-but-curious* warden to prevent the sender from completely controlling the outputs of the signature algorithm. Note that a warden is allowed to send a forged signature to convince the receiver that the signature is valid. Accordingly, the warden will not help the sender to construct a subliminal channel.

4.2. Construction

- **Setup:** Let (p, q, g) be a discrete logarithm triple associated with group $\mathbb{G}_{g,p}$. Let A be the sender of message $M \subseteq \{0,1\}^*$, B be the receiver of M and W be the warden. It chooses $t \in_R (1, q)$, t to W and computes $T = g^t \mod p$. Let H_0, H_1, H be three hash functions, where $H_0 : \{0,1\}^* \to \mathbb{G}_{g,p}$, $H_1 : \{0,1\}^* \to (1, q)$, and $H : \{0,1\}^* \times \mathbb{G}_{g,p} \to (1, q)$. Then, the public parameters are $Params = (p, q, g, H_0, H_1, H, T)$.
- **KeyGen:** It returns $x \in_R (1, q)$ as a secret key and the corresponding public key is $y = T^x \mod p$.
- **Subliminal-Free Sign:** The detailed process is shown in Figure 1, which is described as follows:

  (1) W chooses two secret large integers c and d satisfying $cd = 1 \mod q$. Also, W chooses $k_w \in_R (1, q)$, thus $\gcd(k_w, q) = 1$. Then W computes $\alpha = g^{k_w c} \mod p$ and sends α to A.

  (2) A chooses $k_a \in_R (1, q)$, thus $\gcd(k_a, q) = 1$. Then A computes $h_0 = H_0(M)$, $\beta = \alpha^{k_a h_0} \mod p$ and sends (h_0, β) to W.

  (3) W computes $r = \beta^d = \alpha^{k_a h_0 d} = g^{k_a k_w h_0 cd} \mod p = g^{k_a k_w h_0} \mod p$, $v_1 = y^{k_w^{-1}} \mod p$ and sends (r, v_1) to A.

  (4) A computes $e = H(M \parallel r)$, $f = e^x \mod p$ and $v_2 = g^{k_a h_0} \mod p$. Then A prepares a non-interactive zero knowledge proof $DL_e(f) = DL_T(y)$ and sends (e, f, v_2) to W.

  (5) W verifies the non-interactive zero knowledge proof. If it fails, W terminates the protocol. Otherwise, W computes $u = k_w v_1^{-1} f^{-1} v_2^{-1} \mod p$, $\theta = u^{-1} t \mod p$ and sends θ to A.

  (6) A computes s' and then sends (M, s') to W:

$$\begin{aligned} s' &= k_a h_0 + \theta \cdot (v_1^{-1} f^{-1} v_2^{-1}) \cdot xe \\ &= k_a h_0 + (u^{-1} t) \cdot (v_1^{-1} f^{-1} v_2^{-1}) \cdot xe \\ &= k_a h_0 + (v_2 f v_1 k_w^{-1} t) \cdot (v_1^{-1} f^{-1} v_2^{-1}) \cdot xe \\ &= k_a H_0(M) + k_w^{-1} xte \mod q. \end{aligned}$$

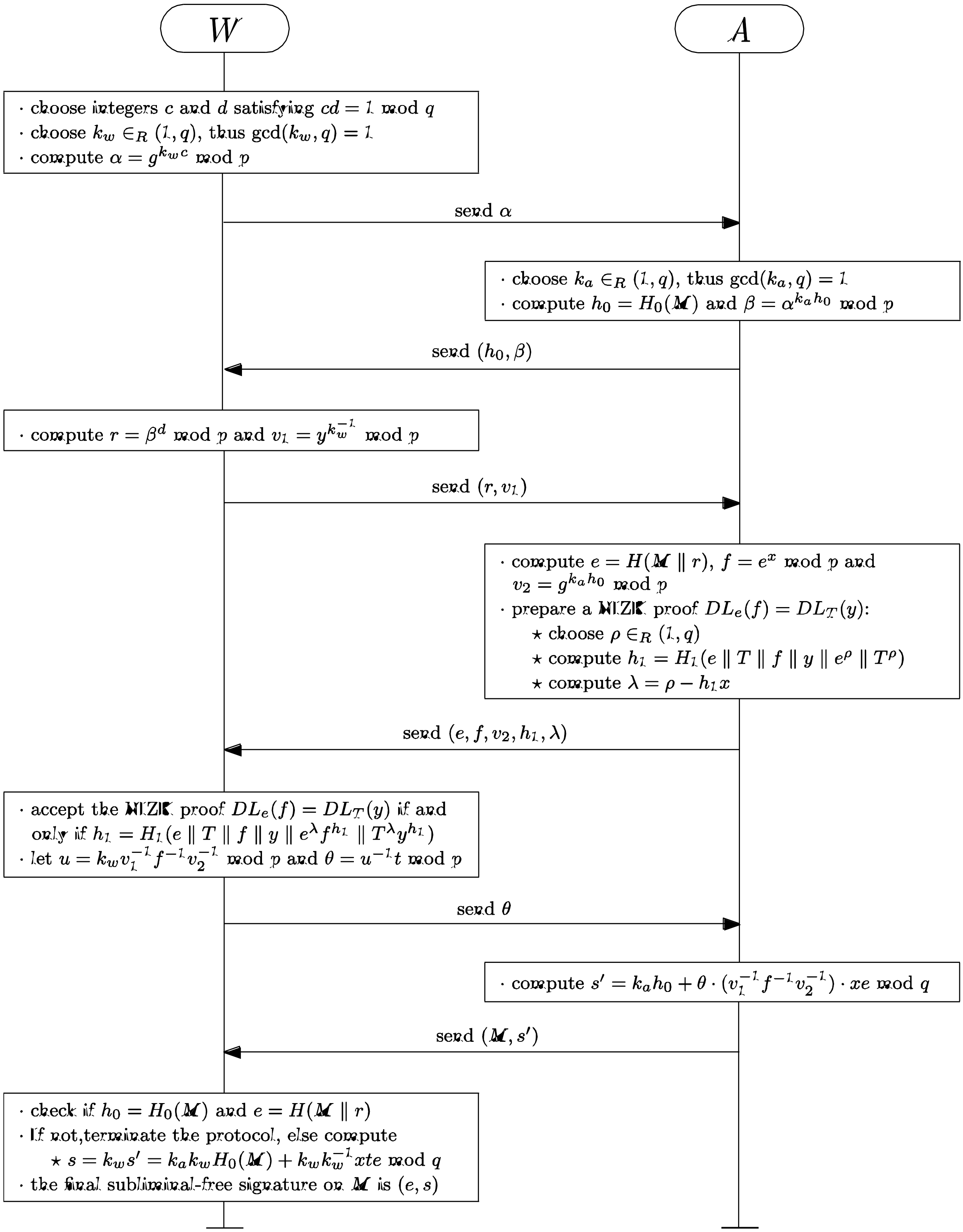

W
A
· choose integers c and d satisfying $cd = 1 \bmod q$
· choose $k_w \in_R (1, q)$, thus $\gcd(k_w, q) = 1$
· compute $\alpha = g^{k_w c} \bmod p$
send α
· choose $k_a \in_R (1, q)$, thus $\gcd(k_a, q) = 1$
· compute $h_0 = H_0(\boldsymbol{M})$ and $\beta = \alpha^{k_a h_0} \bmod p$
send (h_0, β)
· compute $r = \beta^d \bmod p$ and $v_1 = y^{k_w^{-1}} \bmod p$
send (r, v_1)
· compute $e = H(\boldsymbol{M} \| r)$, $f = e^x \bmod p$ and $v_2 = g^{k_a h_0} \bmod p$
· prepare a NIZK proof $DL_e(f) = DL_T(y)$:
$\star$ choose $\rho \in_R (1, q)$
$\star$ compute $h_1 = H_1(e \| T \| f \| y \| e^\rho \| T^\rho)$
$\star$ compute $\lambda = \rho - h_1 x$
send $(e, f, v_2, h_1, \lambda)$
· accept the NIZK proof $DL_e(f) = DL_T(y)$ if and only if $h_1 = H_1(e \| T \| f \| y \| e^\lambda f^{h_1} \| T^\lambda y^{h_1})$
· let $u = k_w v_1^{-1} f^{-1} v_2^{-1} \bmod p$ and $\theta = u^{-1} t \bmod p$
send θ
· compute $s' = k_a h_0 + \theta \cdot (v_1^{-1} f^{-1} v_2^{-1}) \cdot xe \bmod q$
send $(\boldsymbol{M}, s')$
· check if $h_0 = H_0(\boldsymbol{M})$ and $e = H(\boldsymbol{M} \| r)$
· If not,terminate the protocol, else compute
$\star$ $s = k_w s' = k_a k_w H_0(\boldsymbol{M}) + k_w k_w^{-1} xte \bmod q$
· the final subliminal-free signature on $\boldsymbol{M}$ is (e, s)

Figure 1: Generation of the subliminal-free signature

(7) Sign: Upon receiving (M, s'), checks if $h_0 = H_0(M)$ and $e = H(M \parallel r)$. If not, W terminates the protocol, else W computes

$$\begin{aligned} s &= k_w s' = k_a k_w H_0(M) + k_w k_w^{-1} xte \\ &= k_a k_w H_0(M) + xte \mod q. \end{aligned}$$

Then W sends the signature message $(M, (e, s))$ to B.

- **Verify:** After receiving the signature message $(M, (e, s))$, B computes $r' = g^s y^{-e} \mod p$ and $e' = H(M \parallel r')$. B returns 1 if and only if $e = e'$.

5 Analysis of the Proposed Subliminal-free Signature

5.1 Consistency of our Construction

On one hand, if $(M, (e, s))$ is valid, we have $s = k_a k_w H_0(M) + xte \mod q$. Thus,

$$\begin{aligned} r' &= g^s y^{-e} = g^{k_a k_w H_0(M) + xte \mod q} y^{-e} \\ &= g^{k_a k_w H_0(M)} T^{xe} y^{-e} = g^{k_a k_w H_0(M)} y^e y^{-e} \\ &= g^{k_a k_w H_0(M)} = r \mod p, \end{aligned}$$

and then $e' = H(M \parallel r') = H(M \parallel r) = e$.

On the other hand, if $e = e'$, the signature message $(M, (e, s))$ is valid. Otherwise, we have $s \neq k_a k_w H_0(M) + xte \mod q$, and then $r' \neq r$. However, $e' = H(M \parallel r') = H(M \parallel r) = e$. Thus, a collision of H is obtained, which is infeasible for a secure hash function.

5.2 Existential Unforgeability

Theorem 1. If $\mathbb{G}_{g,p}$ is a (t', ϵ')-CDH group, then the proposed scheme is $(t, q_{H_0}, q_H, q_S, \epsilon)$-secure against existential forgery on adaptively chosen messages in random oracle model, where

$$\begin{aligned} t &\geq t' - (q_H + 3.17 q_S) \cdot C_{Exp}, \\ \epsilon &\leq \epsilon' + q_S \cdot (q_{H_0} + q_S) 2^{-l_M} + q_S (q_H + q_S) 2^{-l_r} + q_H 2^{-l_q}. \end{aligned}$$

Notice that C_{Exp} denotes the cost of a modular exponentiation in $\mathbb{G}_{g,p}$.

Proof. Let $\mathcal{F}$ be a forger that $(t, q_{H_0}, q_H, q_S, \epsilon)$-breaks our proposed scheme. We construct a "simulator" algorithm $\mathcal{S}$ which takes $((p, q, g), (g^a, g^b))$ as inputs and runs $\mathcal{F}$ as a subroutine to compute the function $DH_{g,p}(g^a, g^b) = g^{ab}$ in t' steps with probability ϵ' where

$$\begin{aligned} t' &\leq t + (q_H + 3.17 q_S) \cdot C_{Exp}, \\ \epsilon' &\geq \epsilon - q_S \cdot (q_{H_0} + q_S) 2^{-l_M} - q_S (q_H + q_S) 2^{-l_r} - q_H 2^{-l_q}. \end{aligned}$$

Setup: $\mathcal{S}$ makes the signer's verification key $y = g^a \mod p$ public, where the signing key a is unknown to $\mathcal{S}$. Aiming to translate $\mathcal{F}$'s possible forgery $(M, (e, s))$ into an answer to the function $DH_{g,p}(g^a, g^b)$, $\mathcal{S}$ simulates a running of the proposed scheme and answers $\mathcal{F}$'s queries. $\mathcal{S}$ uses $\mathcal{F}$ as a subroutine and maintains three lists L_0, L_1, L, L_s, where L_0, L_1, and L are used to record $\mathcal{F}$'s queries to oracle H_0, H_1, and H, respectively. Remember that L is used to record simulation of the signing oracle and all lists are empty at first.

Query: $\mathcal{F}$ makes the following queries:

- H_0 **query** $\mathcal{O}_{H_0}(M)$: Suppose that the forger $\mathcal{F}$ provides a query M as input to the H_0-oracle. If a term (M, h_0) can be found in the list L_0, $\mathcal{S}$ returns h_0, else $\mathcal{S}$ returns $h_0 \in_R \mathbb{G}_{g,p}$ and adds it into L_0.
- H_1 **query** $\mathcal{O}_{H_1}(e, T, f, y, e^\rho, T^\rho)$: Suppose that the forger $\mathcal{F}$ provides a query $(e, T, f, y, e^\rho, T^\rho)$ as input to the H_1-oracle. If a term $((e, T, f, y, e^\rho, T^\rho), h_1)$ can be found in the list L_1, $\mathcal{S}$ returns h_1, else $\mathcal{S}$ returns $h_1 \in_R (1, q)$ and adds it into L_1.

- H **query** $\mathcal{O}_H(M,r)$: Suppose that the forger $\mathcal{F}$ provides a query (M,r) as input to the H-oracle. If a term $((M,r),e)$ can be found in the list L, $\mathcal{S}$ returns e, else $\mathcal{S}$ chooses $\tau \in_R (1,q)$ and computes $e = g^{b\tau} \mod p$. Then $\mathcal{S}$ adds $((M,r),e)$ into the list L and returns e.
- **Key generation query** $\mathcal{O}_{KeyGen}(\cdot)$: $\mathcal{S}$ chooses $x \in_R (1,q)$ and returns x. Then $\mathcal{S}$ makes T^x public.
- **Signing query** $\mathcal{O}_{Sign}(M)$: Suppose that the forger $\mathcal{F}$ asks for a signature on a message M after the H_0 and H oracle queries. Algorithm $\mathcal{S}$ attempts to create a valid signature $(M,(e,s))$ without knowing the signing key a. The process of the simulation proceeds as follows.

  (1) If $\mathcal{S}$ finds a term (M,h_0) in the list L_0, it aborts the simulation. Otherwise, $\mathcal{S}$ chooses $h_0 \in_R \mathbb{G}_{p,g}$ and adds (M,h_0) into L_0, and then let $H_0(M) = h_0$.

  (2) After receiving r, if $\mathcal{S}$ finds a term $((M,r),e)$ in the list L, it aborts the simulation. Otherwise $\mathcal{S}$ chooses $j \in_R (1,q)$ and computes $f = y^j \mod p$, $e = T^j \mod p$, then it adds $((M,r),e)$ into L and defines $H(M \parallel r) = e$. Finally $\mathcal{S}$ sends (e,f) to the forger $\mathcal{F}$. Note that $DL_e(f) = DL_T(y)$, that is, $e^a = f \mod p$.

  (3) After receiving h_0 and v_1, $\mathcal{S}$chooses $s' \in_R (1,q)$ and computes $v_2 = g^{s'} v_1^{-e} \mod p$, and then it sends v_2 to the forger $\mathcal{F}$.

  (4) The simulator $\mathcal{S}$ sends s' to the forger $\mathcal{F}$. Then $\mathcal{F}$ obtains a signature (e,s) on the message M, where $s = k_w s' = k_a k_w H_0(M) + xte \mod q$.

Forgery: For a new message M, suppose that the simulator $\mathcal{S}$ calls the forger $\mathcal{F}$ and $\mathcal{F}$ obtains a valid signature $(M,(e,s))$.

Solving the CDH Problem: $\mathcal{S}$ can solve the CDH problem with non-negligible probability when the following two conditions hold.

- **Condition 1.** The forger $\mathcal{F}$ has ever queried H oracle on (M,r), that is, a term including (M,r) can be found in the list L.
- **Condition 2.** The discrete logarithm equation $DL_e(f) = DL_T(y)$ holds, where $T^a = y \mod p$.

According to Condition 1, we have $e = H(M \parallel r) = g^{b\tau}$. Condition 2 means $e^a = f \mod p$. Hence, $f = \left(g^{b\tau}\right)^a = \left(g^{ab}\right)^\tau \mod p$ and $f^{\frac{1}{\tau}} = g^{ab} \mod p$. Obviously the simulator $\mathcal{S}$ has successfully solved the function $DL_{g,p}(g^a, g^b) = g^{ab}$.

Probability Analysis: For simplicity, let ϵ_{abort} be the probability that the algorithm $\mathcal{S}$ aborts the simulation, NH be the event that the forger $\mathcal{F}$ produces a valid forgery $(M,(e,s))$ without querying H oracle on (M,r), and NQ be the event that $\mathcal{F}$ produces a valid forgery $(M,(e,s))$ and $DL_e(f) \neq DL_T(y)$. Then the probability that $\mathcal{S}$ outputs a correct solution to the CDH challenge $DL_{g,p}(g^a, g^b)$ is at least $\epsilon - (\epsilon_{abort} + \Pr(NH \cup NQ))$. The detailed process is as follows:

- **Case 1.** The signing oracle simulation might fail at Step (1). This event occurs if the simulator $\mathcal{S}$ finds a tuple including M in the list L_0. Since there are at most $q_{H_0} + q_S$ such message M, the probability of failure is at most $(q_{H_0} + q_S)\, 2^{-l_M}$. Therefore, the probability that $\mathcal{S}$ aborts at Step (1) for any of the q_S signing queries is not more than $q_S\,(q_{H_0} + q_S)\, 2^{-l_M}$.
- **Case 2.** The signing oracle simulation might fail at Step (2). Suppose that only the message M has been determined at Step (1) and r is not fixed. This event occurs if the simulator $\mathcal{S}$ finds a tuple including (M,r) in the list L. Since there are at most $q_H + q_S$ such tuple (M,r), the probability of hash collision is at most $(q_H + q_S)\, 2^{-l_r}$. Therefore, the probability that $\mathcal{S}$ aborts at Step (2) for any of the q_S signing queries is not more than $q_S\,(q_H + q_S)\, 2^{-l_r}$.
- **Case 3.** If the event $NH \cup NQ$ occurs, $\mathcal{S}$ cannot solve the CDH problem. Observe that $\Pr(NH \cup NQ) = \Pr(NH \cap \overline{NQ}) + \Pr(NQ)$. The probability $\Pr(NH \cap \overline{NQ})$ means both the event NH and $\overline{NQ}$ occur. Hence the equation $f^{-a} = e = H(M \parallel r)$ holds for a valid forged signature. Since H is a random oracle, the equation holds with the probability not more than 2^{-l_q}. We now compute the probability $\Pr(NQ)$. Suppose that $r = g^k \mod p$, $y = T^x = g^{tx} \mod p$, and $f = e^{x'} \neq e^x \mod p$. Considering the fact that the forged signature $(M,(e,s))$ is valid and according to the signature verification algorithm, we have

$r = g^s y^{-e} \mod p$, hence $k = s - etx$ and $H(M \parallel r) = e = \frac{s-k}{tx}$. Since H is a random oracle, the forger $\mathcal{F}$ finds the above r during all the H-oracle queries with the probability not more than $q_H 2^{-l_q}$.

From the above analysis, it follows that the algorithm $\mathcal{S}$ solves the CDH problem with probability at least

$$\begin{aligned} & \epsilon - (\epsilon_{abort} + \Pr(NH \cup NQ)) \\ = \quad & \epsilon - \left(q_S\left(q_{H_0} + q_S\right)2^{-l_M} + q_S\left(q_H + q_S\right)2^{-l_r} + q_H 2^{-l_q}\right) \end{aligned}$$

,which gives the security result.

Time Analysis: The running time of $\mathcal{S}$ is mainly from the running time of $\mathcal{F}$ and a number of modular exponentiations in group $\mathbb{G}_{g,p}$. Note that two multi-exponentiations are approximately equal to 1.17 exponentiations in cost [30]. It is easy to conclude that the running time of $\mathcal{S}$ is approximately $t + (q_H + 3.17 q_S)C_{Exp}$.

5.3 Subliminal-freeness

It can be seen from the proposed scheme that the receiver B can only obtain the signature message $(M, (e, s))$ and temporary value r in addition to the verification public key y, thus it is necessary for the sender A to use e, s or r as a carrier when transmitting subliminal information.

In the following, we demonstrate that none of e, s and r can be controlled by A. On one hand, although the parameters $(\alpha, v_1, \theta) = (g^{k_w c}, y^{k_w^{-1}}, u^{-1}t) \mod p$ can be obtained by A, the secret exponents c, d and the secret parameters t, u are unknowable to him. Thus, A cannot obtain any information about k_w and g^{k_w}. Particularly, A knows nothing of k_w and g^{k_w} in the whole process of signing, hence the value of $s = k_w s' \mod p$ cannot be controlled by A. On the other hand, although the signer A computes $e = H(M \parallel r)$, nothing of k_w and g^{k_w} is available to him. Thus, the value of $r = g^{k_a k_w H_0(M)} \mod p$ cannot be controlled by A, and hence the value of e cannot be controlled. Note that if the value r generated by the warden W is not used by A in the Step (4), W can detect this fact in the Step (7) and terminate the protocol. Furthermore, if A attempts to directly compute k_w from g^{k_w}, he has to solve the discrete logarithm problem in group $GF^*(p)$, which is infeasible according to the intractability assumption of DLP.

As can be known from the above analysis, no information can be transmitted to the receiver B by the sender A in the proposed scheme. Thus, we realize the complete subliminal-freeness of the subliminal channels existing in the random session keys in Schnorr signature scheme.

5.4 Efficiency Analysis

The proposed scheme firstly completes the subliminal channels existing in the random session keys in Schnorr signature scheme. We only take modular exponentiation operations into consideration. In fact, compared with modular exponentiation operations, other operations such as modular multiplication [31] and hash are negligible. In the proposed scheme, in order to generate a subliminal-free signature, the sender and the warden need 4.34 and 3 modular exponentiation operations besides pre-computation, respectively. It is noted that, the time cost of a simultaneous modular exponentiation of the form $g^{\lambda}h^{\mu}$ in $\mathbb{G}_{g,p}$ is 1.17 times of that of a single modular exponentiation [30]. In addition, 6 message exchanges are needed between the sender and the warden. Figure 2 shows the computation cost of subliminal-free signature for the sender and the warden, which has been investigated based on OPENSSL library with a Celeron 1.1 GHz processor as the the sender and a Dual-Core 2.6 GHz processor as the warden. It easily follows from Figure 2 that a subliminal-free signature can be generated within 10 ms, which is desirable for real-world applications.

In general, as the first provably secure subliminal-free variant of Schnorr signature, the proposed scheme is efficient and practical.

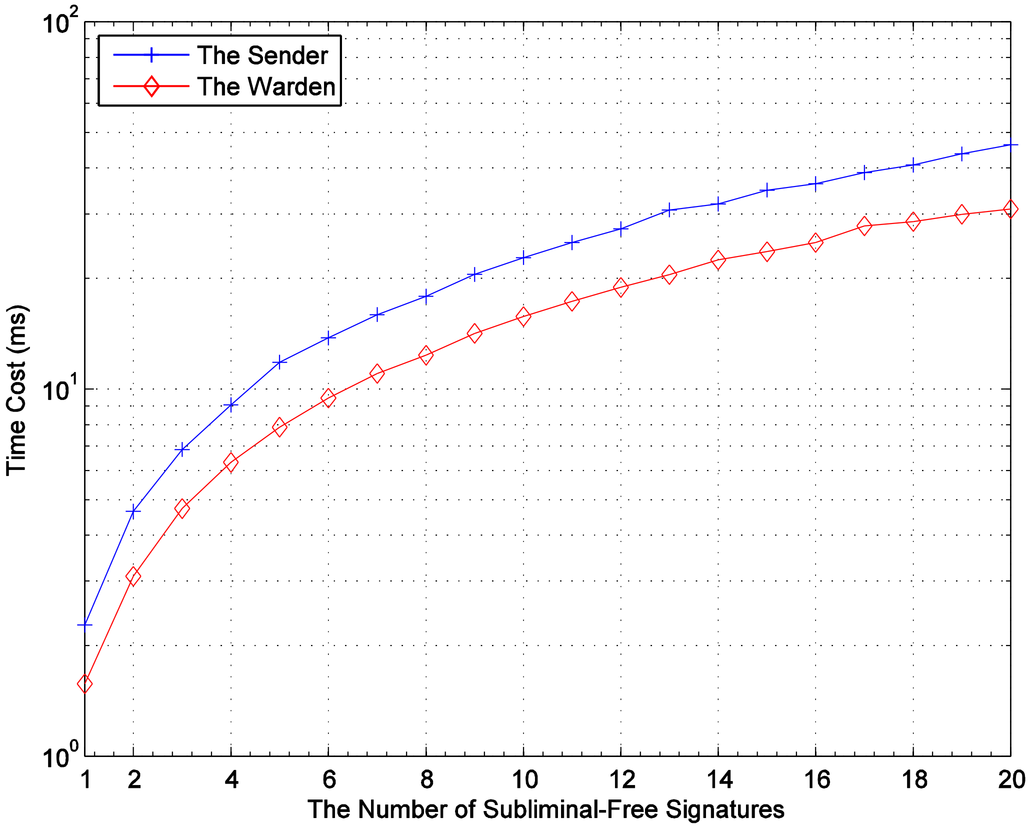


Figure 2: Computation cost of subliminal-free signatures

6 Conclusions and Future Work

In this paper, we formalize the notion and security model of subliminal-free signature, and a subliminal-free protocol for Schnorr signature scheme is proposed. The proposed protocol completely closes the subliminal channels existing in the random session keys in Schnorr signature scheme. More strictly, it is completely subliminal-free in computational sense, and its security relies on the CDH assumption in the random oracle model. In addition, it is indispensable for the sender and the warden to cooperate with each other to sign a given message, and the warden is honest-but-curious and cannot forge a signature independently.

It would be interesting to construct subliminal-free signature schemes provably secure in the standard model.

Acknowledgments

The author gratefully acknowledges the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China (Grant Nos. 61402366, 61272037, 61272457, and 61472472), the Ministry of Industry and Information Key Project Fund (Grant No. 2013ZX03002004), and the Natural Science Foundation of Shaanxi Province (Grant No. 2013JZ020).

References

[1] G. J. Simmons, “The Prisoner’s problem and the subliminal channel,” in *Advances in Cryptology-CRYPTO'83*, Springer, pp. 51-67, 1984.

[2] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu, “Reversible watermarking: current status and key issues,” *International Journal of Network Security*, vol. 2, no. 3, pp. 161-170, 2006.

[3] R. Goudar and P. More, “Hybrid covert channel an obliterate for information hiding,” in *Proceedings of the 3th International Conference on Trends in Information, Telecommunication and Computing*, Springer, pp. 609-613, 2013.

[4] P. Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data,” *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, pp. 1-4, 2012.

[5] B. Surekha and G. Swamy, “Sensitive digital image watermarking for copyright protection,” *International Journal of Network Security*, vol. 15, no. 2, pp. 113-121, 2013.

[6] Y. Tsai, W. Huang, and B. Peng, “An efficient and distortion-controllable information hiding algorithm for 3D polygonal models with adaptation,” *International Journal of Network Security*, vol. 17, no. 1, pp. 66-71, 2015.

[7] C. P. Schnorr, “Efficient identification and signatures for smart cards,” in *Advances in Cryptology-CRYPTO'89*, Springer, pp. 239-252, 1990.

[8] L. Yang, C. M. Li, T. Hwang, “Subliminal channels in the identity-based threshold ring signature,” *International Journal of Computer Mathematics*, vol. 86, no. 5, pp. 753-770, 2009.

[9] C. L. Chen and J. J. Liao, “A fair online payment system for digital content via subliminal channel,” *Electronic Commerce Research and Applications*, vol. 10, no. 3, pp. 279-287, 2011.

[10] Y. Desmedt, “Simmons' protocol is not free of subliminal channels,” in *Proceedings of the 9th IEEE Workshop on Computer Security Foundations*, pp. 170-175, 1996.

[11] K. Kim F. Zhang, B. Lee, “Exploring signature schemes with subliminal channel,” in *Symposium on Cryptography and Information Security'03*, pp. 245-250, 2003

[12] D.-R. Lin, C. Wang, Z.-K. Zhang, and D. J. Guan, “A digital signature with multiple subliminal channels and its applications,” *Computers & Mathematics with Applications*, Vol. 60, No. 2, pp. 276-284, 2010.

[13] G. J. Simmons, “Subliminal communication is easy using the DSA,” in *Advances in Cryptology-EUROCRYPT'93*, Springer, pp. 218-232, 1994.

[14] X. Xin and Q. Li, “Construction of subliminal channel in ID-based signatures,” in *International Conference on Information Engineering*, pp. 159-162, 2009.

[15] G. J. Simmons, “The subliminal channels of the US digital signature algorithm (DSA),” in *Advances in Cryptology-Cryptography-SPRC'93*, pp. 15-16, 1993.

[16] G. J. Simmons, “An introduction to the mathematics of trust in security protocols,” in *Computer Security Foundations Workshop VI*, pp. 121-127, 1993.

[17] G. J. Simmons, “Results concerning the bandwidth of subliminal channels,” *IEEE Journal on Selected Areas in Communications*, vol. 16, pp. 463-473, 1998.

[18] Q. Cai and Y. Zhang, “Subliminal channels in the NTRU and the subliminal-free methods,” *Wuhan University Journal of Natural Sciences*, vol. 11, pp. 1541-1544, 2006.

[19] D. Zheng, Q. Zhao, and Y. Zhang, “A brief overview on cryptography,” (in Chinese) *Journal of Xi’an University of Posts and Telecommunications*, vol. 15, no. 6, pp. 1-10, 2013.

[20] M. Blum, A. D. Santis, S. Micali, and G. Persiano, “Noninteractive zero-knowledge,” *SIAM Journal on Computing*, vol. 20, no. 6, pp. 1084-1118, 2006.

[21] U. Feige, D. Lapidot, and A. Shamir, “Multiple noninteractive zero knowledge proofs under general assumptions,” *SIAM Journal on Computing*, Vol. 29, No. 1, pp. 1-28, 1999.

[22] J. Groth, R. Ostrovsky, and A. Sahai, “Perfect non-interactive zero knowledge for NP,” in *Advances in Cryptology-EUROCRYPT'06*, Springer, pp. 339-358, 2006.

[23] H. Lipmaa, “Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments,” in *Theory of Cryptography*, Springer, pp. 169-189, 2012.

[24] R. Pass, “Unprovable security of perfect NIZK and non-interactive non-malleable commitments,” in *Theory of Cryptography*, Springer, pp. 334-354, 2013.

[25] Y. Zhang, H. Li, X. Li, and H. Zhu, “Provably secure and subliminal-free variant of schnorr signature,” *ICT-EurAsia'13*, Springer, pp. 383-391, 2013.

[26] C. P. Schnorr, “Efficient signature generation by smart cards,” *Journal of cryptology*, vol. 4, no. 3, pp. 161-174, 1991.

[27] A. Fiat and A. Shamir, “How to prove yourself: practical solutions to identification and signature problems,” in *Advances in Cryptology-CRYPTO'86*, Springer, pp. 186-194, 1986.

[28] D. Chaum and T. P. Pedersen, “wallet databases with observers,” in *Advances in Cryptology-CRYPTO'92*, Springer, pp. 89-105, 1993.

[29] G. J. Simmons, “Subliminal channels: past and present,” *European Transactions on Telecommunications*, vol. 5, no. 4, pp. 459-474, 1994.

[30] Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+ cost (encryption),” in *Advances in Cryptology-CRYPTO'97,* Springer, pp. 165-179, 1997.

[31] G. C. Rao, P. Lakshmi, and N. Shankar, “A new modular multiplication method in public key cryptosystem,” *International Journal of Network Security*, vol. 15, no. 1, pp. 23-27, 2013.

Yinghui Zhang received his Ph.D degree in Cryptography from Xidian University at 2013. Currently, he works at Xi’an University of Posts and Telecommunications. His research interests are in the areas of wireless network security, cloud security and cryptography.

Hui Li received B.Sc. degree from Fudan University in 1990, M.Sc. and Ph.D. degrees from xidian University in 1993 and 1998. In 2009, he was with Department of ECE, University of Waterloo as a visiting scholar. Since 2005, he has been the professor in the school of Telecommunications Engineering, Xidian University, China. Now, he is the director of International Affairs Office and dean of School of International Education. His research interests are in the areas of cryptography, wireless network security, information theory and network coding. He has published over 130 papers in academic journals and conferences. He is the co-author of two books. He served as TPC co-chair of ISPEC 2009 and IAS 2009, general co-chair of E-Forensic 2010, ProvSec 2011 and ISC 2011.

Xiaoqing Li received her M.S. and Ph.D. degrees from Xi'an Jiaotong University and Xidian University in 2007 and 2011, respectively. Her research interests are in the areas of network security and secure routing protocol. She has published papers on the international conference IAS, INCoS, and on the Chinese Journal of Electronics, Journal on Communications, Journal of Computer Research and Development, etc.

Hui Zhu received his B.S. degree in Telecommunications Engineering from Xidian University, the M.S. degree in Computer System Architecture from Wuhan University, and the Ph.D. degree in Information Security from Xidian University, in 2003, 2005 and 2009, respectively. He is currently an associate professor in the School of Telecommunications Engineering, Xidian University. His research interests include information security and public key cryptography.

A Novel Trust Based System to Detect the Intrusive Behavior in MANET

Deverajan Ganesh Gopal[1] and R. Saravanan[2]

(Corresponding author: Deverajan Ganesh Gopal)

School of Computing Science and Engineering, Vellore Institute of Technology, India[1]
School of Information Technology and Engineering, Vellore Institute of Technology, India[2]
(Email: ganeshgopal@vit.ac.in and rsaravanan@vit.ac.in)

(Received Apr. 20, 2014; revised and accepted July 5 & Dec. 12, 2014)

Abstract

MANET is vulnerable to several challenging security breaches because of dynamic nature. In this work, we propose an IDS that is based on trust rates. The entire work of this system can be compartmentalized into three phases. They are Pre-eminent node selection, Inter-cluster trust rate computation, Intra-cluster trust rate computation. In the first phase of this work, a pre-eminent node is selected based on the trust rate. The reason for the incorporation of the cluster based IDS is the effective utilization of energy, which is essential for dynamic MANET. The next phase of this work focuses on the inter-cluster trust rate computation. This is carried out by the Bayes Theorem. The next phase of the work is intra- cluster trust rate computation and this is done by the Dempster-Shafer theory. The system is tested in both aspects of routing and intrusion detection. The proposed system shows remarkable accuracy rate.

Keywords: Bayes Theorem, Dempster-Shafer Theory; MANET.

1 Introduction

A Mobile Ad hoc Network (MANET) is composed of several mobile nodes that are geographically dispersed. The concept of centralised authority is absent in this type of network and hence the nodes depend on each other, in order to transmit packets. Hence, it is evident that the nodes act both as routers and as hosts. Some of the applications of MANET include sensor networks, conferences and emergency based network [3].

MANET is vulnerable to several challenging security breaches because of dynamic nature and the attacks can either be active or passive. Active attacks may be in the form of packet tamper, packet deletion and packet replication. Passive attacks can be triggered by eavesdropping or silent listening, which affects the confidentiality. These attacks may completely shatter the entire network [8]. The best way to get rid of all these attacks is the deployment of an effective Intrusion Detection System (IDS) [7].

An IDS is vigilant against security attacks, or simply it monitors the behavior of nodes. IDS can only detect the attacks but cannot respond to it. Thus, the goal of an effective IDS is keeping an eagle-eye over the nodes and to detect the security threats.

The IDS can be deployed in two ways. The first way is deployment of IDS in every node or in the cluster head alone, which is the second option. This concept is depicted in Figure 1.

It is not feasible to deploy IDS to all nodes, because of the energy restriction of the mobile nodes. This problem can be handled by the second way of IDS deployment. In this case, the entire network is partitioned into several clusters, such that all the nodes of the network come under any of the cluster.

The constituent nodes of each cluster select a pre-eminent node. The IDS can be deployed in such pre-eminent nodes alone, such that these nodes can take care of the constituent nodes. Red coloured nodes in Figure 1(b) are the pre-eminent nodes and the other nodes are constituent nodes. The dotted circles represent the cluster.

In MANET, an IDS can take any one of the three different forms. They are stand- alone, cooperative or hierarchical [9]. The stand-alone form of IDS is executed in all the nodes and local response can be observed. The main pitfall of this architecture is the detection accuracy [6].

In the cooperative architecture of IDS, all nodes possess the local IDS but they share the data among themselves and work cooperatively [6]. Finally, in the hierarchical architecture of IDS, the network is broken into several clusters and a cluster head is chosen, based on a valid criterion. These cluster heads are more powerful than the normal

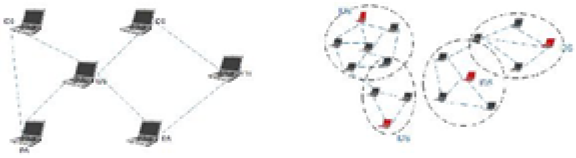


Figure 1: (a). Stand alone architecture of IDS, (b) Cluster based IDS

nodes [7]. The main merit of this architecture is the effective utilization of energy and the drawback is that this type of architecture is complex to adapt highly mobile MANETs [6].

In this work, we propose an IDS that is based on trust rates. The entire work of this system can be compartmentalized into three phases. They are

1) Pre-eminent node selection;

2) Inter-cluster trust rate computation;

3) Intra-cluster trust rate computation.

In the first phase of this work, a pre-eminent node is selected based on the trust rate.

The reason for the incorporation of the cluster based IDS is the effective utilization of energy, which is essential for dynamic MANET. The next phase of this work focuses on the inter- cluster trust rate computation. This is carried out by the Bayes Theorem. The next phase of the work is intra-cluster trust rate computation and this is done by the Dempster-Shafer theory.

This is followed by the summation of trust rates calculated by both the second and third phase of the system and this rate is termed as genuine trust. The outcome of this step yields a promising trust rate and the behavior of the node is predicted. The genuine trust is fed into the Ant-based clustering algorithm. This algorithm clusters the normal and the abnormal nodes separately and saves it for future reference. This list of abnormal nodes are notified to the pre-eminent node for proceed with further action.

The list of normal nodes is considered in routing by taking the path in which maximum normal nodes are present. This work is analysed with respect to routing and intrusion detection accuracy. The experimental outcome proves the efficiency of this work.

2 Proposed Work

In this work, we propose an IDS that is based on trust rates. The entire work of this system can be compartmentalized into three phases and are explained in this section. The assumptions of this work are every cluster knows its neighbor or nearby cluster and they enter a mutual agreement, such that two different clusters mutually calculate the trust rates of the constituent nodes.

To exemplify this concept, consider four different clusters A, B, C and D, where A is the immediate neighbor of C and the immediate neighbor cluster of B is D. In this case, there-eminent node of A and C enter into an agreement, so do the B and D. The trust rates of constituent nodes are computed mutually by A and C and the same process are carried out by B and D. This assumption is conceived by this work while computing the intra-cluster trust rate computation. The next assumption is that a trustworthy node remains trustworthy till the recovery process. A cluster can be established only with the one hop neighbors.

The entire work of this system can be compartmentalized into three phases. They are

1) Pre-eminent node selection;

2) Inter-cluster trust rate computation;

3) Intra-cluster trust rate computation.

In the first phase of this work, a pre-eminent node is selected based on the trust rate. The reason for the incorporation of the cluster based IDS is the effective utilization of energy, which is essential for dynamic MANET. The next phase of this work focuses on the inter- cluster trust rate computation. This is carried out by the Bayes? theorem. The next phase of the work is intra-cluster trust rate computation and this is done by the Dempster-Shafer Theory.

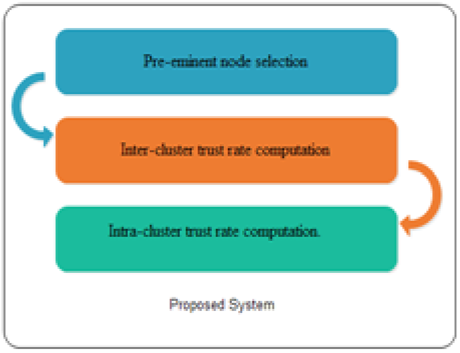

Pre-eminent node selection
Inter-cluster trust rate computation
Intra-cluster trust rate computation.
Proposed System

Figure 2: (Overflow of Proposed System

2.1 Cluster Establishment

In this work, we enforce a limit that every cluster can have the maximum of 7 nodes. This is to make the cluster to operate more effectively. After the deployment of nodes, if a cluster does not have maximum number of constituent nodes, it can send join_request to other nodes.

A node is chosen as the pre-eminent node among all the constituent nodes of the cluster. The pre-eminent node is chosen by taking the trust rate into account. A node with the highest trust rate in the cluster is chosen as the pre-eminent node. The trust rate is calculated by taking the packet delivery ratio and battery backup or energy into account.

Both the values range from 0 to 1 and a preferable value is set for both these parameters. The preferable value for packet delivery ratio and battery backup is 0.7 and 0.7 respectively. The threshold is fixed as 1.4. If a node's trust rate is greater than the fixed threshold, then that node is preferably the pre-eminent node. The trust rate of a node can be computed by the following.

$$Tr_{rate} = pdr + b_b \tag{1}$$

where pdr is the packet delivery ratio and b_b is the battery backup.

The packet delivery ratio can be computed by considering the in and out ratio of the forwarding history evidences. In normal case, in-ratio must be equal to the out-ratio. If the in-ratio is twice the out ratio, then the degree of selfishness will be 0.5. If the out- ratio is zero, then the node is considered to be completely selfish or it could be because of energy drop out.

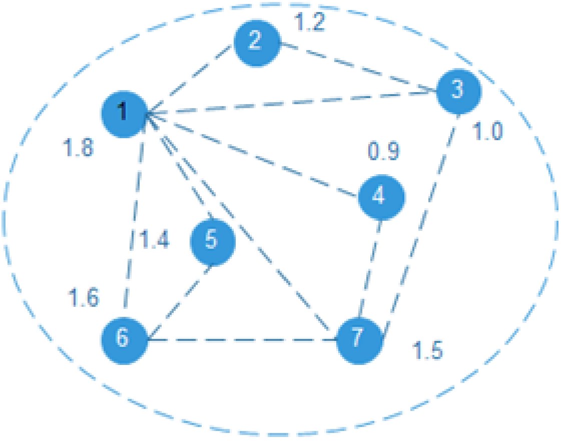


Figure 3: A Pre-eminent node selection

Let γ be the in-ratio of packets and μ be the out-ratio of the packets. If $\gamma = \mu$, then the node is trustworthy, that is, it forwards all the received packets and actively participates in the network. This type of node renders its fullest cooperation to the network.

If $\gamma = \mu/2$, then the node is partially trustworthy. This type of node will forward the packets sometimes and not always. The behavior of such nodes varies with respect to time. If the value of $\mu = 0$, then the node is malicious and it may affect the entire network.

It can be noted from Figure 3 that the node with the highest trust value is chosen as the pre-eminent node. The trust value is computed by Equation (1) and the details are tabulated in Table 3.

Table 1: Sample Trust Value Table

Degree	In-Out Ratio	Description
1	$\gamma = \mu$	Trustworthy Node
2	$\gamma = \mu/2$	Partially Trustworthy Node
3	$\mu = 0$	Malicious Node

Table 2: Energy Value Table

Case	Energy value	Description
1	1	Full energized node
2	0.75	Pretty good energy
3	0.5	Half energized node
4	0.25	Poor energized node
5	0	Energy drained node

Table 3: Detecting the nature of node

Node ID	PDR	Battery Backup	Scenario	Status of the Node
Node 1	0.9	0.9	$1.8 > 1.4$	Trustworthy
Node 2	0.9	0.3	$1.2 < 1.4$	Untrustworthy
Node 3	0.3	0.7	$1.0 < 1.4$	Untrustworthy
Node 4	0.4	0.5	$0.9 < 1.4$	Untrustworthy
Node 5	0.7	0.7	$1.4 = 1.4$	Trustworthy
Node 6	0.8	0.8	$1.6 > 1.4$	Trustworthy
Node 7	0.7	0.8	$1.5 > 1.4$	Trustworthy

In this case, if the same node is retained as the pre-eminent node for a long time, then the battery back-up will deteriorate soon. By considering the dynamic nature of MANET and the aforementioned point, the cluster is re-established for every five seconds.

2.2 Inter-cluster Trust Rate Computation

The inter-cluster trust rate computation is carried out by Bayes' therorem. Bayes' theorem was proposed by Rev. Thomas Bayes, in the year 1763 [5]. The inter-cluster trust rate is computed by clubbing both the packet delivery ratio and battery backup together. The total trust is given by Equation (2):

$$P(tr|pdr, b_b) = \frac{P(pdr|tr, b_b) \times P(tr|b_b)}{P(pdr|b_b)} \tag{2}$$

In Equation (2), $P(tr|pdr, b_b)$ is the posterior probability. $P(pdr|tr, b_b)$ is the prior probability. $P(tr|b_b)$ is called as the likelihood and it provides the probability of trust rate for the battery backup. $P(pdr|b_b)$ is the normalizing factor.

Algorithm 1: Algorithm for pre-eminent node selection

```
Input: Set of nodes
Output: Clusters
Begin
$cn_{th} = 7$;
For every 5 seconds
Randomly select a node;
Draw a circle that encloses 7 nodes;
if ($cn < 7$)
Broadcast join request;
For every $cn$ of a cluster
Do
Compute $Tr_{rate} = pdr + b_b$;
Find the ID of node with greatest $Tr_{rate}$
Declare it as pre-eminent node
End
```

The likelihood function of $P(pdr|tr, b_b) = P(pdr|tr)$. The probability of trust rate is given by

$$P(tr|pdr, b_b) = \frac{P(pdr|tr) \times P(tr|b_b)}{P(pdr|b_b)} \tag{3}$$

$P(pdr|tr)$ is calculated by Bayes' theorem and is given below.

$$P(pdr|tr) = \frac{P(tr|pdr) \times P(pdr)}{P(tr)} \tag{4}$$

Equation (4) is applied in Equation (3) and is presented in Equation (5).

$$P(tr|pdr, b_b) = \frac{P(tr|pdr) \times P(tr|b_b) \times P(pdr)}{P(pdr|b_b) \times P(tr)} \tag{5}$$

The normalizing factor is eliminated and the resultant equation is provided below.

$$P(tr|pdr, b_b) = P(tr|pdr) \times P(tr|P(tr|b_b). \tag{6}$$

The maximum trust value that can be obtained by this Bayes' theorem is 1. If the node's in-ratio is equal to the out-ratio of packets and if the node is fully energized, then the trust rate is 1. Trust rate may turn to 0 if the packet delivery ratio and the battery backup is not up to the mark.

This trust rate is calculated by the pre-eminent node for all its constituent nodes and is stored in the local table of every constituent node. This way of trust rate computation serves well.

2.3 Intra-cluster Trust Rate Computation

The intra cluster trust rate computation is done by the Dempster-Shafer theory. The assumptions of this phase are every cluster knows its neighbor or nearby cluster and they enter a mutual agreement, such that two different clusters mutually calculate the trust rates of the constituent nodes.

To exemplify this concept, consider four different clusters A, B, C and D, where A is the immediate neighbor of C and the immediate neighbor cluster of B is D. In this case, the pre-eminent node of A and C enter into an agreement, so do the B and D. The trust rates of constituent nodes are computed mutually by A and C and the same process are carried out by B and D. This assumption is conceived by this work while computing the intra-cluster trust rate computation.

Dempster-Shafer theory is introduced by Arthur P. Dempster [2]. This theory is also known as evidence theory. Dempster-Shafer theory is impressive because of the feature that it requires no prior knowledge of the probabilistic methodology, as in Bayes' theorem.

In this phase, we combine the trust rate computed by the corresponding pre-eminent node and the mutually agreed pre-eminent node, in order to arrive at a genuine trust rate. This can be given by the following.

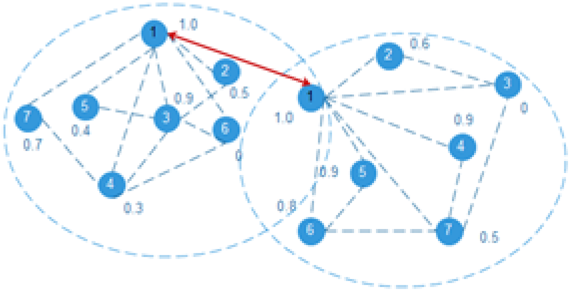


Figure 4: Intra-cluster trust computation

A node can either be trustworthy or untrustworthy and there is special case in which the node is either trustworthy or untrustworthy [?]. This can be written as

$$x : \Omega = \{T, \bar{T}\}. \tag{7}$$

T represents that the node x is trustworthy and $\bar{T}$ indicates that the node is untrustworthy. This could be explained more by the hypothesis, as shown below.

$$\begin{aligned} H &= \{T\} && (8)\\ \bar{H} &= \bar{T} && (9)\\ U &= \Omega && (10) \end{aligned}$$

In Equation (8), the equation represents that the node is trustworthy. The node is untrustworthy and is given in Equation (9). Equation (10) indicates that the node is either trustworthy or untrustworthy. Suppose, the probability of trustworthiness of a node is given by μ, then

$$\begin{cases} S1(H) & = \mu \\ S1(\bar{H}) & = 0 \\ S1(U) & = 1 - \mu \end{cases} \tag{11}$$

The probability function of un-trustworthiness of a node is given by Equation (12).

$$\begin{cases} S1(H) & = 0 \\ S1(\bar{H}) & = \mu \\ S1(U) & = 1 - \mu \end{cases} \tag{12}$$

In the next step, we combine the trust rate computed by the native pre-eminent node of a cluster along with the trust rate computed by the mutually agreed pre-eminent node. In this case, there is no need to check for the trustworthiness of pre-eminent node, as the node with highest trust rate is selected as the pre-eminent node, with faster recycling. The decisions made are combined and is provided below. There are three possible cases.

Case 1.

This is the case in which both the computations show that the node is trustworthy and it is given by

$$S1(H) \oplus S2(H) \frac{1}{w}[S1(H)S2(H) + S1(H)S2(U) + S1(U)S2(H)]. \tag{13}$$

Case 2.

This is the case in which both the computations show that the node is untrustworthy and it can be written as

$$S1(\bar{H}) \oplus S2(\bar{H}) \frac{1}{w}[S1(\bar{H})S2(\bar{H}) + S1(\bar{H})S2(U) + S1(U)S2(\bar{H})]. \tag{14}$$

Case 3.

In this case the node can either be trustworthy or untrustworthy and it is represented as

$$S1(U) \oplus S2(U) = \frac{1}{w} S1(U)S2(U). \tag{15}$$

w in Equations (13)-(15) can be given by

$$\begin{aligned} w &= S1(H)S2(H) + S1(H)S2(U) + S1(U)S2(H) + S1(\bar{H})S2(\bar{H}) + S1(\bar{H})S2(U) \\ &\quad + S1(U)S2(\bar{H}) + S1(U)S2(U). \end{aligned} \tag{16}$$

The genuine trust rate falls between 0 and 1. If the node's trust rate is 1, then the node is completely trustworthy. In case, if the node's trust rate is 0.5, then the node is either trustworthy or untrustworthy and the final case is that if the node's trust rate is 0, then it indicates the fact that the node is untrustworthy. Accurate trust rates are obtained on combining the resultant trust rates of inter and intra cluster.

The trust rates obtained for all the nodes are fed into the Ant based clustering algorithm and is explained in the next section.

2.4 Ant Based Clustering Algorithm

Ant based clustering algorithm is known for its efficiency. In this work, the genuine trust rates obtained from the previous phase are fed as input. The trust rates are dispersed in the grid and the ant randomly chooses a trust rate. The ant moves over the grid and the trust rate is probabilistically placed only when the probability range is higher than the probability of trust rate placement. This process continues until all the trust rates are placed perfectly in cluster.

Algorithm 2: Ant based clustering algorithm

```
Input: Genuine trust rates
Output: Clustered outcome of trustworthy and untrustworthy nodes
Distribute genuine trust rates (gtr) in grid
Each ant chooses a gtr and place randomly in grid
Select each ant randomly and it moves randomly over grid
Ant probabilistically drops gtr over grid
Continue this process until all gtrs are placed in grid
End process
```

Table 4: Sample Cluster Data

Trustworthy Nodes	Untrustworthy Nodes	Either Trustworthy or Untrustworthy Nodes
A1, A3, A7	A4, A6	A2, A5
B1, B4, B5, B6	B3	B2, B7

The outcome of this algorithm is a list of trustworthy, untrustworthy and nodes that are either trustworthy or untrustworthy. The list of untrustworthy nodes is forwarded to the pre-eminent node and it handles the problem. While routing, the path with maximum number of trustworthy nodes alone is chosen, such that the packet delivery ratio is terrifically improved.

2.5 Intrusion Detection

After the result update with the list of trustworthy, untrustworthy and nodes that are either trustworthy or untrustworthy, the pre-eminent node is responsible for handling such attacks. Handling the security breaches is out of the scope of this work. The detected report is submitted and then the intrusion is handled by the recovery process.

This work effectively makes use of the trust rate and the objective of the system is achieved. Clustering of trustworthy, untrustworthy and nodes that are either trustworthy or untrustworthy is achieved by ant based clustering algorithm. A small concern of routing is considered, in which the path with maximum number of trustworthy nodes is chosen.

3 Experimental Analysis

The performance of this system is tested in two angles. Initially, we focus on routing. In this work, only a small concern of routing is considered. The path with several trustworthy nodes is chosen as the route for forwarding

Algorithm 3: Overall algorithm

```
// Pre-eminent node selection
Begin
$cn_{th} = 7$;
For every 5 seconds
Randomly select a node
Draw a circle that encloses 7 nodes
if ($cn < 7$)
Broadcast join request
For every cn of a cluster
Do
Compute $Tr_{rate} = pdr + b_b$
Find the ID of node with greatest $Tr_{rate}$
Declare it as pre-eminent node
End
//Inter-cluster trust rate computation
Pre-eminent node calculates trust rate for all constituent nodes
S1: $P(tr|pdr, b_b) = P(tr|pdr) \times P(tr|P(tr|b_b)$
// Intra-cluster trust rate computation
S2: Neighbor pre-eminent node calculates trust rate for all constituent nodes mutually (based on assumption)
Calculate genuine trust by combining S1 and S2
//Cluster trustworthy and untrustworthy nodes separately
Disperse genuine trust rates in the grid
Ant randomly chooses the trust rates and clusters them in the grid
Continue the process until all the genuine trusts are located
Send the report to the pre-eminent node
//Situation handling
Track the untrustworthy nodes and take necessary action
```

packets and the analysis is carried out based on speed variation and the number of nodes variation.

The routing aspect of this work is compared with TSR1, TSR2, TDSR and DSR [10]. TSR1 and TSR2 are proposed in the same work but TSR1 renders more attention towards control packets and TSR2 pays more attention on data packets. The performance metrics considered are packet delivery ratio, end to end delay, and throughput.

3.1 Experimental Setup

The network size of our system is chosen as $1000 \times 1000m^2$. Wireless bandwidth is the data rate of the connection and is measured by bits/second. In our proposed system, the wireless bandwidth is 2 MB/Sec. The transmission range of the mobile node is fixed as 100 meters. In wired networks, the destination node can receive the packet from the source, only if the destination node is in the transmission range of the source node. In case, if the destination node is not within the transmission range of the source node, then the packet is transmitted via some intermediate node. In our case, the mobile nodes act both as a node and a router.

The random waypoint mobility model is exploited in this work and it makes sense that a mobile node remains in a location for a certain period of time, which is termed as 'pause'. After the time gets expired, the mobile node starts to choose a destination and the speed. Then, the node traverse towards the destination node at the chosen speed and again it will get paused. The maximum speed of the node of this work is 10m/sec. The node pause time is set as 20 seconds.

We have employed NS-2 for simulation. Un-slotted carrier-sense multiple access protocol is employed and it avoids collision [4] for packet transmission. We distribute 30 nodes in a 1000 by 1000 meter. The transmission radius of all nodes for a hop is given as 250 meters.

3.2 Performance Analysis

Performance metrics such as Packet delivery ratio, end-to-end delay and throughput, are employed to evaluate the performance of our algorithm and the graphs of these performance metrics are presented from Figure 2 - Figure 7. The proposed work is compared with the existing works such as DSR, TDSR, TSR1 and TSR2. Among these works,

Table 5: Simulation Parameters

Simulation Parameters	Value
Simulation Time	250 sec
Dimension	$1000m \times 1000m$
Node count	35
Mobility Model	Random waypoint
Traffic Nature	Constant Bit Rate
Transmission Radius	250 m

TSR1 and FTDSR2 are proposed in the same work but with different characteristic features. TSR1 pays more attention towards control packets and FTDSR2 focuses on data packets. On result analysis, it is proved that control packets are more important than data packets in MANET.

The performance of the system is analysed in two different aspects. The first aspect of analysis focuses on routing and the second aspect of analysis concentrates on intrusion detection. We have conducted two different tests for routing by varying the speed and nodes.

Packet Delivery Ratio (PDR). PDR is the ratio of packets that are successfully sent to the destination node from the source node and are computed by Equation (17) and the results are presented in Figure 1.

$$PDR = \frac{\sum Number - of - Packets - Received)}{\sum Number - of - packets - sent} \times 100. \tag{17}$$

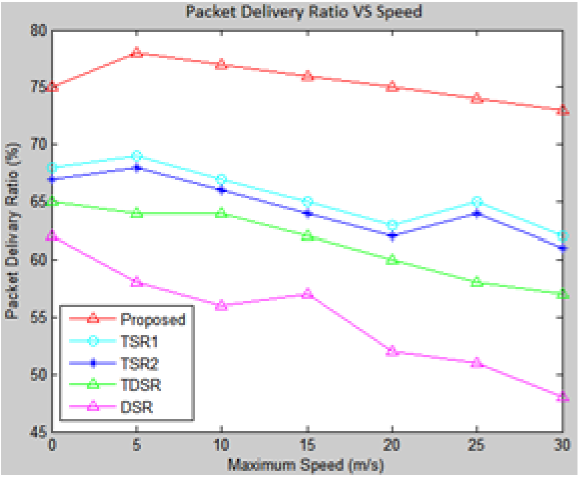


Figure 5: Packet delivery analysis vs. speed

Our system shows 75% packet delivery ratio with respect to speed and 80% packet delivery ratio with respect to number of nodes.

Average Latency (A_{ly}). The average time taken by the packets to reach the destination node from the source node and is calculated by

$$A_{ly} = \frac{\sum(Arrival\_Time - Sent\_Time)}{\sum Number\_of\_Connections} \tag{18}$$

Our proposed scheme proves least average latency and outperforms all the protocols. The end-to-end delay of our system starts from 16 seconds with respect to speed and 0.01 seconds with respect to node count.

Throughput. The amount of data transmitted per unit time and it is calculated by

$$Throughput = \frac{Size\_of\_the\_Packets(bits)}{Time\_Taken(sec)} \tag{19}$$

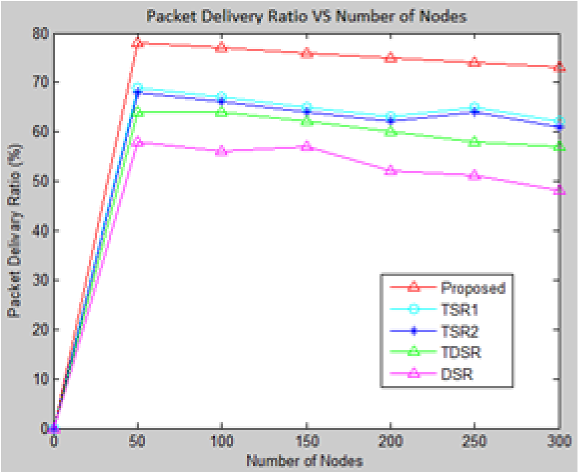


Figure 6: Packet delivery analysis vs. node count

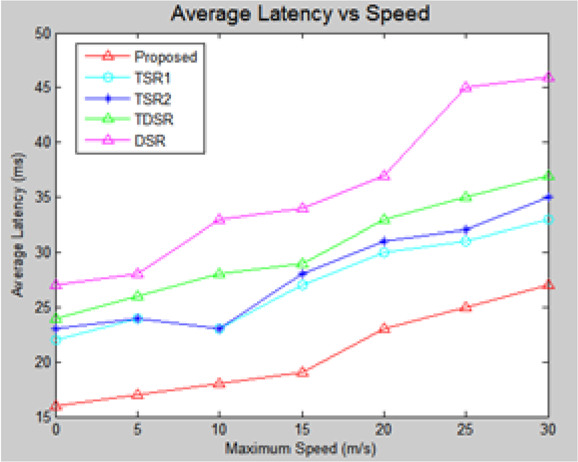


Figure 7: Average latency vs. speed analysis

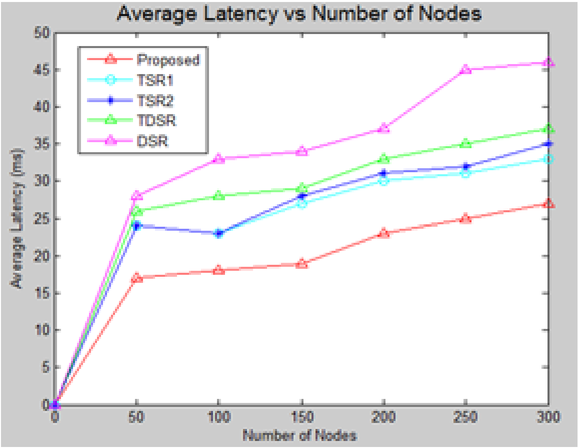


Figure 8: Average latency analysis vs. node count

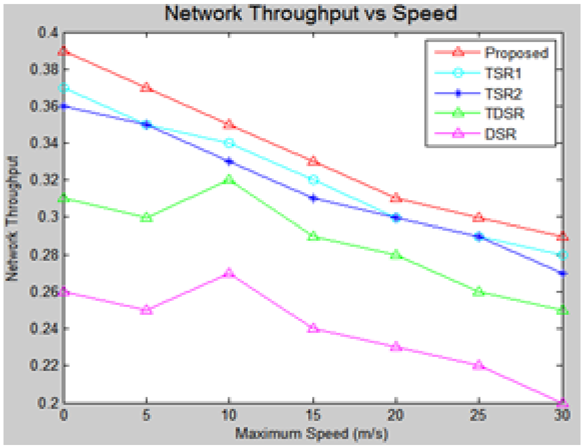


Figure 9: Throughput analysis vs. speed

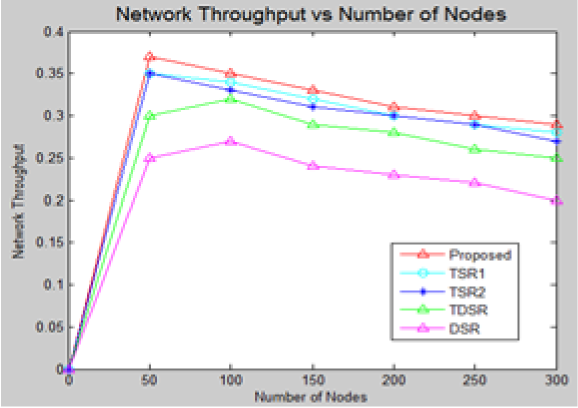


Figure 10: Throughput analysis vs. node count

Throughput is directly proportional to the packet delivery ratio and thus the throughput of the proposed work is higher than the existing works. The proposed work can transmit 0.39 packets per second with respect to speed and 0.37 packets per second with respect to node count.

Intrusion Detection Accuracy. It is the accuracy rate of intrusion detection and it can be calculated by

$$Intrusion\_detection\_accuracy = \frac{Number\_of\_correct\_detection\_of\_intrusion}{Number\_of\_intrusions\_detected} \tag{20}$$

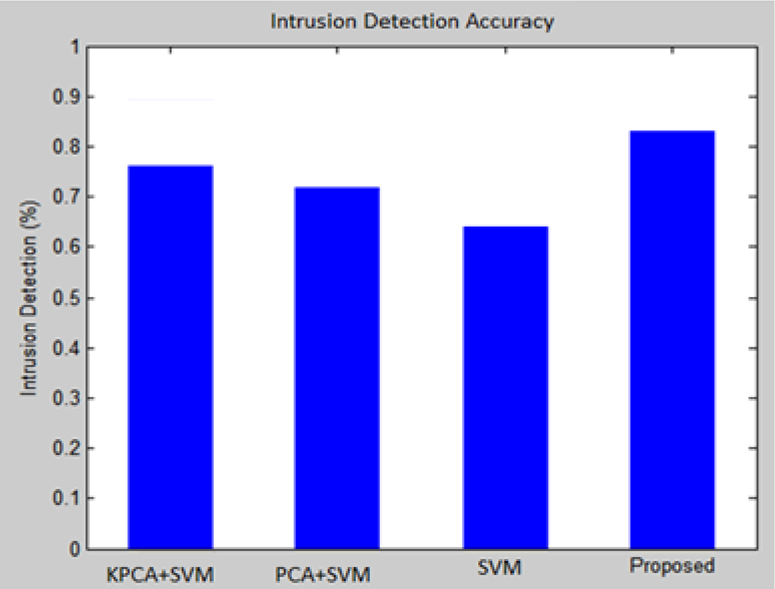


Figure 11: Intrusion detection accuracy

Intrusion detection accuracy of the proposed work is compared with the system that employs $KPCA+SVM$, $PCA+SVM$ and SVM alone. The detection accuracy of our system is 94.3% and is better than the compared systems.

Intrusion Error Rate. It is the wrong detection of intrusion out of the total intrusions detected and it can be calculated by

$$Intrusion\_detection\_accuracy = \frac{Number\_of\_wrong\_detection\_of\_intrusion}{Number\_of\_intrusions\_detected} \tag{21}$$

Intrusion error rate of our system is much lesser than the existing works such as $KPCA+SVM$, $PCA+SVM$ and SVM alone. The error rate of the proposed system is 5%, and is tolerable to some extent.

From the experimental results, it is evident that the intrusion detection system works well with lesser error rate.

4 Conclusion

In this work, we propose an IDS that is based on trust rates. The entire work of this system is compartmentalized into three phases and they are Pre-eminent node selection, Inter-cluster trust rate computation, Intra-cluster trust rate computation. Inter-cluster trust rate is computed by Bayes? theorem and the intra-cluster trust rate is calculated by the Dempster-Shafer theory. The computed genuine trust is fed into the ant based clustering algorithm. Finally, the proposed work is analysed in terms of routing and intrusion detecting potential. The system shows better accuracy rates for intrusion detection with minimum error rate. Trust rates are computed in two different ways and then, the computed trust rates are combined. This combined trust rate is named as the genuine trust rate and is fed into Ant based clustering algorithm. In future, the problem of computation overhead can be addressed.

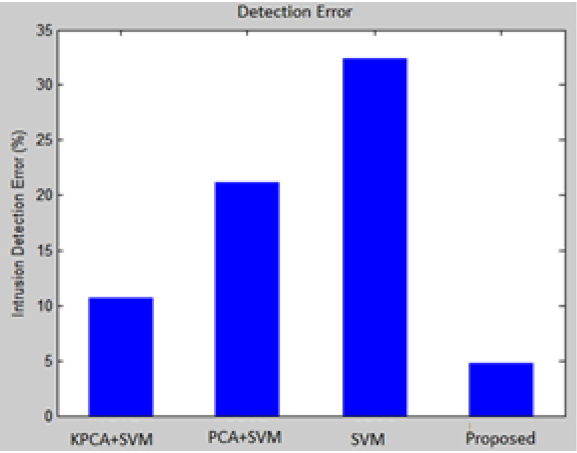


Figure 12: Detection error rate

References

[1] T. M. Chen and V. Venkataramanan, "Dempster-safer theory for intrusion detection in ad hoc networks", *IEEE Internet Computing*, vol. 9, pp. 35–41, 2005.

[2] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping", *The Annals of Mathematical Statistics*, vol. 38, no. 2, pp. 325–339, 1967.

[3] G. G. Deverajan, R. Saravanan, "Selfish node detection based on evidence by trust authority and selfish replica allocation in MANET", *International Journal of Information and Communication Technology*, 2014.

[4] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[5] J. Grover, "An Introduction to Bayes' theorem and Bayesian belief networks (BBN)", *Strategic Economic Decision-Making*, vol. 9, pp 1–9, 2013.

[6] S. Mutlu, G. Yilmaz, "Distributed cooperative trust based i ntrusion detection framework for MANETs", in *The Seventh International Conference on Networking and Services*, pp. 292–298, 2011.

[7] C. Panos, C. Xenakis, I. S. Stavrakakis, "A novel intrusion detection system for MANETS", *International Conference on Security and Cryptography*, pp.1-10, 2010.

[8] R. Sharman, S. Sharma, "Performance analysis of intrusion detection in MANET", *Computer Technology and Applications*, vol. 2, pp. 456–462, 2011.

[9] R. Shrestha, K. H. Han, D. Y. Choi, S. Jo Han, "A novel cross layer intrusion detection system in MANET", in *24th IEEE Conference on Advanced Information Networking and Applications*, pp. 647–654, 2010.

[10] Bo Wang, X. Chen, W. Chang, "A light-weight trust-based QoS routing algorithm for ad hoc networks", *Pervasive and Mobile Computing*, vol. 13, pp. 164–180, 2014.

[11] X. Wang, "An intrusion detection model based on ant principle", in *International Forum on Information Technology and Applications*, pp. 362–366, 2010.

Deverajan Ganesh Gopal working as Associate Professor in School of Computing Science and Engineering. He is an active researcher. He is a PhD student working under the supervision of Dr. R. Saravanan. His research areas include wireless networks, network security and cloud computing.

R. Saravanan completed his doctoral thesis in the area of Approximation Algorithms in 1997 at the Ramanujan Institute for Advanced Study in Mathematics and obtained the Ph.D degree from University of Madras. He obtained M.E in the branch of Computer Science and Engineering at the College of Engineering, Guindy, Anna University, Chennai. He has about two decades of teaching and research experience. He has rich research experience in areas of algorithms and published more than seventy five research papers. His areas of research include approximation algorithms, mobile computing, cryptography, and network security. He is a life member of Computer Society of India, Cryptology Research Society of India and Ramanujan Mathematical Society and also he is a member of IEEE. He served as a director during Aug 2010 - Jan 2013 and also as a dean during Feb 2013 - Jan 2014 at VIT University.

Taxonomy on Security Attacks on Self Configurable Networks

Noor Mohd[1], Singh Annapurna[2], H. S. Bhadauria[2]
(Corresponding author: Noor Mohd)

Govind Ballabh Pant Engineering College, Pauri Garhwal, Uttarakhand, India[1]
Department of Computer Science and Engineering, Govind Ballabh Pant Engineering College[2]
Pauri Garhwal, Uttarakhand, India[2]
(Email: decentnoor@rediffmail.com)

(Received Jan. 2, 2014; revised and accepted July 5 & Nov. 15, 2015)

Abstract

Designing an intrusion detection system for a mobile wireless system is technically a difficult task. Due to more mobile computing devices are coming into existence, in variable size, capabilities, mode of interaction, and so on. One day mobile devices and its applications are omnipresent in the world. Mobile devices are using wireless technologies like Bluetooth, Infrared, Wibree, Zigbee, 802.11, IrDA, WiMax (802.16), Wireless Sensor Network (802.15) or ultrasound. These devices are using different technologies but one thing is common to them is that they are cooperative in nature. And due to this nature and their sophisticated applications they are vulnerable to threats and attacks. In the recent years numerous new attacks are identified which are not present in the wired networks. And wired networks intrusion detection system is completely failed to fix. This paper discusses the security attacks and intrusion detection systems methodology for self configurable networks.

Keywords: Intrusion Detection System; Mobile Adhoc Networks; Self Configurable Networks; Wireless Networks; Wireless Sensor Networks.

1 Introduction

Security challenges emerge due to the ad hoc and dynamic nature of mobile ad hoc networks (MANET), in which devices do not know each other a priori, but still need to develop spontaneous interactions between themselves.

Adhoc networks nodes are free to move arbitrarily with different speeds [38]; thus, the network topology may change randomly and at unpredictable times. Some or all of the nodes in an ad hoc network may rely on batteries or other exhaustible means for their energy [19, 46]. For these nodes, the most important system design optimization criteria may be energy conservation. Wireless links continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communications - after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

There are many applications of MANETs. As a matter of fact, any day-to-day application such as electronic email and file transfer can be considered to be easily deployable within an ad hoc network environment. Web services are also possible in case any node in the network can serve as a gateway to the outside world [7]. In this discussion, we need not emphasize wide range of military applications possible with ad hoc networks. Not to mention, the technology was initially developed keeping in mind the military applications, such as battlefield in an unknown territory where an infrastructure network is almost impossible to establish or maintain. In such situations, the ad hoc networks having self-organizing capability can be effectively used where other technologies either fail or cannot be deployed effectively.

The advances on miniaturization techniques and wireless communications have made possible the creation and subsequent development of the Wireless Sensor Networks (WSN) paradigm [20, 36, 57]. The main purpose of WSN is to serve as an interface to the real world, providing physical information such as temperature, light, radiation, etc. to a computer system [13, 23, 34, 51]. The major difference between this type of networks and wired networks is their decentralized and specialized nature. In WSN, all its members collaborate towards the common goal of obtaining or deducing certain physical information from their environment. Moreover, WSN is capable of self-organization, thus it can be deployed in a certain context without requiring the existence of a supporting infrastructure.

The functionality and behavior of WSN are also different from another wireless network paradigm, Mobile Ad Hoc Network (MANET). First, all devices in WSN are totally autonomous, not controlled by human users. Also, those devices are much more constrained in terms of battery life and processing power, so it can only offer a simple and predefined set of tasks, whereas a MANET node is usually a PDA-like device with much more functionality and resources. In addition, the density of WSN is usually higher than in MANET.

The infrastructure of WSN can be divided into two parts, the data acquisition network and the data dissemination network [3, 16]. The data acquisition network contains the sensor network "per se": sensor nodes and base stations. Sensor nodes are a collection of small devices with the task of measuring the physical data of its surroundings, and base stations are powerful devices in charge of collecting data from the nodes and forwarding control information from the users [49, 58]. On the other hand, the data dissemination network is a combination of wired and wireless networks that provides an interface of the data acquisition network to any user.

In addition to those traditional security issues, we observe that many general-purpose sensor network techniques (particularly the early research) assumed that all nodes are cooperative and trustworthy. This is not the case for most, or much of, real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality [1, 44].

In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks. Furthermore, due to the inherent unattended feature of wireless sensor networks, we argue that physical attacks to sensors play an important role in the operation of wireless sensor networks [43].

The security of a network system can be provided with the help of intrusion prevention system and intrusion detection system [30, 40]. Both techniques need to complement each other to provide a highly secure environment [26]. They play different roles in different states of the network. Security mechanism (X.800) is provided by intrusion prevention system, and more useful in preventing outside attacks. When a node of a system is compromised, the attacker owns all its cryptographic information, so encryption and authentication cannot defend against a trusted but malicious user. Therefore, the role of intrusion detection is more important. And this is not an intelligent idea to load heavy applications on the tiny mobile devices for security. Proactive applications are consuming batteries on continuous basis but reactive security systems like intrusion detection system is a good solution for these kind of mobile systems, where cooperation is the primary goal.

Most of today's wired IDSs, which rely on real-time traffic parse, filter, format and analysis, usually monitor the traffic at switches, routers, and gateways. The lack of such traffic monitoring points makes traditional wired IDSs inadequate for infrastructure less wireless network platforms. There are also some characteristics of an infrastructure less wireless network such as dynamic topology, mobile/semi-mobile and immobile nodes, disconnected operations, problem of localization which seldom exist in the wired network.

2 Attack Model

Two kinds of threat models are discussed in infrastructure less wireless networks, one attack model is internal threat from trusted sources, and external threat models from outside the network by unauthorized nodes. External threats are very easy to be detected. Internal attacks are posed by the internal trusted node which is compromised by the attacker. And it is very difficult to distinguish between a regular or malicious communication. In this section we will discuss the generalized attack models whether it is internal or external threat on the basis of layered architecture for communication.

2.1 Attack Models in the MAC Layer

The attacks on the MAC layer are also known as an unfair use of a transmission channel. For the wireless networks it is purely based on the fair share of radio waves. But an intruder or malicious node can prevent other nodes in the network from getting transparent share of the channel. This activity can be considered as a denial of service (DoS) attack against the neighbors which are participating in a fair competition for allocation of transmission channels in a contention based network. Since the competing neighbors are deprived of their fair share of the transmission channel. Possible methods for unfair use of the transmission channel are as follows:

Ignoring the MAC Protocol.

Protocols like 802.11, uses request for transmission (RTS) and clear for transmission (CTS) mechanism to notify the neighbors that how long the transmission channel will be reserved by the node for successful transmission [18]. The availability of these protocols avoided the problem of collision [47] . But a misbehaving node can violate these protocols. Hence the competing neighbors are unable to get a fair share of channels [50]. This imposes a long delay at the output queues of the nodes and finally packets are timed out and get removed.

Network Partition.

Garbage can consist of packets of unknown formats, violating the proper sequence of a transaction (e.g. sending a data packet without exchanging RTS and CTS) or simply random bits used as static noise by misbehaving nodes [15, 52]. Garbage data may result in too many collisions and may consume a significant part of the available Channel capacity.

Malicious Flooding.

Deliver unusually large amount of data or control packets to whole network or some targeted nodes [8, 23, 39, 56]. We can distinguish two kinds of flooding attack. First one is the route request (RREQ) flooding attack. It ignores the network limitations for sending RREQ messages and sends a large number of RREQ packets with a maximum time to live (TTL) value addressing nodes that do not exist in the network.

The second is called data flooding attack. In this malicious node first sets up paths to all nodes in the network and then sends large volumes of useless data packets to all nodes along these paths, depleting in this way the available network bandwidth. Both attacks consume the available network resources and disallowing other nodes to communicate correctly.

Network Partition.

A connected network is partitioned into sub networks where nodes in different sub networks cannot communicate even though a route between them actually does exist [37, 54].

Sleep Derivation.

A node is forced to exhaust its battery power. It can be achieved by Denial of Service attack. Even it is not denial of service but sending the targeted node unnecessary request to process.

On-Off Attack.

A malicious node may alternatively behave well and badly to stay undetected while disrupting services [35]. Some time it acts as malicious and some time it acts as trusted node. So fooling the Intrusion detection system if present any in the network.

2.2 Attack Models in the Network Layer

The security threat on the network layer is called as anomaly in packet forwarding. Packet forwarding includes the data packets and control packets as well. This section is not considering the circuit switching based network because the research is based on wireless communication. This layer is the sophisticated and soft target of the attackers for both attack models internal and external threat. An anomaly in packet forwarding for different wireless network takes the different forms. Some attacks are specific to the specific architecture and most of them are generalized for all heterogeneous wireless environments.

Blackhole Attack/Sinkhole Attack.

In blackhole attack alias sinkhole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [4, 27, 41]. In this way attacker node will always have the availability in replying to the route request and thus attract the whole traffic on the network and intercept the data packet and further it may retain it or drop it.

Wormhole Attack.

A tunnel is created between two nodes that can be utilized to secretly transmit packets. Wormhole [9, 25, 39, 44] is a term adopted to describe an attack against the routing protocol in which two cooperating malicious nodes create a tunnel between two points of the network. The attack is possible even if none hosts were compromised and even attacked network introduced a strong authentication and encryption algorithms. This is the most difficult attack to trace it and counter it.

Byzantine Attack.

This attack is derived from Two Armies [1] problem of Byzantine valley. Two armies, each led by a general, are preparing to attack a fortified city. The armies are encamped near the city, each on its own hill. A valley separates the two hills, and the only way for the two generals to communicate is by sending messengers through the valley. Unfortunately, the valley is occupied by the city's defenders and there's a chance that any given messenger sent through the valley will be captured (this scenario assumes that while the two generals have agreed that they will attack, they haven't agreed upon a time for attack before taking up their positions on their respective hills).

[1] http://en.wikipedia.org/wiki/Army

The two generals must have their armies attack the city at the same time in order to succeed. They must thus communicate with each other to decide on a time to attack and to agree to attack at that time, and each general must know that the other general knows that they have agreed to the attack plan. Because acknowledgement of message receipt can be lost as easily as the original message, a potentially infinite series of messages are required to come to consensus.

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets [17, 48, 53] which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior.

The Sybil Attack.

In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network [27]. The incorrect information can be a variety of things, including the position of the nodes, signal strengths, making up nodes that do not exist.

Denial of Service Attack.

A node is prevented from receiving and sending data packets to its destinations. Attacker sends the unnecessary data packets to targeted node to void its main services.

In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A denial of service (DoS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate [32]. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the network protocol stack [21]. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel [10]. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service.

Rushing Attack.

This kind of attack is applied on reactive routing protocols. In this an attacker that can forward ROUTE REQUESTs more quickly than legitimate nodes can do so, can increase the probability that routes that include the attacker will be discovered rather than other valid routes [24, 28]. This is called as rushing to find out route in order to incorporate attack on the targeted node.

Packet Drop.

Packet drop is most common attack [5, 22, 45]. It is done not only individually but with the help of all kind of attacks including blackhole, denial of service and Sybil attack.

Delay in Packet Transmissions.

An attacker is doing unnecessary delay for transferring the packets to the destination to disrupt the Quality of Service [39].

Fabricated Route Messages.

Route messages with malicious contents are injected into the network [11]. Due to the cooperative nature of self configurable networks, this kind of attack is most dangerous and malicious contents are spreading throughout the networks via the trusted node and will destroy the complete network.

False Source Route

An incorrect route is advertised on the network, setting the route length to be the shortest, regardless where the destination is [31]. And vice a versa can also be applicable to forcefully adopt more vulnerable route.

Cache Poisonings.

Information stored in routing tables is modified, deleted or injected with false information [29]. Spreading this information and misguiding the whole network.

Selfishness.

A node is not serving as a relay node to other nodes [33]. It may be saving its battery for particular process to disrupt or probe the network.

2.3 Attack Models in the Transport Layer

The transport layer has very specific protocols including TCP, UDP and real time streaming protocols like SCTP and RSVP. But infrastructures less wireless networks are not designed to handle the real time streaming. Instead they use the service of UDP and TCP for data transfer. Though TCP has been extensively used for the wired network but is being used for mobile Adhoc network in the transport layer [42]. As there is no complementary protocol available for providing the connection oriented services in the infrastructure less wireless network. Though there is some principle difference in TCP for wired network and TCP for wireless network but basic functionality is same.

Session Hijacking.

Session hijacking is a critical error and gives an opportunity to the malicious node to behave as a legitimate system. All the communications are authenticated only at the beginning of session setup. The attacker may take the advantage of this and commit session hijacking attack. At first, he or she spoofs the IP address of target machine and determines the correct sequence number. After that he performs a DoS attack on the victim. As a result, the target system becomes unavailable for some time. The attacker now continues the session with the other system as a legitimate system.

Attacks using the TCP Segment Header.

1) Denial of Service Attack.
   There are various types of DoS attacks are possible. But for this chapter we consider the case of the TCP/IP header only.

2) Guest/Remote to Local (R2L) Login Attack (unauthorized access from a remote system).
   An attacker, who does not have rights of authentication on a targeted node, gains local access to extract files from the system, or modifies data in transit to the system.

3) Probing: Surveillance and Other Probing.

   a. Ping Sweep/IP Sweep.
      Ping (beacon signal) sweep is a technique used to identify which range of IP addresses map to live node. In this ICMP ECHO request are sent to multiple hosts. If a given address node is live, it will reply with an ICMP ECHO. A ping command is often used to verify that a network device/node is functioning or not.

   b. Port Sweep.
      Port sweep is a method to probe a server or host for open ports and not the working ports to launch the zombie attack.

   c. SYN Scan.
      SYN scan is another form of TCP scanning. The port scanner software generates raw IP packets, and then monitors the responses from the targeted node. This scan type is called as ”half-open handshaking”. Exactly, as it never opens a full TCP connection. The port scanner software generates a SYN packet. If the targeted node port is open, it will reply with a SYN-ACK packet. The scanner node will reply with a RST packet, and thus closing the connection before handshaking completed.

   d. SYN Scan with FIN.
      SYN scans are not surreptitious enough; firewalls are present in general (for the wired network). Scanning and blocking packets in the form of SYN packets are possible by the firewall. Then FIN bit ON packets are able to pass through firewalls without any modification. Closed ports from the targeted node will reply to a FIN packet with an appropriate RST packet, whereas open targeted ports will ignore the packets.

Attacks using UDP Header.

UDP Flood Attack: UDP is a connectionless protocol and it does not require any connection setup procedure to transfer data [14]. A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on the victim, the system will go down.

2.4 Attack Models in the Application Service Layer

The application layer is more vulnerable compared with other layers. Application layer holds the attraction of the attacker because all needed information is present in this layer. This layer holds the user data, and supports many protocols such as HTTP, SMTP, TELNET, and FTP. But for Adhoc network environment. Application protocol may be differing according to the nature of the node. So this layer in Adhoc network is called as MANET traffic generation layer and in wireless Sensor network it is called as service layer. There are various forms of attacks are available for this layer but the most common attack types are discussed below.

Masquerading.

A bogus registration is an active attack in which an attacker does a registration with a bogus care-of-address by masquerading itself as someone else [2]. By advertising fraudulent beacons, an attacker might be able to attract a MN (mobile node) to register with the attacker as if MN has reached HA (home agent) or FA (foreign agent). Now, the attacker can capture sensitive personal or network data for the purpose of accessing network and may disrupt the proper functioning of network. It is difficult for an attacker to implement such type of attack because the attacker must have detailed information about the agent.

Repudiation.

In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication [55]. Example of repudiation attack is a commercial system in which a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction Non-repudiation is one of the important requirements for a security protocol in any communication network.

Data Corruption/Modification.

It includes all kind of active attacks including data corruption and modification in original message [12].

Table 1: Attack models on different layers

Attack Models on Application Layer	Masquerading, Repudiation, Data Corruption/Modification	
Attack Models on Transport Layer	Attack Based on TCP segment Header	Session Hijacking, Denial of Service Attack, Probing
	Attacks Based on UDP Header	Flood Attacks
Network Layer Attack	Black hole attack/Sinkhole attack, Wormhole attack, Byzantine attack, The Sybil attack, Denial of Service Attack, Rushing Attack, Packet Drop, Delay in Packet Transmissions, Fabricated route messages, False Source Route, Cache Poisonings, Selfishness	
Attack Models on MAC layer Attacks	Ignoring the MAC protocol, Jamming the transmission channel with garbage, Malicious flooding, Network Partition, Sleep Derivation, On-Off Attack	

3 Conclusions

In this paper we discussed the possible attack models in each layer for self configurable networks. Self configurable networks include mobile Adhoc networks, Wireless Sensor networks, and Mesh networks. These self configurable networks are much popular among the researchers due their wide application in human life including monitoring, habitat monitoring, weather forecasting, earth quake forecasting, and future possible ecommerce applications. These networks are cooperative networks so they can be deceived by the intruders. So, discussion of possible attacks leads the direction of security and safety of these networks.

References

[1] A. E. Abbas, H. Shahnawaz, "Tumbling multilevel channel conflicts in mobile ad hoc networks", in *Proceedings of the 3rd IEEE International Advance Computing Conference (IACC'13)*, pp. 174–180, 2013.

[2] M. Aiash, A. Al-Nemrat, D. Preston, "Securing address registration in location/ID split protocol using ID-based cryptography", in *Proceedings of 11th International Conference on Wired/Wireless Internet Communication (WWIC'13)*, LNCS 7889, pp. 129–139, Springer, 2013.

[3] R. Alesii, F. Graziosi, S. Marchesani, C. Rinaldi, M. Santic, F. Tarquini, "Short range wireless solutions enabling ambient assisted living to support people affected by the Down syndrome", in *IEEE EuroCon'13*, pp. 340–346, 2013.

[4] A. Anzar, H. Shahnwaz, S. C. Gupta, "QoS by multiple cluster head gateway approach in mobile ad hoc network", in *Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC'11)*, pp. 174–176, 2011.

[5] S. Banerjee, M. Sardar, K. Majumder, "AODV based black-hole attack mitigation in MANET", in *Advances in Intelligent Systems and Computing*, pp. 345–352, 2014.

[6] M. Behzadi, R. Mahmod, M. Barati, A. B. H. Abdullah, M. Noura, "A new framework for classification of distributed denial of service (DDOS) attack in cloud computing by machine learning techniques", *Advanced Science Letters*, vol. 20, no. 1, pp. 175–178, 2014.

[7] C. Bouras, G. Gioumourtzis, A. Gkamas, V. Kapoulas, D. Politaki, E. Tsanai, "Evaluation of video transmission in emergency response ad hoc networks", in *International Conference on Data Communication Networking (DCNET'13)*, pp. 27–35, 2013.

[8] N. Chaisamran, T. Okuda, S. Yamaguchi, "Using a trust model to reduce false positives of sip flooding attack detection in IMS", in *Proceedings of International Computer Software and Applications Conference*, pp. 254–259, 2013.

[9] U. K. Chaurasia, V. Singh, "MAODV: Modified wormhole detection AODV protocol", in *6th International Conference on Contemporary Computing (IC3'13)*, pp. 239–243, 2013.

[10] E. Dondyk, L. Rivera, C. C. Zou, "Wi-Fi access denial of service attack to smartphones", in *International Journal of Security and Networks*, vol. 8, no. 3, pp. 117–129, 2013.

[11] M. Erritali, B. El Ouahidi, "A review and classification of various VANET intrusion detection systems", in *National Security Days*, pp. 1–6, 2013.

[12] D. Fiala, "Detection and correction of silent data corruption for large-scale high-performance computing", in *IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*, pp. 2069–2072, 2011.

[13] L. Fu, G. Zheng, J. Li, "Multi-track mobile data collection mechanism for wireless sensor networks", *Telkomnika*, vol. 12, no. 2, pp. 1424–1430, 2014.

[14] J. Gao, Y. Chen, "Detecting DOS/DDOS attacks under IPv6", in *Proceedings of the 2012 International Conference on Cybernetics and Informatics*, LNEE 163, pp. 847–855, Springer, 2013.

[15] A. Ghosal, S. D. Bit, "A jamming-attack-defending data forwarding scheme based on channel surfing in wireless sensor networks", *Security and Communication Networks*, vol. 6, no. 11, pp. 1367–1388, 2013.

[16] P. Giménez, B. Molina, J. Calvo-Gallego, M. Esteve, C. E. Palau, "I3WSN: Industrial intelligent wireless sensor networks for indoor environments", *Computers in Industry*, vol. 65, no. 1, pp. 187–199, 2014.

[17] N. K. Gupta, K. Pandey, "Trust based Ad-hoc on demand routing protocol for MANET", in *6th International Conference on Contemporary Computing (IC3'13)*, pp. 225–231, 2013.

[18] S. Hamrioui, M. Lalam, "Incidence of the improvement of the transport-MAC protocols interactions on MANET performance", in *Proceedings of the 8th ACM International Conference on New Technologies in Distributed Systems (NOTERE'08)*, pp. 15, 2008.

[19] C. C. Hsu, H. W. Yang, C. C. Yang, "An adaptive TTL-based AODV routing protocol for mobile Ad Hoc networks", *Journal of Applied Sciences*, vol. 13, no. 17, pp. 3579–3583, 2013.

[20] Y. Hu, Y. Ding, K. Hao, L. Ren, H. Han, "An immune orthogonal learning particle swarm optimization algorithm for routing recovery of wireless sensor networks with mobile sink", *International Journal of Systems Science*, vol. 45, no. 3, pp. 337–350, 2014.

[21] H. Jing, W. Wen, "Research on the detection and defense systems against DDoS attacks in ad hoc networks", *WIT Transactions on Information and Communication Technologies*, vol. 2, pp. 1161–1168, 2014.

[22] I. Khalil, S. Bagchi, N. Abuali, M. Hayajneh, "DISA: Detection and isolation of sneaky attackers in locally monitored multi-hop wireless networks", *Security and Communication Networks*, vol. 6, no. 12, pp. 1524–1538, 2013.

[23] I. M. Khalil, A. Khreishah, F. Ahmed, K. Shuaib, "Dependable wireless sensor networks for reliable and secure humanitarian relief applications", *Ad Hoc Networks*, vol. 13, pp. 94–106, 2014.

[24] H. Kim, R. De Oliveira, B. Bhargava, J. Song, "A novel robust routing scheme against rushing attacks in wireless ad hoc networks", *Wireless Personal Communications*, vol. 70, no. 4, pp. 1339–1351, 2013.

[25] L. Y. Luan, Y. F. Fu, P. Xiao, L. X. Peng, "Preventing wormhole attacks in wireless mesh networks", *Applied Mechanics and Materials*, vol. 443, pp. 440–445, 2014.

[26] H. M. Lugo-Cordero, R. K. Guha, "What defines an intruder? An intelligent approach", in *Proceedings of the 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS'13)* pp. 31–36, 2013.

[27] M. A. Mutaz, L. Malott, S. Chellappan, "Leveraging platoon dispersion for Sybil detection in vehicular networks", in *11th Annual Conference on Privacy, Security and Trust (PST'13)*, pp. 340–347, 2013.

[28] A. Nadeem, M. P. Howarth, "An intrusion detection & adaptive response mechanism for MANETs", *Ad Hoc Networks*, vol. 13 (PART B), pp. 368–380, 2014.

[29] S. Y. Nam, S. Djuraev, M. Park, "Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks", *Computer Networks*, vol. 57, no. 18, pp. 3866–3884, 2013.

[30] Q. Nasir, Z. A. Al-Mousa, "Honeypots aiding network forensics: Challenges and notions", *Journal of Communications*, vol. 8, no. 11, pp. 700–707, 2013.

[31] N. Naveen, A. Annalakshmi, K. R. Valluvan, "Trust node valuation and path reliability technique for intrusion detection in MANET", in *Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME'13)*, pp. 468–472, 2013.

[32] T. G. Ni, X. Q. Gu, H. Y. Wang, "Detecting DDoS attacks against DNS servers using time series analysis", in *Telkomnika*, vol. 12, no. 1, pp. 753–761, 2014.

[33] D. Pan, H. Zhang, W. Chen, K. Lu, "Transmission of multimedia contents in opportunistic networks with social selfish nodes", in *Multimedia Systems*, pp. 1–12, 2013.

[34] S. Peng, C. P. Low, "Prediction free energy neutral power management for energy harvesting wireless sensor nodes", *Ad Hoc Networks*, vol. 13, pp. 351—367, 2014.

[35] L. F. Perrone, S. C. Nelson, "A study of on-off attack models for wireless ad hoc networks", in *1st Workshop on Operator-Assisted (Wireless-Mesh) Community Networks (OpComm'06)*, pp. 1–10, 2006.

[36] M. V. Ramesh, "Design, development, and deployment of a wireless sensor network for detection of landslides", *Ad Hoc Networks*, vol. 13, pp. 2–18, 2014.

[37] S. Rangarajan, A. Bhan, P. Daoutidis, "Identification and analysis of synthesis routes in complex catalytic reaction networks for biomass upgrading", in *Applied Catalysis B: Environmental*, pp. 149–160, 2014.

[38] S. Sarkar, K. Majumder, "A survey on power aware routing protocols for mobile ad-hoc network", in *Advances in Intelligent Systems and Computing*, pp. 313–320, 2014.

[39] S. Sengan, S. C. Pandian, "Trustworthy position based routing to mitigate against the malicious attacks to signifies secured data packet using geographic routing protocol in MANET", *WSEAS Transactions on Communications*, vol. 12, no. 11, pp. 584–603, 2013.

[40] V. Serdiouk, "Technologies for protection against insider attacks on computer systems", *Communications in Computer and Information Science*, vol. 374 (PART II), pp. 75–84, 2013.

[41] H. Shahnawaz, S. C. Gupta, "Black hole attack in AODV & friend features1unique extraction to design detection engine for intrusion detection system in mobile adhoc network", *Journal of Engineering Science and Technology*, vol. 7, no. 5, pp. 623–634, 2012.

[42] H. Shahnawaz, S. C. Gupta, "Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network", *International Journal of Computer Science & Information Technology*, vol. 2, no. 4, pp. 1569–1573, 2011.

[43] H. Shahnawaz, S. C. Gupta, C. Mukesh, H. L. Mandoria, "A proposed model for intrusion detection system for mobile adhoc network", in *International Conference on Computer and Communication Technology (ICCCT'10)*, pp. 99–102, 2010.

[44] H. Shahnawaz, R. C. Joshi, S. C. Gupta, "Design of detection engine for wormhole attack in Adhoc network environment", *International Journal of Engineering and Technology*, vol. 4, no. 6, pp. 381–395, 2012.

[45] A. Sharma, S. Vashistha, "Improving the QOS in MANET by enhancing the routing technique of AOMDV protocol", in *Advances in Intelligent Systems and Computing*, pp. 381–392, 2014.

[46] N. Shirali, S. Jabbedari, "Topology control in the mobile ad hoc networks in order to intensify energy conservation", *Applied Mathematical Modelling*, vol. 37, no. 24, pp. 10107–10122, 2013.

[47] A. Stavrou, A. K. Ghosh, "A security architecture for information assurance and availability in MANETs", in *Proceedings of IEEE Military Communications Conference (MILCOM'08)*, pp. 1–8, 2008.

[48] H. Tian, X. Chen, B. Wei, Y. Liu, "Security analysis of a suite of deniable authentication protocols", *International Journal of Network Security*, vol. 15, no. 5, pp. 384–389, 2013.

[49] F. Tiegang, T. Guifa, H. Limin, "Deployment strategy of WSN based on minimizing cost per unit area", *Computer Communications*, vol. 38, no. 1, pp. 26–35, 2014.

[50] A. T. Toyserkani, E. G. Strom, A. Svensson, "An efficient broadcast MAC scheme for traffic safety applications in automotive networks", in *IEEE Wireless Communications and Networking Conference (WCNC'06)*, pp. 2100–2105, 2006.

[51] G. Tuna, V. C. Gungor, K. Gulez, "An autonomous wireless sensor network deployment system using mobile robots for human existence detection in case of disasters", *Ad Hoc Networks*, vol. 13, pp. 54–68, 2014.

[52] H. M. Wang, M. Luo, Q. Yin, X. G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks", *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2007–2020, 2013.

[53] J. Wang, J. Yao, Q. Wu, "Stealthy-attacker detection with a multidimensional feature vector for collaborative spectrum sensing", *IEEE Transactions on Vehicular Technology*, vol. 62, no. 8, pp. 3996–4009, 2013.

[54] J. Wellons, Y. Xue, "The robust joint solution for channel assignment and routing for wireless mesh networks with time partitioning", *Ad Hoc Networks*, vol. 13 (PART A), pp. 210–221, 2014.

[55] W. Wu, J. Zhou, Y. Xiang, L. Xu, "How to achieve non-repudiation of origin with privacy protection in cloud computing", *Journal of Computer and System Sciences*, vol. 79, no. 8, pp. 1200–1213, 2013.

[56] M. Yu, "An adaptive method for source-end detection of pulsing DoS attacks", *International Journal of Security and its Applications*, vol. 7, no. 5, pp. 279–288, 2013.

[57] W. Zeng, J. Cote, X. Chen, Y. A. Kim, W. Wei, K. Suh, B. Wang, Z. J. Shi, "Delay monitoring for wireless sensor networks: An architecture using air sniffers", *Ad Hoc Networks*, vol. 13, pp. 549–559, 2014.

[58] D. Zhou, F. Xu, L. Wu, S. S. Peng, "Formation of real-time wireless sensor network based on CC2530", in *Applied Mechanics and Materials*, pp. 1868–1871, 2013.

Noor Mohd received B. Tech degree in Computer Science & Engineering from HNB Garhwal University Srinagar Pauri ,Uttarakhand,India and M.Tech degree in Computer Science & Engineering from Uttarakhand Technical University,Dehradun, Uttarakhand, India. He is pursuing Ph.D. from Govind Ballabh Pant Engineering College Pauri ,Uttarakhand,India. His research interests are in security of Wireless Adhoc Networks, Sensor Networks, and Wireless Mesh Networks. He published various international research papers in reputed journals.

Annapurna Singh received M. Tech. (2003) from Banasthali Vidyapeeth, Banasthali, India; did her Ph.D. (2012) from Uttarakhand Technical University, Dehradun in Computer Science Engineering. From 2003 to till date she worked as lecturer in various Engineering Colleges of India and presently working as an Assistant Professor in Computer Science Engineering of G.B. Pant Engineering College, India.

H. S. Bhadauria received B. Tech. (1999) (Computer Science & Engineering), M. Tech. (2004) (Electronics Engineering) both from Aligarh Muslim University, Aligarh; did his Ph.D. (2013) from Indian Institute of Technology, Roorkee, India. He has published some 20 research papers in International and National Journals and Conferences. His areas of Interest are Digital Image and Digital Signal Processing.

Guide for Authors

International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:

For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.