International Journal of Information Technology and Management

Vol. VIII, Issue No. XII, May-2015, ISSN 2249-4510

ANALYSIS OF THE ISSUES OF WIRELESS AD HOC NETWORK STRATEGIES IN THE COMPUTER COMMUNICATION

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VIII, Issue No. XII, May-2015, ISSN 2249-4510

Analysis of the Issues of Wireless Ad Hoc Network Strategies in the Computer Communication

Dr. S. S. Riaz Ahamed[1] P. Senthil Selvi[2]

Abstract – An ad hoc mobile network is a compilation of mobile nodes that are energetically and arbitrarily located in such a way that the interconnections flanked by nodes are accomplished of changing on a frequent basis. The main goal of such an ad hoc network routing protocol is truthful and well-organized route organization between a pair of nodes so that communication may be delivered in a timely manner. In this paper we examine routing protocols for ad hoc networks and evaluate these protocols based on a given set of parameters.

Keywords: Ad Hoc Mobile Network, Protocol, Nodes.

----------X----------

INTRODUCTION

The advent of mobile devices such as smartphones and tablets has posed an unprecedented traffic demand on current mobile communications infrastructure. For instance, AT&T has reported that wireless data traffic has increased by 20,000% in just five years (2007-2012), and that an exponential traffic increase should be expected in the years to come [13]. Following similar reports, mobile operators have started to look for alternative solutions to alleviate the impact of the so-called “mobile data crunch” problem. As an immediate (and partial) solution to this problem, many operators are currently deploying their own WiFi networks to offload their core network infrastructure by encouraging their customers to switch to WiFi as much as possible. Given the importance and scale of the problem, data offloading has become an active area of research in the past few years [14-16].

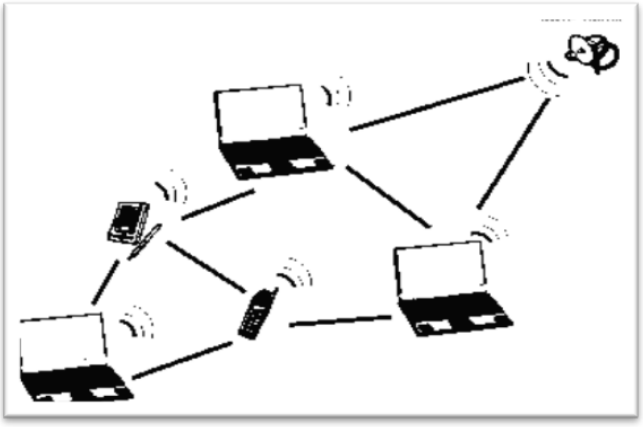
REVIEW OF LITERATURE:

Strategy-Proof Routing in Wireless Ad Hoc Networks [18]

Ad hoc networks (multi-hop wireless networks) are expected to revolutionize wireless communications in the next few years by complementing more traditional networking paradigms (Internet, cellular networks, satellite communications); they can be considered as the technological counterpart of the concept of 'ubiquitous computing'. However, in order for this scenario to become reality, several issues must be adequately addressed. One of these issues is how to stimulate cooperation among the network nodes. In fact, the nodes of an ad hoc network are usually owned by different authorities (private users, professionals, companies, and so on), and a voluntary and 'unselfish' participation of the nodes in the execution of a certain network-wide task cannot be taken for granted. Concepts borrowed from the theory of Mechanism Design can be used to tackle this problem. Mechanism Design is the branch of Game Theory that studies how to design protocols that stimulate players (in our case, network nodes) to behave 'unselfishly', cooperating to the achievement of a global goal. A distributed protocol with this feature is called strategy-proof [18].

One of the fundamental tasks any ad hoc network must perform is routing. Since the network is in general multi-hop, a routing protocol is needed in order to discover and maintain routes between far away nodes, allowing them to communicate along multi-hop paths. Unless carefully designed, routing protocols are doomed to perform poorly in presence of 'selfish' node behavior. In general, a network node has no interest in forwarding a packet on behalf of another node, since this action would only have the effect of consuming its resources (energy, and available bandwidth). Thus, if many of the nodes act selfishly (as may well be the case when nodes are owned by different authorities), only a few multi-hop communications will take place, and the network functionality is compromised. Thus, the definition of strategy-proof routing protocols for ad hoc networks is of fundamental importance [18].

In our research, which is a joint activity with Stephan Eidenbenz at Los Alamos National Labs, USA, we have developed and studied a protocol for strategy-proof route discovery and packet forwarding in ad hoc networks. In particular, we have considered a reference application scenario in which the network is used to provide a certain wireless service (eg, internet access). In principle, ad hoc networking could be used to increase the service coverage: instead of requiring each customer to be directly connected to the base station, customers could be allowed to reach the base station along multi-hop paths, using the wireless devices (laptop, PDA, and so on) of other customers as intermediate nodes (see Figure). This way, the area in which the service is available could be much larger than the radio coverage area of the base station.



A multi-hop wireless network for internet access. The base station provides internet access to the network nodes through multi-hop wireless paths (red lines).

Source from: [18]

In order to implement such an ad hoc network successfully, intermediate nodes must be motivated to act 'unselfishly', relaying packets on behalf of others. Typically, intermediate nodes receive compensation in the form of monetary payment for their "unselfish" behavior, which at least covers the cost that a node incurs by forwarding packets.

Our proposal is to use a protocol that implements a fully distributed, reverse, second-price single-item auction with reserve price. The basic idea is simple: when new customers want to access the service, they issue a 'connection request', stating the maximum amount that they are willing to pay (the reserve price). The connection request represents maximum commitment of the customer: if the connection actually takes place for less than the declared price, the customer only pays this amount. In this way, the customer has full control of the maximum amount of money that he will have to pay in order to send the packets. By using a second price auction mechanism (second-price auctions are necessary to ensure strategy-proofness), the minimum path to the destination is identified and, if the amount of money the sender should pay is below the reserve price, the transaction takes place.

After having formally investigated and proved that our protocol is strategy-proof, we are now working on its implementation and simulation. We are also investigating the overall economic efficiency and feasibility of our incentive-based system [18].

PHISHING ATTACKS AND THEIR POTENTIAL IMPACTS:

Phishing is a kind of social-engineering attack in which criminals use spoofed email messages to trick people into sharing sensitive information or installing malware on their computers. Victims perceive these messages as being associated with a trusted brand, while in reality they are only the work of con artists. Rather than directly target the systems people use, phishing attacks target the people using the systems. Phishing cleverly circumvents the vast majority of an organization's or individual's security measures. It doesn't matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish.

The word “phishing” originally comes from the analogy that early Internet criminals used email lures to “phish” for passwords and financial data from sea of Internet users. The use of “ph” in the terminology is partly lost in the annals of time, but most likely linked to popular hacker naming conventions such as “Phreaks” which traces back to early hackers who were involved in “phreaking” – the hacking of telephone systems.

Phishing has been classified into web-based phishing and exploit-based phishing [1]. All the attacks which exploit well-known vulnerabilities in popular web browsers to install malware on the victim’s machine come under exploit-based phishing. Visually deceptive phishing can be further classified into using deceptive text, or copying images in the URL [2, 3]. Users can be fooled by making fake websites with a very minor difference in the spelling of the domain name. For example, a difference between the letters “l” and “i” can escape the untrained eye, and “paypal.com”, and “paypai.com” can appear to be the same. Phishers also use non-printing characters and non- ASCII Unicode characters [4].

Rogue Access Points - A rogue access point is any Wi-Fi access point connected to a network that has been installed without authorization from network administrators, or has been planted by a malicious user to carry out phishing or a man-in-the-middle attack. Rogue Access Points (R.A.P.s) constitute arguably a big security threat to Wireless (Wi-Fi) networks today [6]. It is not under the management of network administrators and does not necessarily conform to network security policies. In [5], the

authors classify RAPs into 4 types: improperly configured, unauthorized, phishing and compromised. Our focus will be on phishing RAPs. The phishing scam that was reported on Gmail, Yahoo and AOL Email, 30,000 email log-in credentials from these websites were hacked and posted online. It was later removed, but some of the compromised emails had already sent spams. Users received an email from Yahoo telling them that Yahoo needed to verify their email account as it had been idle for a long time. In May 2009 there were reports of phishing attacks on Face book [7-12].

CONCLUSION:

There are manifold pre cautions previously in place such as web browsers taking preventative measures to blacklist compromised websites, although this can also present further concerns for genuine businesses who are also a victim of cyber fraud. There are a lot of pre-emptive events and precautions that organizations' can also put into practice to make sure their websites and networks remain protected. This has now become more vital than ever in ensuring that customer trust is not damaged.

REFERENCES:

1. Tyler Moore, "Cooperative attack and defense in distributed networks" Technical Report, UCAM-CL-TR-718, ISSN 1476-2986

2. Stajano, F. and Wilson, P. Understanding scam victims: Seven principles for systems security. *Commun. ACM 54*, 3 (Mar. 2011), 70–75.

3. Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. *Commun. ACM 50*, 10 (Oct. 2007), 94–100.

4. Hong, J. Why have there been so many security breaches recently? Blog@CACM

5. Moore, T. and Clayton, R. Examining the impact of Website take-down on phishing. In *Proceedings of the Anti-Phishing Working Group's Second Annual eCrime Researchers Summit* (Pittsburgh, Oct. 3–5, 2007), 1–13.

6. Dhamija, R., Tygar, J.D., and Hearst, M.A. Why phishing works. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Quebec, Apr. 24–27). ACM Press, New York, 2006, 581–590;

7. Cova, M., Kruegel, C., and Vigna, G. There is no free phish: An analysis of 'free' and live phishing kits. In *Proceedings of the Second USENIX Workshop on Offensive Technologies* (San Jose, CA, July 28, 2008). Usenix;

8. Krastev, N. U.S. indicts dozens from Eastern Europe in Internet theft scheme. *Radio Free Europe* (Oct. 1, 2010);

9. Sheng, S., Holbrook, M.B., Kumaraguru, P., Cranor, L.F., and Downs, J.S. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Atlanta, Apr. 10–15). ACM Press, New York, 2010, 373–382.

10. Litan, A. Phishing attack victim's likely targets for identity theft. Gartner Group, May 2004.

11. Herley, C. and Florencio, D. A Profitless endeavor: Phishing as a tragedy of the commons. In *Proceedings of the New Security Paradigms Workshop* (Lake Tahoe, CA, Sept. 22–25, 2008).

12. Fette, I., Sadeh, N., and Tomasic, A. Learning to detect phishing emails. In *Proceedings of the 16th International World Wide Web Conference* (Banff, Canada, May 8–12, 2007), 649–656.

13. "Mobile data traffic surpasses voice," http://www.cellular-news.com/story/42543.php.

14. B. Han, P. Hui, A. Kumar, M. Marathe, J. Shao, and A. Srinivasan, "Mobile data offloading through opportunistic communications and social participation," IEEE Trans. on Mobile Computing, vol. 11, no. 5, pp. 821–834, 2012.

15. G. Iosifidis, L. Gao, J. Huang, and L. Tassiulas, "An iterative double auction for mobile data offloading," in Proc. WiOpt, 2013, pp. 154–161.

16. X. Zhuo, W. Gao, G. Cao, and S. Hua, "An incentive framework for cellular traffic offloading," IEEE Trans. on Mobile Computing, vol. 13, no. 3, pp. 541–555, 2014.

17. S. Singh, H. Dhillon, and J. Andrews, "Offloading in heterogeneous networks: Modeling, analysis, and design insights," IEEE Trans. on Wireless Communications, vol. 12, no. 5, pp. 2484–2497, 2013.

18. http://www.ercim.eu/publication/Ercim_News /enw57/santi.html