Adaptive Traffic Filtering for Efficient and Secure IP-Mobility

Mirco Marchetti Michele Colajanni

Department of Information Engineering
University of Modena and Reggio Emilia
Modena, Italy
{mirco.marchetti, michele.colajanni}@unimore.it

ABSTRACT

The Mobile IP (MIP) protocol that supports node mobility in IP networks may be implemented through two routing schemes: triangular routing and reverse tunneling. While triangular routing guarantees better performance because of shorter routing paths, it is not compatible with egress filtering policies enforced by many firewalls. As a result, it is necessary to recur to the slower reverse tunneling routing scheme that causes lower mobile connection throughput and higher round trip times. In this paper, we propose an innovative adaptive traffic filtering technique in which egress filtering rules are dynamically and automatically modified to reflect the presence of mobile nodes inside the protected network. The proposed scheme, called *secure triangular routing*, guarantees the best trade-off between performance and security because it enables triangular routing without violating network security policies. Viability and performance improvements of the proposed solution have been demonstrated by experiments carried out through a prototype. The proposed solution does not require any modification in correspondent nodes or in their networks, and it fully complies with the MIP protocol specifications.

Categories and Subject Descriptors

C.2.1 [**Computer-communication networks**]: Network architecture and design—*Network communications*; C.2.3 [**Computer-communication networks**]: Network operations—*Network management*

General Terms

Design, Performance, Security

1. INTRODUCTION

We are witnessing a steady increase in both number and computational power of Internet-ready mobile devices, such as smartphones, PDAs, Internet tablets, subnotebooks and laptops. However, the great potential of mobile devices is limited by the lack of node mobility support in the IP protocol. Whenever a mobile node roams between two different networks, its IP address has to change for it to be valid in the new destination network. Hence, the mobile node is no more reachable with its previous IP address, and all the previously opened connections are interrupted. As an example, the lack of mobility support in the IP protocol prevents a mobile node to roam through different networks while downloading long files or streaming multimedia contents.

Mobility support in commonly deployed IP networks can be achieved through the *Mobile IP* protocol [14, 12, 15], that allows transparent routing of IP datagrams to mobile nodes across the Internet. This goal is reached through the introduction of two new entities, (the *Home Agent* and the *Foreign Agent*), that receive and route datagrams on behalf of the mobile node leveraging tunneling techniques. Thanks to this additional routing layer, a mobile node is always reachable with its home IP address, even though connected through a foreign network with a completely different address space. In particular, the default Mobile IP routing scheme is called *triangular routing*: IP datagrams sent to the mobile node are intercepted and routed by home and foreign agents, while datagrams generated by the mobile nodes are routed as common Internet traffic, flowing directly from the mobile node to the destination.

A serious problem of this routing scheme lays in its incompatibility with *egress filtering* policies [22], recommended as best practices [8] useful to prevent all network attacks based on source IP address spoofing. If the foreign network implements egress filtering, all the IP datagrams generated by the mobile node are blocked at the foreign network's boundary, because their source IP address do not belong to the network's address space. To overcome this drawback, the commonly adopted solution is to employ an alternative routing scheme: *reverse tunneling*. While being compliant with egress filtering policies, reverse tunneling employs a longer routing path, invariably resulting in higher round trip time and lower throughput. It is then possible to identify a clear trade-off between network security and mobile connections performance.

The main contribution of this paper is the design of a new dynamic and automatic traffic filtering approach, called *secure triangular routing* able to overcome this trade-off. Secure triangular tunneling guarantees the same performance of triangular routing while fully complying with egress filtering best practices. The basic idea is to dynamically update traffic filtering rules to reflect the presence of a mobile node

Q2SWinet'08, October 27-28, 2008, Vancouver, BC, Canada.

inside the protected network. When a mobile node roams into a foreign network, the foreign agent (trusted element in any MIP enabled network) interacts with the traffic filtering element (typically a firewall, or a border router) adding the rules needed for IP datagrams generated by the mobile node to pass through the network border without being blocked. The same rules are automatically removed as soon as the mobile node leaves the foreign network.

Viability of the proposed solution is demonstrated through a prototype, developed by modifying the source code of *Dynamics*, a popular and open source MIP implementation [4]. The prototype has been used to evaluate the performance gain of the proposed solution in realistic scenarios characterized by different network conditions.

In Section 2, we outline the elements of the MIP protocol that are relevant to the considered problem. In Section 3, we present the novel solution, called *secure triangular routing*, with a special focus on security and design of a prototype implementation. In Section 4, we describe the experimental evaluation of the proposed and existing solutions. In Section 5, we discuss related work. Some conclusions are drawn in Section 6.

2. MOBILE IP

The aim of the Mobile IP (MIP) [14, 12, 15] protocol is to allow mobile hosts to communicate with other mobile or fixed host in the Internet through the IP protocol. For this to happen, MIP provides a way to contact a mobile node using its home address (i.e., the IP address assigned to the mobile node when it is connected to its home network) independently of its current position. This goal is reached through the deployment of a simple infrastructure, consisting of two mobility agents installed in both the home network and the foreign network (defined as the network to which the mobile node is currently connected). These mobility agents are called *home agent* and *foreign agent* respectively.

It is possible to identify three main operations in the MIP protocol: discovery, registration and tunneling.

The *discovery* phase allows a mobile node that is roaming within a foreign network to discover the foreign agent and start the registration phase, required to obtain an IP address valid within the foreign network address space. This temporary IP address is called *care of address*. Foreign agent discovery is normally achieved through *agent advertisement* messages, periodically broadcasted by the foreign agent itself. Alternatively, an impatient mobile node may force a foreign agent to immediately send an agent advertisement message by broadcasting an *agent solicitation* message.

After having discovered a foreign agent inside the foreign network, the mobile node starts the *registration* phase by sending a *registration request* message to the prospective foreign agent. This request is forwarded to the home agent, that send a *registration reply* message to grant or deny the registration. The reply is processed by the foreign agent and then forwarded to the mobile node, concluding the registration phase. To improve the MIP security, *MIP authentication extensions* provide the ability to mutually authenticate mobile node, home agent and foreign agent, as well as to prevent reply attacks.

After having accomplished both the discovery and registration phases, a mobile node connected to the Internet through a foreign network has two different IP addresses: the (permanent) home address and the (temporary) care of address. MIP defines two different routing and tunneling schemes that can be used to make a mobile node reachable through its home address independently from its current position: *triangular routing* and *reverse tunneling*.

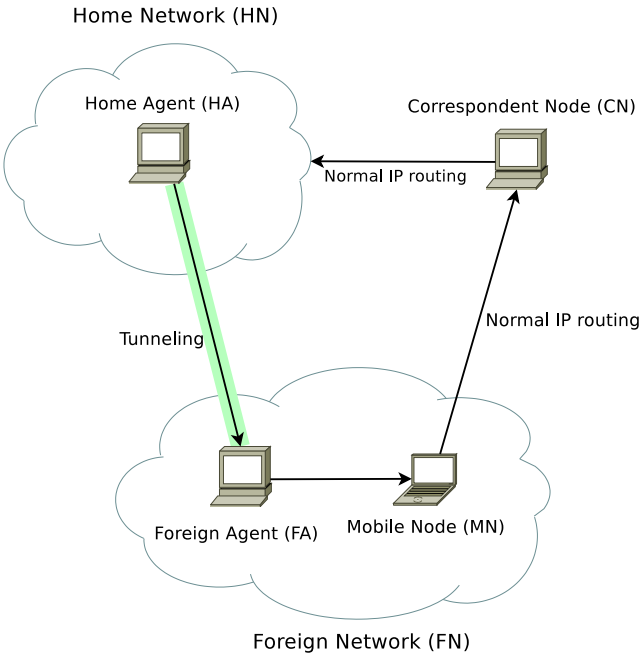

Figure 1: Triangular routing

2.1 Triangular routing

The path followed by packets sent through triangular routing is sketched in Figure 1. IP datagrams sent by the correspondent node to the mobile node are always able to reach the home network by mean of normal IP routing. Once those datagrams are inside the home network, they are intercepted by the home agent and sent to the current mobile node's care of address through a tunnel, whose endpoint is the mobile node's foreign agent. The encapsulated datagrams are then received by the foreign agent that extracts the original datagrams from the tunnel and delivers them to the mobile node. Hence, communication between correspondent node and mobile node is mediated by home agent and foreign agent. On the other hand, IP datagrams originating from the mobile node and addressed to the correspondent node are delivered through normal IP routing, without the need for any tunneling operation. Triangular routing is the default routing scheme adopted by the MIP protocol, however its use can be prevented by the enforcement of popular traffic filtering policies at the perimeter of the involved networks. In particular, it is not possible to communicate through the triangular routing scheme if the foreign network applies *egress filtering*.

2.2 Egress filtering

Egress filtering [22] is a traffic filtering policy applied by firewalls and border routers at the boundary of networks. The main idea behind egress filtering is to prevent the nodes connected inside a network to generate IP datagrams with a spoofed source address. Source address spoofing is a very simple and effective way to hide the real source of an IP data-

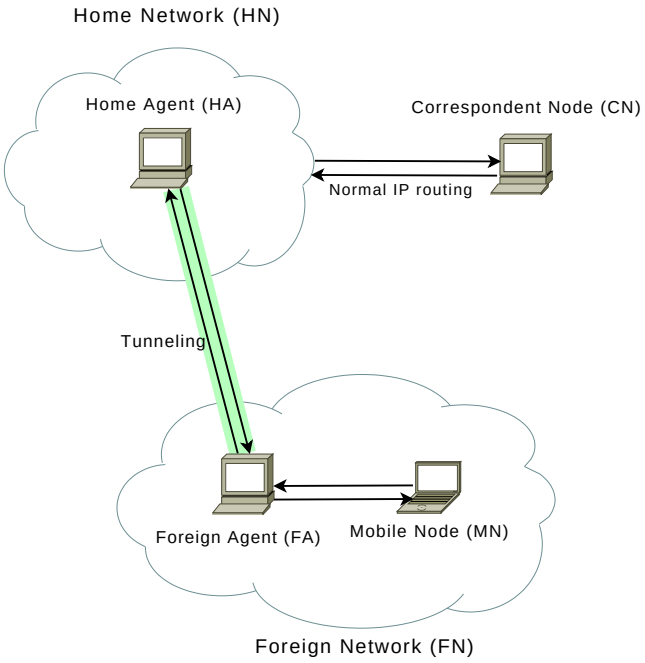

Figure 2: Reverse tunneling

gram, and this technique is widely used in several network-based attacks (such as DoS and DDoS) and stealth network scanning activities. For those reason, adoption of egress filtering policies is a widespread best practice [8]. In most of the cases, egress filtering policies are implemented by checking whether or not the source address of IP datagrams generated from inside the network belongs to the network's address space. If it is so, the source IP address is topologically valid, and the datagram is allowed to leave the network. On the other hand, if the source address does not belong to the network address space the datagram is dropped.

Egress filtering, however, is not compatible with MIP's triangular routing. All the datagrams generated by a mobile node connected to the Internet through a foreign network have its home address as source address. Such address is a routable IP address belonging to the mobile node's home network, hence it is not topologically correct within the foreign network address space. As a result, if the foreign agent's security policies include the egress filtering best practice, all the datagrams generated by the mobile node are dropped at the foreign network's border, preventing any communication between mobile node and correspondent node. To overcome this problem, thus enabling mobile node to communicate even if the foreign network apply egress filtering, the MIP protocol allows to fall back to the less efficient reverse tunneling.

2.3 Reverse tunneling

As shown in Figure 2, reverse tunneling differs from triangular routing in the path followed by IP datagrams generated by the mobile node.

To avoid sending invalid network packets through the network boundary, all the datagrams generated by the mobile node are intercepted by the foreign agent and forwarded to the home agent through a tunnel. The source address of network packets used for tunneled communication is the foreign agent's IP address, which is topologically valid inside the foreign network and not dropped by the network device implementing the egress filtering policy. The mobile node then decapsulates the original datagrams from the tunnel, and relays them to the correspondent node through normal IP routing. The source IP address of these network packets is the mobile node's home address, which is topologically valid with respect to the home network's address space. Hence this routing scheme complies with the egress filtering security policy.

Reverse tunneling's downside is that the use of a tunnel to forward packets from the foreign agent to the home agent necessarily implies a longer routing path, resulting in a higher round trip time between mobile node and correspondent node. Moreover, depending on the transport protocol employed for communication, an higher round trip time may also cause a sensible throughput decrease (as is the case of TCP).

3. SECURE TRIANGULAR ROUTING

The main contribution of this paper is the description of a dynamic and automatic network management technique able to overcome the trade-off between MIP connection performance and network security policies.

When egress filtering policies are enforced at the network boundaries, the packet filter (whether a border router or firewall) checks that the source address of all the outgoing packets is valid within the protected network's address space. The main reason because the check is performed on the address space, rather than verifying that the source address belongs to one of the hosts currently active inside the network, is to simplify the network filter management. Indeed a similar implementation would be more effective, preventing a node to generate IP datagrams with spoofed IP addresses belonging to the network address space, but currently unused. However, such a filtering policy would require the implementation of a tracking mechanism to keep trace of all the active hosts connected inside the network. Moreover, the list of active addresses should be continuously updated to reflect host connections, disconnections and IP address changes. This operation may be not practical, especially for networks with non-trivial size and with a high churn rate. Moreover, that tracking mechanism should be secured, thus preventing an attacker to make the tracking system believe that arbitrary IP addresses are currently active (leading to the introduction of unauthorized traffic filtering rules) or inactive (thus preventing its legitimate owner to communicate).

Our proposal is based on the simple observation that, within the scope of mobile nodes relying on the MIP protocol, this tracking mechanism already exists, and offers all the required guarantees of security and data freshness. Indeed, the foreign agent always knows both the care of address and the home address of all the mobile nodes currently allowed to connect to the Internet through the foreign network. These information are constantly updated, and MIP registration mechanisms provides strong security guarantees by leveraging authentication extensions.

We propose to make the most of this foreign agent's knowledge by dynamically reconfiguring the packet filter. This design choice allows for a dynamic and completely automatic update of the packet filtering rules used to enforce

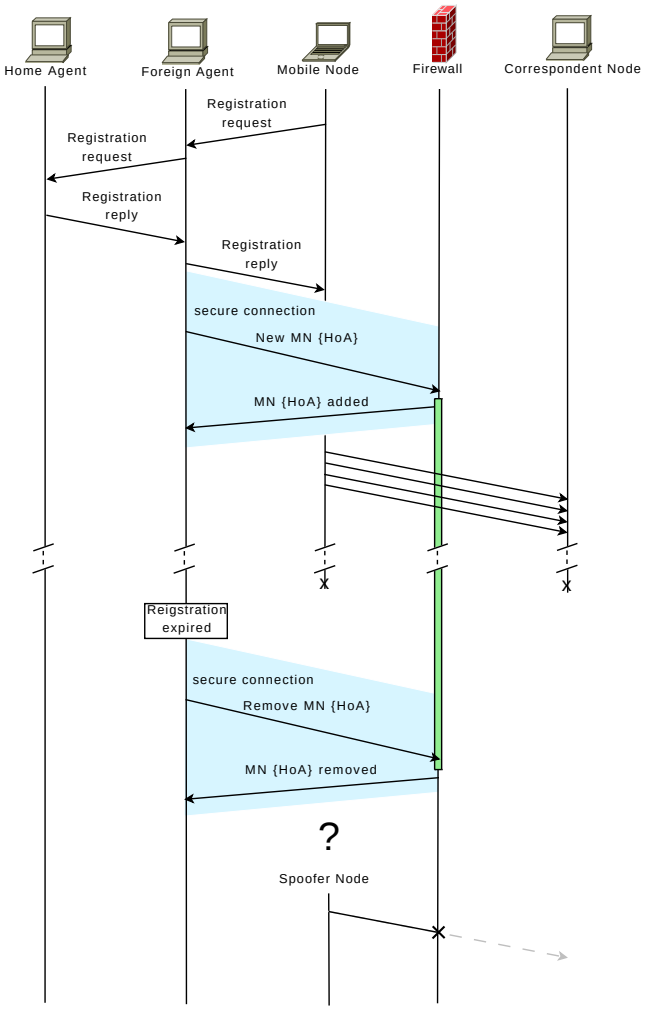

Figure 3: Secure Triangular Routing: activity diagram

the egress filtering security policy, thus taking into account the mobile nodes that are currently connected inside the network. Following that idea, we extend the MIP registration phase by adding the steps required to interact with the packet filter. An activity diagram describing the proposed registration scheme is depicted in Figure 3.

The first four messages exchanged in Figure 3 represent the standard MIP registration phase. After having received a registration reply message from the home agent allowing the registration phase to continue, the foreign agent opens a connection with the packet filter (a firewall, in this example) and adds a single rule that allows IP datagram having the mobile node home address (HoA) as source address to leave the protected network. This rule is also automatically removed by the foreign agent as soon as the registration expires (for example, because the mobile node node roams to a different foreign network, or because the registration is not renewed). Hence, after the registration expires a possible attacker (the "spoofer node" in Figure 3) is not able to send spoofed IP datagrams using the mobile node's home address.

The proposed approach, called *secure triangular routing* (STR) allows the use of the more effective triangular routing scheme, without the need to relax the foreign network's security policies. STR can be deployed just by modifying the foreign agent's implementation. Moreover, being the modified foreign agent fully compliant with the MIP standard, no modification in other mobility agents, network components or correspondent and mobile nodes is required.

3.1 Security considerations

The addition of the rule necessary to allow IP datagrams having the mobile node's home address as source address to leave the protected network is *not* a relaxation of the egress filtering security policy. Each mobile node already registered to the foreign agent, although only temporarily, is connected to the network and is authorized to send its network packet through the network boundary.

The integration between foreign agent and packet filter allows us to leverage all the security properties of the MIP protocol with authentication extension. Mutual authentication among foreign agent, mobile node and home agent is guaranteed, as well as protection from replay attacks. Those mechanisms effectively prevent attacker nodes from exploiting the STR implementation by replaying previously eavesdropped traffic to force the foreign agent in a fake registration and to feed stale or deliberately false rules to the packet filter. The connection between foreign agent and the packet filter has also to be secured, providing mutual authentication among these two network elements, as well as protection from man in the middle and replay attacks. All these guarantees can be easily achieved through the application of widespread cryptographic primitives (see Section 3.2).

Increased security levels may also be achieved by limiting foreign agent's ability to modify the packet filter ruleset. In particular, the foreign agent only needs to be able to:

- add a rule allowing IP datagrams with a single known source address that does not belong to the network address space to *leave* the network (no new traffic is allowed to enter the protected network)
- remove a packet filter rule, but *only if that rule has previously been added by the foreign agent itself* (all the other filtering rules are not modified)

Other limitations can be arbitrarily imposed on the highest number of rules that the foreign agent may add and on the highest rate at which those rules can be added, thus preventing a compromised foreign agent to disrupt packet filter performance by adding too many rules at a too high rate.

All these security measures effectively prevent the exploitation of dynamic packet filter reconfiguration by an attacker. Hence, we state that STR is as secure as a standard MIP implementation, while being able to achieve better performance.

3.2 Prototype implementation

We demonstrate the viability of the proposed solution through a fully functional prototype, based on open source software.

The prototype is based on a modified version of the *Dynamics* [4] MIP implementation. To enable the interaction between the foreign agent and the packet filter, we identified the functions used by Dynamics to establish and tear down the tunnel between foreign agent and home agent. This tunnel is used in both the triangle routing and reverse tunneling configurations, is established only after a successful

registration and is destroyed immediately after the registration expires or the mobile node becomes unreachable. In Dynamics, those functions are called *create_tunnel_upwards* and *set_expr_timer* respectively.

In our STR implementation, we modified those function to spawn a new process whose only purpose is to interact with the packet filter. Filtering rule update is then performed in parallel with tunnel management, thus minimizing the time required to complete the mobile node handoff. This concurrency does not introduce race conditions, because communications between home agent and foreign agent happens by means of IP datagrams that comply with egress filtering policies, and that are not dropped by the packet filter even though filtering rules have not been updated yet. The current implementation also checks the outcome of the packet filter interaction. If for any reason (for example, a temporary inability to communicate with the packet filter) the filtering rules can not be updated, the foreign agent is able to fall back to the slower reverse tunneling scheme, thus guaranteeing mobile nodes' connectivity.

While the proposed STR approach is generally applicable, the design and deployment of the interface between the foreign agent and the packet filter is necessarily influenced by the technology used to implement the egress filtering policy. In our prototype, traffic filtering policies are enforced through a Linux firewall, running iptables[1].

The foreign agent adds and removes iptables rules indirectly, by opening an SSH connection to the firewall and executing an interface script. The SSH connection provides public key mutual authentication between foreign agent and firewall, as well as protection from eavesdropping, replay and men in the middle attacks. The script's aim is to restrict the actions that the foreign agent may perform to the bare minimum, as well as decouple foreign agent activities from the specific commands used to modify the iptables ruleset.

4. EXPERIMENTAL RESULTS

4.1 Experimental setup

The performance gain that can be achieved by adopting the proposed solution has been evaluated through several experiments carried out in an emulated network setup. The topology is shown in Figure 4.

We deployed the MIP agents in two different networks, connected to the Internet. The foreign network is connected to the Internet through a firewall, implementing the egress filtering best practice: only IP datagrams with a routable source address belonging to the network address space are allowed to go through the network boundary. The home network is connected to the Internet through a gateway, that may also implement traffic filtering best practices (we do not make any assumption on the ability of the home network's gateway to filter network packets). Home agents and foreign agents have been implemented with our modified version of Dynamics, installed on Linux machines. Correspondent node and mobile node are normal Linux machines, and do not require any MIP-related software, nor modification in the TCP/IP stack. For the sake of simplicity, in the described experimental setup the correspondent node is a fixed host connected to the Internet. However we do not make any assumption on the correspondent node ability to roam among different network, and the correspondent node may well be a mobile node itself. On the other hand, the mobile node is assumed to roam from the home network to the foreign network.

[1]http://www.netfilter.org/projects/iptables/

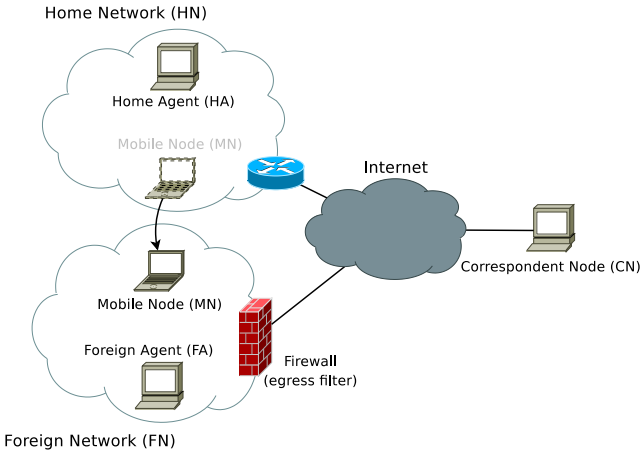

Figure 4: Emulated network topology

The described network topology has been realized by emulating all the required hosts through User Mode Linux (UML)[2]. The *netem*[3] WAN emulator has also been installed on all the nodes connected to the Internet (the firewall in the foreign network, the gateway in the home network, and the correspondent node) to emulate different bandwidth, network delay and packet loss constraints. Our STR implementation has been installed in the foreign agent, while the home agent runs an unmodified Dynamics installation (though nothing prevents the use of STR in the home agent, also). Our experimental setup has been validated by opening TCP connections between the mobile node and the correspondent node (the mobile node downloaded large files from an Apache web server installed in the correspondent node) and verifying the mobile node ability to roam to the foreign network while maintaining the connection active.

This experimental setup has been used to measure the performance of network communications between correspondent node and mobile node in both reverse tunneling and secure triangular tunneling scenarios. In particular, we experimentally evaluated two metrics relevant to the end-to-end communication performance: round trip time and TCP connection throughput.

4.2 Round Trip Time

The graph shown in Figure 5 compares the round trip time (RTT) values of IP datagrams sent between the mobile node and the correspondent node using reverse tunneling and secure triangular routing schemes. RTT measurements have been repeated under different network conditions. The Y-axis represent the RTT, measured in milliseconds, wile the X-axis represent the delay introduced by netem on the home network's gateway, affecting all the network packets flowing between the home network and the Internet. By varying this delay we are able to increase the "network distance" between the home network and both the correspondent node and the

[2]http://user-mode-linux.sourceforge.net/
[3]http://www.linuxfoundation.org/en/Net:Netem

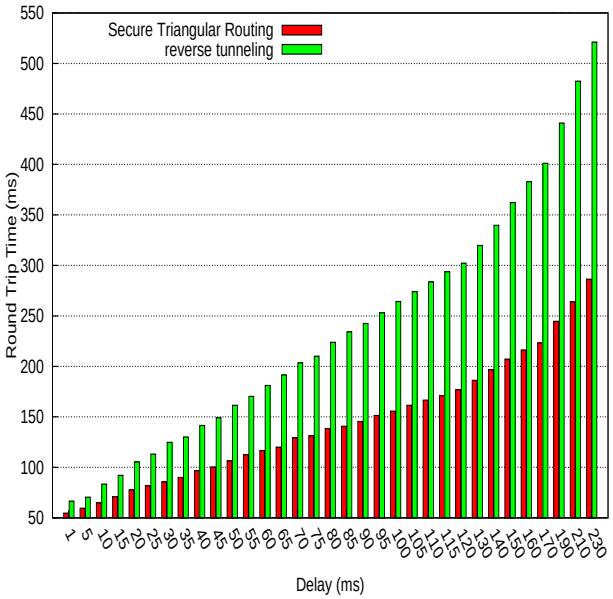

Figure 5: Round Trip Time comparison between secure triangular routing and reverse tunneling

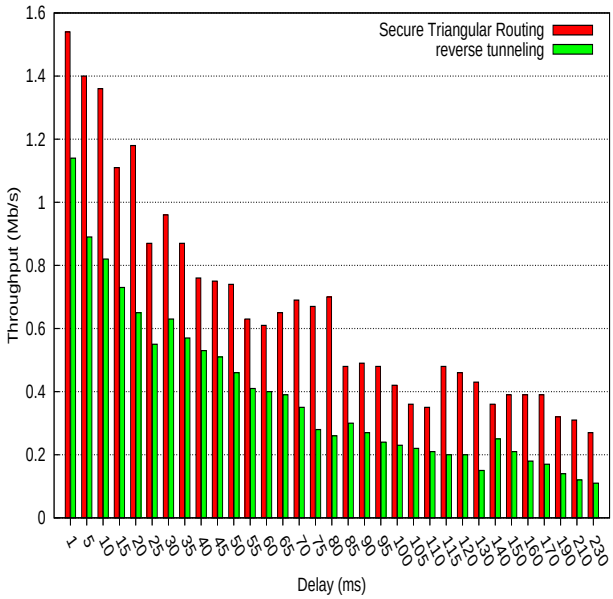

Figure 6: Throughput comparison between secure triangular routing and reverse tunneling

foreign network. The delay introduced by netem on the foreign network's gateway is fixed and equal to 45ms.

As expected, the RTT for both the routing schemes increases with the increase of the delay between the home network and the Internet. However, due to its asymmetry, triangular routing RTTs are always lower with respect to reverse tunneling. Moreover, triangular routing performance gain steadily increases for higher network delays.

4.3 Throughput

To evaluate the impacts of higher RTT values on end-to-end MIP performance, we measured the throughput of TCP connections between the mobile node and the correspondent node. Throughput measurements have been carried out using the network benchmark tool *netperf*[4]. In analogy with Section 4.2, throughput has been measured for different delays introduced by netem on the home network's gateway. Each measurement has been repeated until netperf reached a confidence interval of 2% with 99% confidence. Experimental data are shown in Figure 6. The X-axis represents the delay introduced by netem on the home network's gateway, while measured throughput is shown on the Y-axis.

It is possible to observe how detrimental a large value of RTT is for the TCP protocol. While higher delays invariably results in a lower throughput for both the routing schemes, the throughput achieved through secure triangular routing is consistently higher than the reverse tunneling throughput. As observed for the RTT, the performance gain that can be achieved using triangular tunneling grows with the growing of the network delay.

5. RELATED WORK

Several papers addressing performance and security issues of the Mobile IP protocol have been published in literature. In particular we directly compare with works published in the areas of routing optimization and security concerns.

5.1 Routing Optimization

In the fundamental trade off between routing efficiency and backward compatibility with all the standard IP hosts commonly connected to the Internet, MIP favours compatibility and transparency. This choice allows mobile nodes to communicate with correspondent nodes without requiring any modification in their software stack or in their networks. The main drawback is that triangle routing may be far from the optimal IP routing, especially if there is a significant distance between the home network and the foreign network. This problem is further exacerbated when, due to packet filtering policies applied by the involved networks, reverse tunneling becomes necessary.

The sub-optimal routing issue has been addressed by the same authors of the Mobile IP protocol in [16], where an extension to Mobile IP is proposed that allows the correspondent node to send IP datagrams directly to the mobile node, thus achieving the same efficiency level of normal IP routing. To obtain this result, the correspondent node needs to maintain an updated cache of *binding addresses*, used to store the care of addresses currently associated to all the mobile nodes with whom the correspondent node is communicating. The need to modify the networking stack of all the correspondent nodes accordingly represent the main drawback of this solution, as well as the main reason that prevents the integration of route optimization within the MIP protocol specifications.

Similar in principle to the main idea in [16], are the solutions proposed in [25] and [23]. In particular, in [25] authors propose to move the burden of storing and maintaining the binding cache list from the correspondent node to the border router of the correspondent node's network. While this solution allows a mobile node to communicate transparently with unmodified correspondent nodes, it requires mod-

[4]http://www.netperf.org/

ifications of the border router's software of (ideally) every network, including correspondent node's networks. On the other hand, in [23] the binding cache is not maintained by the correspondent node's border router, but by a completely new network element, called *correspondent agent*. From a compatibility perspective, [23] differs from [16] and [25] because no modifications are required in correspondent nodes or in their existing network component. Again, the introduction of a new mobility agent is required in (ideally) every network.

Our work clearly differentiates from the solution previously published in literature. We believe that any solution requiring modifications in the structure of existing networks and in the software stack of their components and hosts is not practical. Hence our main concern is to improve Mobile IP performance, while maintaining the highest possible degree of transparency, compatibility and interoperability with all the currently deployed hosts and network equipment. In this context, we acknowledge the triangular routing as suboptimal, but necessary routing scheme, and focus on removing the need of reverse tunneling.

5.2 Security concerns

The previous efforts in improving MIP security are mainly related to handoff and security associations with mobility agents. Solutions to these problems are described both in the MIP protocol specification [14] and further investigated in [13]. In particular, in [14] the problem represented by firewalling policies is also considered, and solved thanks to the introduction of reverse tunneling.

Several works exist that deal with integration between Mobile IP tunnels and Virtual Private Networks (VPN) [1, 3] and/or firewalls [11]. The proposed solutions provide secure mobile connections through the extensive use of (possibly encrypted) tunneled communications, having VPN concentrators (possibly implemented through modified firewalls or gateways) as endpoints. As an example, In [11] authors assume that networks are protected through a SKIP (Simple Key management for Internet Protocols, [20]) firewall, modified to be aware of Mobile IP packet format and semantic.

All of the proposed solutions relies on the underlying assumptions that all mobile and correspondent nodes are both willing and able to establish an encrypted tunnel or a dedicated VPN for each mobile connection. While this assumption can be true for specific scenarios (such as *Intelligent Transportation Systems* devised in [3]) this is not the general case for normal hosts connected to the Internet.

On the other hand, we only assume that it is possible to modify the filtering rules applied by the packet filter used to protect the foreign network. Moreover, our proposal is fully compliant with the Mobile IP standard, hence it can be easily integrated with VPN or more sophisticated firewalls and gateways whenever it is required by the specific deployment scenario.

5.3 Other Mobile IP optimizations

Several other works have been published that aim to improve performance of mobile connections. Interesting solution have been devised to avoid packet losses during handoffs, through packet buffering schemes [17, 24]. While those proposal do not shorten the handoff delay, they prevent packet losses, and the consequent slow down of TCP connections. Handoff delay can be effectively reduced through regional [5, 21] and hierarchical [2, 9, 7] registration schemes, as well as multiple links [10], and specific configuration of wireless network interface in wireless LAN scenarios [19]. Other ways to omprove the end-to-end throughput of Mobile IP connections have been investigated, like the integration of Mobile IP traffic with Multi Protocol Label Switching (MPLS) [18] and the use of Stream Control Transmission Protocol (SCTP) instead of TCP as transport layer protocol [6]. All these optimization are orthogonal to our work. Moreover, being the proposed solution fully compliant with MIP, nothing prevents their integration.

To the best of our knowledge, secure triangular routing is the first proposal able to achieve the same performance of triangular routing in presence of egress filtering, while not relying on modifications to the Mobile IP protocol, or to correspondent nodes and their networks.

6. CONCLUSIONS

In this paper we present a novel dynamic packet filtering approach, called *secure triangular routing*, able to overcome the trade off between network security and performance typical of the Mobile IP protocol. Secure triangular routing is designed to provide the same performance of *triangular routing* without the need for security policy relaxation in MobileIP-enabled networks. In particular, secure triangular routing can be effectively used in networks implementing egress traffic filtering, thus being able to replace the slower *reverse tunneling* routing scheme. This goal is achieved by automatic and dynamic modification of traffic filtering rules, necessary to reflect the temporary presence of a mobile node inside a network. Both viability and performance of the proposed solution are demonstrated by experiments carried out through a prototype based on open source software. The described solution does not require any modification in correspondent nodes or in their networks, and it fully complies with the MIP protocol specifications. Hence, secure triangular tunneling is immediately applicable to all currently deployed IP networks.

7. REFERENCES

[1] T. Braun and M. Danzeisen. Secure mobile ip communication. In *Proc. of the 26th Annual IEEE Conference on Local Computer Networks (LCN'01)*, Tampa, FL, USA, November 2001.

[2] R. Cáceres and V. N. Padmanabhan. Fast and scalable handoffs for wireless internetworks. In *Proc. of the 2nd ACM Annual International Conference on Mobile Computing and Networking (ACM MOBICOM'96)*, New York, USA, November 1996.

[3] A.-T. Cheng, C.-H. Wu, J.-M. Ho, and D. Lee. Secure mobile ip communication. In *Proc. of the 2004 IEEE International Conference on Networking, Sensing and Control*, Taipei, Taiwan, March 2004.

[4] Dynamics mobile ip. *http://dynamics.sourceforge.net*.

[5] E. Fogelstroem, A. Jonsson, and C. E. Perkins. Mobile ipv4 regional registration. *Request For Comments 4857 (Experimental), Internet Engineering Task Force*, June 2007.

[6] S. Fu and M. Atiquzzaman. Improving end-to-end throughput of mobile ip using sctp. In *Proc. of the 2003 Workshop on High Performance Switching and Routing (HPSR 2003)*, Turin, Italy, June 2003.

[7] R. Hsieh, Z. G. Zhou, and A. Sereviratne. S-mip: a seamless handoff architecture for mobile ip. In *Proc. of the 22nd Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM 2003)*, San Francisco, USA, March 2003.

[8] T. Kilallea. Recommended internet service provider security services and procedures. *Request For Comments 3013, Internet Engineering Task Force*, November 2000.

[9] W. Ma and Y. Fang. Dynamic hierarchical mobility management strategy for mobile ip networks. *IEEE Journal on Selected Areas in Communications*, 22(4):664–676, May 2004.

[10] T. Min, T. Lin, and K. Jianchu. A seamless handoff approach of mobile ip based on dual link. In *Proc. of the First IEEE International Conference on Wireless Internet (WICON'05)*, Budapest, Hungary, July 2005.

[11] G. Montenegro and V. Gupta. Sun's skip firewall traversal for mobile ip. *Request For Comments 2356, Internet Engineering Task Force*, June 1998.

[12] C. E. Perkins. Mobile networking through mobile ip. *IEEE Internet Computing*, 2(1):58–69, January 1998.

[13] C. E. Perkins. Mobile ip and security issue: an overview. In *Proc. of the First IEEE/Popov Workshop on Internet Technologies and Services*, Moscow, Russia, November 1999.

[14] C. E. Perkins. Mobile ip. *IEEE Communications Magazine*, 40(5):66–82, May 2002.

[15] C. E. Perkins. Mobility support for ipv4. *Request For Comments 3344, Internet Engineering Task Force*, August 2002.

[16] C. E. Perkins and D. B. Johnson. Route optimization in mobile ip. *IETF Internet Draft*, February 2000.

[17] C. E. Perkins and K.-Y. Wang. Optimized smooth handoffs in mobile ip. In *Proc. of the 1999 IEEE Symposium on Computers and Communications*, Red Sea, Egypt, July 1999.

[18] Z. Ren, C.-K. Tham, C.-C. Foo, and C.-C. Ko. Integration of mobile ip and multiprotocol label switching. In *Proc. of the 2001 IEEE International Conference on Communications (ICCâĂŹ2001)*, Helsinki, Finland, June 2001.

[19] S. Sharma, N. Zhu, and T. cker Chiueh. Low-latency mobile ip handoff for infrastructure-mode wireless lans. *IEEE Journal on Selected Areas in Communications*, 22(4):643–652, May 2004.

[20] M. Song, J. Huang, R. Feng, and J. Song. Simple key managementfot internet protocols (skip). In *Proc. of the Internet Society's 1995 International Networking Conference (INET'95)*, Honolulu, HI, USA, June 1995.

[21] M. Song, J. Huang, R. Feng, and J. Song. A distributed dynamic mobility management strategy for mobile ip networks. In *Proc. of the 6th International Conference on ITS Telecommunications (ITST 2006)*, Chegdu, China, June 2006.

[22] A. Wool. Direction-based filtering in firewalls. *Elsevier Computers and security*, 23(6):459–468, September 2004.

[23] C.-H. Wu, A.-T. Chen, S.-T. Lee, J.-M. Ho, and D. T. Lee. Bi-directional route optimization in mobile ip over wireless lan. In *Proc. of the 56 IEEE Vehicular Technology Conference (VTC 2002)*, Vancouver, Canada, September 2002.

[24] L. Zhang, J. Cao, and S. K. Das. A mailbox-based scheme for improving mobile ip performance. In *Proc. of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03)*, Providence, RI, USA, May 2003.

[25] P. Zhou and O. W. W. Yang. Reverse routing: An alternative to mip and romip protocols. In *Proc. of the 1999 IEEE Canadian Conference on Electrical and Computing Engineering*, Alberta, Canada, May 1999.