

Minimising Cost of Lawful Interception in Mobile IP

Shahnaz Kouhbor and Philip Branch

Centre for Informatics and Applied Optimisation
University of Ballarat
Ballarat, Vic 3353
skouhbor@students.ballarat.edu.au

Centre for Advanced Internet Architectures
Swinburne University of Technology
Hawthorn, Vic 3122
pbranch@swin.edu.au

Abstract - Communications Interception is an essential part of law enforcement used by authorised government agencies to investigate criminal activities. With the growth of IP based applications and new IP technologies such as mobile IP, Internet Service Providers (ISPs) will find themselves increasingly obliged to provide interception capabilities. IP interception is usually done with expensive hardware based systems the cost of which ISPs would like to minimize. In this paper we propose the use of optimisation techniques to find the optimal location(s) of systems in the network needed to be installed while minimising the cost and ensuring complete coverage of the network.

Key words: Lawful Interception (LI), Communication Interception, Wiretapping, Mobile IP, Optimisation

I. INTRODUCTION

The European Telecommunications Standards Institute (ETSI) has described Lawful Interception (LI) as “action (based on law), performed by a network operator/access provider/service provider (NOW/AP/SvP), of making available certain information and providing that information to a law enforcement monitoring facility (LEMF)” [1]. Figure 1 shows the functional roles of Lawful Interception. The purpose of lawful interception is to investigate and prevent crime. The process of lawful interception begins with the interception and collection of various forms of communications, analysis of the intercepted data, and the preparation of evidence used to prosecute the offenders. Normally the interception equipment is placed at the point(s) of interest in the network to capture the traffic of targeted users. Internet interception is based on hardware sniffer systems that trap Internet traffic destined either to or from a party of interest to Law Enforcement Agencies. The optimal placement within the network of these sniffers is the topic of this paper.

Lawful Interception in circuit switched communications is well established. Standards have been written by ETSI and equipment for interception have been developed [2]. In Public Switched Telephone Networks (PSTN), the identity of the user of the telephone handset is easily

established and the route of communications traffic between parties to the communication is easy to determine and intercept. In the PSTN, the handset is physically connected to the local exchange, and all incoming and outgoing calls go through the local exchange. Hence, the local exchange is an obvious location for installing the interception equipment. Unfortunately, this is not the case with Internet based services. Internet services can be accessed in many ways such as through Cyber cafes, Internet kiosks, public libraries all of which are not obvious interception points. Consequently, ISP interception is becoming increasingly important to the Law Enforcement Agencies [3].

Because of the lack of standards and sophisticated equipment to lawfully intercept Internet communications, Internet Service Providers (ISPs) are facing many challenges related to Lawful Interception. This paper looks at the emerging service of Mobile IP and suggests how optimisation techniques can be used to minimise the cost of Lawful Interception compliance. The paper is organised as follows: In Section II, the operation of mobile IP is explained. In Section III, the challenges of lawful interception in mobile IP are described. Section IV describes how optimisation techniques can be used to minimise the cost of compliance of Lawful Interception obligations.

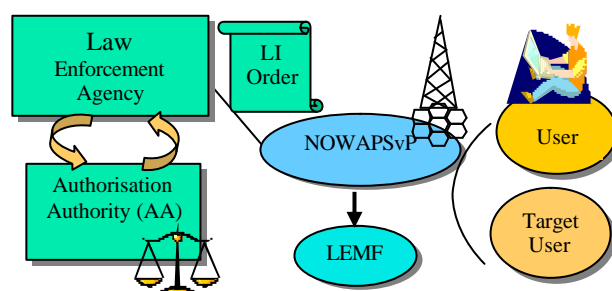


Figure 1: Functional roles of Lawful Interception

II. MOBILE IP

Mobile IP has been developed by the Internet Engineering Task Force (IETF) to enable mobile computer users to stay connected to the Internet and maintain communications as they move from one subnet to another

[4]. The requirement for such an activity is that a mobile node (MN) must continuously use its permanent IP address even as it roams to another area.

To maintain the requirement, MN uses two IP addresses: a fixed **home address** and a **care-of-address** that changes at each new point of attachment. Parties communicating with the MN are unaware of the care-of-address, and send all the data to the MN by its fixed home address. The MN registers its new care-of-address with its home agent as it moves about the network. Mobile IP introduces the following agents and nodes:

- Mobile Node (MN) – User that changes its point of attachment from one subnet to another
- Home Agent (HA) – Router on mobile node’s home network that is in contact with the mobile node. It receives and delivers datagrams to the mobile node through its care-of-address.
- Foreign Agent (FA) – Router on the subnet that the mobile node is visiting. It provides services to the mobile node by routing the datagrams received from the home agent to the mobile node.

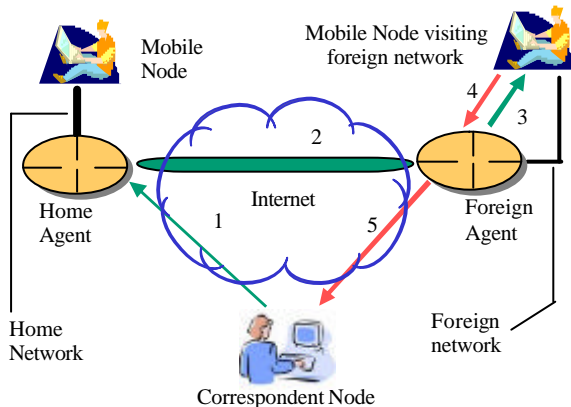


Figure 2: Mobile IP Components and Routing Procedures

The components of mobile IP and routing mechanism are shown in figure 2.

When MN moves from its home network to a foreign subnet (foreign agent), it obtains a care-of-address from that FA. Mobile node obtains this address by listening to the regular advertisement that both home agent and foreign agent make about their services. Then mobile node registers its care-of-address with its home agent through a foreign agent. If home agent accepts the request, it associates the home address of mobile node with its care-of-address, and maintains this association until the registration lifetime is expired. The home address, care-of-address and registration lifetime is called binding for mobile node. The home agent must perform authentication to be certain that registration was originated by mobile node and not any other malicious node.

After registration, the IP datagrams that are sent by the correspondent node for the mobile node are intercepted by the home agent (route 1). After that, the home agent puts the entire packet into an outer IP packet header and tunnels this packet to the mobile node’s care-of-address (route 2). The source address of this new packet is the home agent’s IP address, and the payload is the original IP packet. The foreign agent strips off the outer IP header, and encapsulates the original IP datagram with the mobile node’s new address (care-of address) and delivers it to mobile node (route 3), which is located in the foreign network. IP datagrams from the mobile node to the correspondent node travel directly through the foreign agent and without encapsulation (route 4, 5), as the correspondent node uses a fixed address.

A. Difficulties for LI Associated with Mobile IP

As the mobile node moves around the network, it obtains a care-of-address from each of the foreign agents. Hence, identifying the user for interception purposes is difficult. Another problem associated with mobile IP is related to the pattern of movement of the mobile users around the network. This movement in different parts of the city throughout the day can identify the workload for sniffers used in interception. The size of subnet (broadcast domain) is another issue in mobile IP. The size can identify the number of sniffers that are required to be installed. Reduction of the subnet size can have an effect on security of the network and bandwidth available to mobile users. Although it is very difficult to estimate the pattern of movement of users and the size of subnet, we are planning to use optimisation techniques to find the optimal location(s) of sniffers while minimising the cost and ensuring complete coverage of the network.

III. CHALLENGES OF LI IN MOBILE IP

Until very recently, all Lawful Interception was carried out in the public access network. However, for reasons noted earlier, this is no longer satisfactory.

Mobile IP compounds these difficulties as the user may be using services anywhere. Therefore, there is a need to determine the presence, identity, and location of callers prior to tapping. Loss of packets due to routing mechanism in mobile IP make the process of LI even more challenging. It must also be noted that due to global nature of wireless communications, the jurisdictional problems in criminal and terrorist investigation can be created [5].

The ISPs are obliged to provide facilities for interception on their systems [6]. Due to the difficulty of Internet interception and lack of standards and equipment, ISPs have been forced to use the hardware sniffer systems for interception at present. Due to the high cost of sniffer systems, this is likely to be a significant financial burden on ISPs. Smaller ISPs, especially those in regional and rural areas might find it impossible to comply with government’s Lawful Interception requirements or they

might not be able to offer all services to users. It is estimated that the cost of interception for ISPs in Europe can be from 100,000 Euro to 700,000,000 Euro and penalties for non-compliance will be fines up to 250,000 Euros, civil charges, and house arrest for the CEO of the ISP [7].

IV. OPTIMISATION TECHNIQUES FOR LI IN MOBILE IP (FUTURE INVESTIGATION)

Optimisation problems deal with the solution of problems that must be done in the best possible manner. This type of solution is highly desirable in all fields particularly telecommunications and has received an increasing amount of attention. The objective of an optimisation problem is to optimise (maximise or minimise) some functions f , which is called the objective function. The objective function in most problems depends on several variables (x_1, \dots, x_n) . In many problems the choice values of x_1, \dots, x_n is subject to some constraints.

The optimisation problems in general can be presented as

Maximize (minimize) $f(x)$ subject to $r_i(x) \geq r_i, i = 1, \dots, N$

Here $f(x)$ is the objective function and $r_i(x)$ will be the constraints.

In our case we need to identify variables x_1, \dots, x_n , objective functions, parameters, and constraint in order to be able to generate the optimisation model. The followings are some of the variables that will be considered.

- **Size of subnet (broadcast domain):** cost of interception can be minimised by reducing the number of sniffers installed on the network. This can be achieved, if the size of broadcast domain is increased. However, this would generate other problems such as bandwidth reduction to users. It will also increase the chance of intruders in attacking the network. Figure 3 shows this effect.
- **Pattern of movement of mobile users:** it is important to estimate the potential flow of mobile users in different parts of the city throughout the day, as this can identify the workload necessary for sniffers used for interception. This case is shown in figure 4 and 5.
- **Sniffer systems as backup:** It is important to consider a number of sniffer systems that are required for ISPs to keep as backup for emergency situations.

Other variables or parameters that will affect the optimisation model will be costs related to sniffer maintenance, installation, management, and staff training, Quality of Service (QoS), characteristics of access points, and capacity of routers and sniffers.

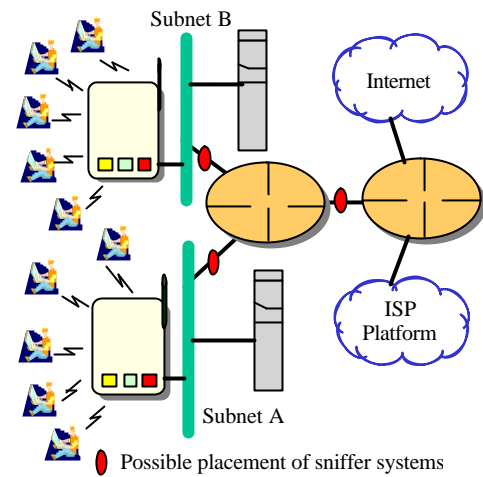


Figure 3: Effect of size of subnet on the cost of interception

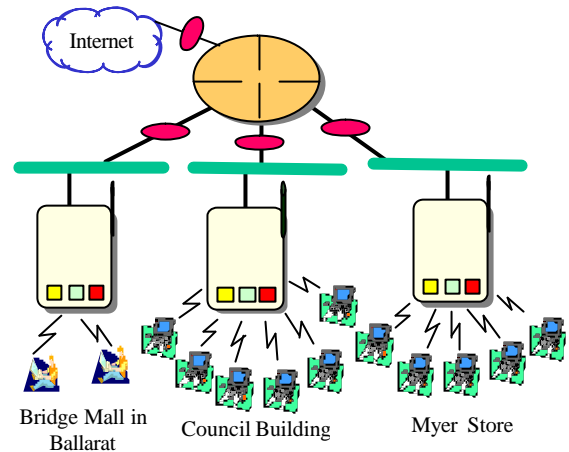


Figure 4: Buildings and stores are occupied by staff from 9 am to 12 noon

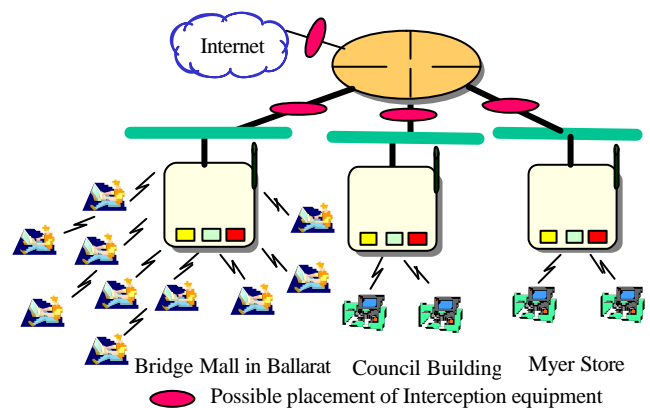


Figure 5: Bridge Mall is visited by mobile users between 12 noon to 2 pm

One of our objective functions will be the total cost of interception, which will also include cost related to sniffer installation, maintenance, and management and our constraint will be the utility or coverage of the network.

We will go through three stages to find the optimal location(s) of sniffers using optimisation techniques.

First stage will involve in construction of the mathematical model which will describes the situations under consideration. There are modern methods of optimisation techniques that can be applied to non-complicated functions, but these will not be so suitable to our problem due to the complication of the problems that were mentioned earlier and other problems such as the location(s) itself. For example if interception is performed along the radio path or some parts of the backbone network, traffic jam might occur. In any case, to find the optimal location(s) of sniffer systems on the network of mobile IP, particular optimisation techniques developed at Centre for Informatics and Applied Optimisation (CIAO) [8], [9], [10], [11] at the University of Ballarat will be used. By finding the optimal location(s) of systems using these optimisation techniques, the cost can be reduced while total network coverage is assured. The second stage is the solution of the problem. There are no universal methods that are applicable for solving this kind of optimisation model. Therefore, an adjustment to existing models and developing new model is required. Last stage is the interpretation of the results obtained and correction of the model if the results are not satisfactory.

V. CONCLUSION

This paper has explained the difficulties in Lawful Interception for IP based applications and particularly for mobile IP. It was highlighted that the cost of interception for ISPs will be significant. We intend using optimisation techniques to find the best location(s) of these systems on the network to reduce the cost of interception.

REFERENCES

- [1] European Telecommunications Standards Institute, "Telecommunications security; Lawful Interception (LI); Requirements for network functions," 2002.
- [2] European Telecommunications Standards Institute, "Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic," 2001.
- [3] M. Acey, "Europe Votes for ISP Spying Infrastructure," In Techweb News, 1999.
- [4] C.E. Perkins, "Mobile Networking Through Mobile IP," IEEE Internet Computing, January-February 1998.
- [5] Department of Justice, Industry Canada Solicitor, General Canada, "Lawful Access – Consultation Document," August 25, 2002
- [6] Australian Commonwealth Parliamentary Library, "Bills Digest No. 67 1997-98, Telecommunications Legislation Amendment Bill 1997.
- [7] J. Baloo, "Lawful Interception of IP Traffic: The European Context," 27 November 2000.
- [8] A.M. Rubinov, "Abstract Convexity and Global Optimisation," Kluwer Academic Publishers, Dordrecht, 2000.
- [9] A.M. Bagirov, "Derivative-free methods for unconstrained nonsmooth optimisation and its numerical analys," Investigacao Operacional, Vol 19, pp. 75-93, 1999.
- [10] A.M. Bagirov and A.M. Rubinov, "Cutting Angle Method and a Local Search," in press, Journal of Global Optimisation.
- [11] A.M Bagirov and J. Zhang, "Hybrid Simulating Annealing Method and Discrete Gradient Method for Global Optimisation," Proceedings of Industrial Mathematics Symposium, Perth, 2003.