Computer Communications xxx (2013) xxx–xxx

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

# Policy-based flow control for multi-homed mobile terminals with IEEE 802.11u standard

Yong Cui [a,*], Xiao Ma [a], Jiangchuan Liu [b], Lian Wang [a], Yuri Ismailov [c]

[a] Department of Computer Science, Tsinghua University, Beijing, PR China
[b] School of Computing Science, Simon Fraser University, Burnaby (Metro-Vancouver), British Columbia, Canada
[c] Ericsson Research Networks and Systems, Torshamnsgatan 23 - 164 80 Kista, Sweden

ARTICLE INFO

*Article history:*
Available online xxxx

*Keywords:*
WLAN
802.11u
Policy
Flow control
Mobility

ABSTRACT

The latest IEEE 802.11u extends the highly popular IEEE 802.11-2007 standard towards supporting interworking with external networks. It however relies on a single 802.11 network interface card only, which fails to support simultaneous access of 802.11 and non-802.11 services. As such, multiple heterogenous wireless network services have yet to be effectively utilized. In this paper, we suggest to extend the original 802.11u STA (STAtion) address allocation and management, which enables multi-homing for 802.11u single interface STA by deploying the MCOA-MIP6 protocol in the network layer (layer 3). We further develop policy flow control for both up-link and down-link packets toward better QoS for mobile users and better resource utilization for carriers.

We have implemented our proposal in a Linux-based testbed. The experimental results have proven that our policy-based flow control mechanism provides better user experience. It also effectively achieves load balancing and enhances fault tolerance.



## 1. Introduction

With the rapid development and deployment of the mobile Internet, the coexistence of heterogeneous wireless mobile networks such as wireless local area network (WLAN) and 3G networks has become common for one location. Meanwhile, an increasing number of user handsets are equipped with multiple network interfaces, enabling potential Internet access through multiple heterogeneous access technologies [1–3]. Since different access technologies offer different levels of QoS, coverage, bandwidth and capacity, it is necessary to choose the most suitable network for each application flow. For instance, a device may prefer to use WiFi to download a large file, while receive a video stream through the long term evolution (LTE) network.

While theoretically possible, the simultaneous multi-access however has yet to be well supported by hosts or by networks. On the host side, the default gateway is often selected as the interface for sending packets. On the network side, packets forwarding in routers remain largely based on destination addresses. Therefore, it remains difficult to apply different policies for interface selection with multi-homed mobile terminal, for downlink or for uplink [4].

There have been significant efforts to fill up the gap. Typical examples include the concurrent multipath transfer extension of stream control transmission protocol (CMT-SCTP) [5] and the multi-path TCP (MPTCP) [6] in the transport layer; The host identify protocol (HIP) [7] between the transport and network layers; The multiple care-of address registration for mobile IPv6 (MCoA-MIP6) [4,8] in the network layer; and the IEEE 802.11u [9] and 3GPP access network discovery and selection function (ANDSF) [10] in the data link layer. Unfortunately, although they enable the use of multiple service providers' networks, there still lacks flexible control of individual data flows in the current multi-homing protocol implementation.

We are particularly interested in the latest IEEE 802.11u, which extends the highly popular IEEE 802.11-2007 standard toward supporting interworking with external networks. It however only provides a generic interface to utilize external subscription service provider networks (SSPNs) through a single 802.11 network interface card, and hence simultaneously accessing 802.11 and non-802.11 services is not supported. In this paper, we suggest to extend the original 802.11u STA (STAtion) address allocation and management, and to enable multi-homing for 802.11u single interface STA by deploying the MCOA-MIP6 protocol in the network layer (layer 3). We further develop policy flow control for both up-link and down-link packets toward better QoS for mobile users and better resource utilization for carriers.

* Corresponding author. Tel.: +86 10 627 85822; fax: +86 10 627 71138.
*E-mail addresses:* cuiyong@tsinghua.edu.cn, cy@csnet1.cs.tsinghua.edu.cn (Y. Cui).

0140-3664/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comcom.2013.09.003

We have implemented our proposal in a Linux-based testbed, which allows mobile terminals to register their multiple care-of-addresses to a home agent to simultaneously use their multiple interfaces. We have also developed a GUI program for collecting and applying user policies. Our experimental results have proven that our policy-based flow control mechanism provides better user experience. It also effectively achieves load balancing and enhances fault tolerance.

The remainder of this paper is organized as follows. We review the related work in Section 2. In Section 3 we introduce our amendments to the original 802.11u to enable multi-homing support, then in Section 4 the concept of policy and policy-based flow control architecture are discussed. In Section 5 we examine the system design and implementation of our approach. Section 6 is the system evaluation and Section 7 concludes the paper.

## 2. Related work

In this section, we provide a brief survey on the efforts made on policy-based flow control of multi-homed mobile terminals. CMT-SCTP [5] uses SCTP multi-homing feature to distribute data through multiple paths in a SCTP session. CMT-SCTP schedules data to multiple paths according to the available bandwidth of each path, i.e., as corresponding congestion windows. Data is sent in arbitrary order when the congestion window space becomes available simultaneously for one or more paths. CMT-SCTP enables multi-homed terminals to transmit data through multi-path, however, it does not take any consideration of user preferences or policies. The multi-path TCP [6] is a protocol introduced by IETF mptcp group that extends the traditional TCP for multi-homing support. Similar to CMT-SCTP, it implements a multi-path transport to transmit data across multiple paths to achieve better performance and robustness [11]. In current MPTCP implementation of UCL [12], it also selects paths for data distribution in arbitrary order that does not involve policy-based flow control. HIP [7] and MCoA-MIP6 [4,8] are IP layer multi-homing protocols that aim to provide multi-homed terminals with mobility and multi-homing capability. By far, they offer restricted opportunities for users to control flows on their own demands. Ref. [13] proposes a framework for policy management of flow distribution for various multi-homing protocols. In this framework, policy is collected, generated and dispatched to all peers absolutely by the end host. However, terminals are usually difficult to learn about the conditions of the entire access network, so that policy generated by the terminal may not be quite accurate. Therefore, we propose the collaborative flow control approach in which policy can be generated by both the terminals and the network side.

## 3. IEEE 802.11u and multi-homing extension

### 3.1. 802.11u Overview

The purposes of augmenting traditional IEEE 802.11-2007 protocol are to allow devices interwork with external networks, aid network discovery and selection, enable information transfer from external networks, and to address MAC layer enhancements that allow higher layer functionality to provide overall end-to-end interworking solution. Compared with 802.11-2007, 802.11u-2011 [9] mainly made two amendments: (1) Network discovery and selection; 802.11u provides the ability to advertise pre-association information to clients. Network selection and AP association are automatically done by protocol instead of user. (2) Interworking service; 802.11u also provides the ability to use non-802.11 networks (e.g. cellular network) under the infrastructure of 802.11. Non-AP STA is allowed to access non-802.11 service provider network services through subscription service provider (SSP) interface. AP can use this interface to communicate with external networks to complete user authentication and service providing.

As shown in Fig. 1 [9], Subscription service provider network (SSPN) access is provisioned by VLAN mapping or L2-tunneling between AP and AAA/data server of external networks. BSS1 and BSS2 belong to one ESS, STA2 is an AP-STA, which connects to a SSPN through SSPN interface. The IP address of the client's wireless network interface is allocated by DHCP server belonging to SSPN.

The second feature of 802.11u provides a practical solution to couple 802.11 and non-802.11 networks, which is the major concern in our paper. However, the traditional 802.11u has its inherent limitations. Once SSPN service is provisioned and used by client, the service provided by WLAN carrier can no longer be accessed, client is only allowed to access one network simultaneously. If the service provided by SSPN fails caused by user mobility, bad signal quality or other reasons, the client has to repeat the process of network discovery, selection and authentication to reconnect to WLAN service, which may introduce extra signaling and delay overhead inevitable. In this paper we present an extension for IEEE 802.11u to improve it.

### 3.2. Multi-homing extension for IEEE 802.11u

In order to make full use of the service provided by WLAN and other SSP networks, we extend the original 802.11u to enable multi-homing support from the entire base station set (BSS)'s perspective.

As depicted in Fig. 2, STA1 is a 802.11 client equipped with one 802.11u interface card. CN represents the corresponding node that STA1 communicates with. AP1 and AP2 both have the ability to access to SSPN and 802.11 LAN simultaneously. The interworking interface consists of two parts: the generic SSPN interface between the AP and the AAA client; and the AAA interface between the AAA client and the corresponding AAA server in the SSPN. Depending on different implementation approaches, the AAA client can be co-located with the AP or stand alone serving as a proxy or translation agent between the SSPN Interface and AAA Interface. The AAA Interface serves as a transparent carrier of the SSPN interface.

The network interface card of STA1 is configured with two different IP addresses. One of them is from the local 802.11 LAN, the other is from the DHCP server belonging to SSPN. STA1 can either use path1 or path2 to communicate with CN. In order to control data flow between STA1 and CN and manage flow control policy, we introduce a L3 mobility management protocol – mobile IP, with multiple CoA registration support. The home agent (HA) is responsible for maintaining the mapping between STA1's identifier (home

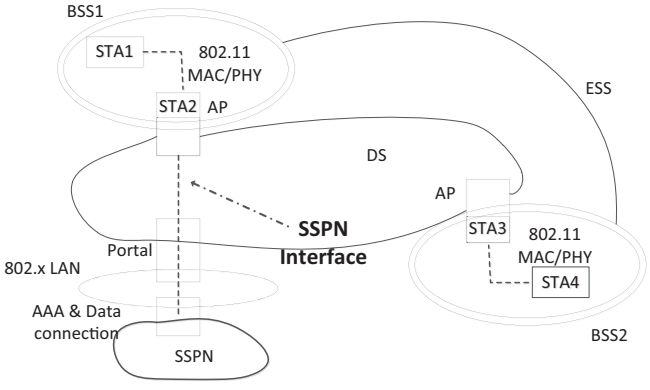


**Fig. 1.** SSPN interface service architecture of IEEE 802.11u [9].

Please cite this article in press as: Y. Cui et al., Policy-based flow control for multi-homed mobile terminals with IEEE 802.11u standard, Comput. Commun. (2013), http://dx.doi.org/10.1016/j.comcom.2013.09.003

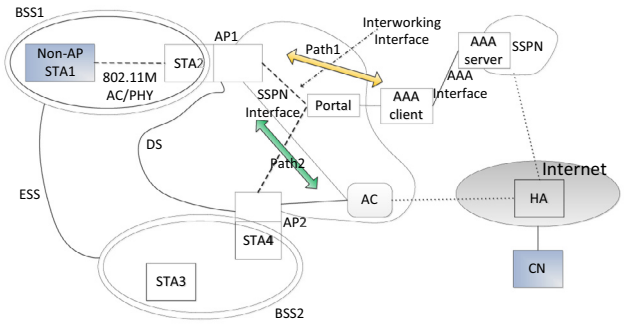


**Fig. 2.** 802.11u Multi-homing extension.

address) and its locators (CoAs), managing flow control policy generated by user or carriers, and controlling different flows to travel through different paths as the semantics of the policy provisioned in HA.

In this architecture, SSPN AAA/data server acts as STA1's foreign agent for SSPN, and STA1 itself is performed as its own foreign agent for 802.11 LAN. As depicted in mobile IP protocol standard, there are two L3-tunnels between HA and these two foreign agents, HA and two foreign agents are responsible for encapsulating/decapsulating data packets between STA1 and CN.

It is worth noting that since the first hop (client to AP-STA) is restricted to 802.11 single link, the total data throughput is therefore limited and cannot be improved by our solution, the advantages of our multi-homing extension mainly include enhancing service availability and fault tolerance.

Only enabling multi-homing is far from enough. Since there are multiple paths between access networks and corresponding node, how to effectively schedule data flows between them to achieve better QoS for network applications and better resource utilization for carriers becomes a significant issue. Next we will introduce our policy based flow control mechanism for multi-homed 802.11u terminals.

## 4. Policy-based flow control for multi-homed mobile terminals

A policy system is usually composed of policy decision point (PDP) and policy enforcement point (PEP) [14]. PDP is responsible for generating the policies while PEP for executing the policies. Fig. 3 shows an example of the policy-based flow control architecture.

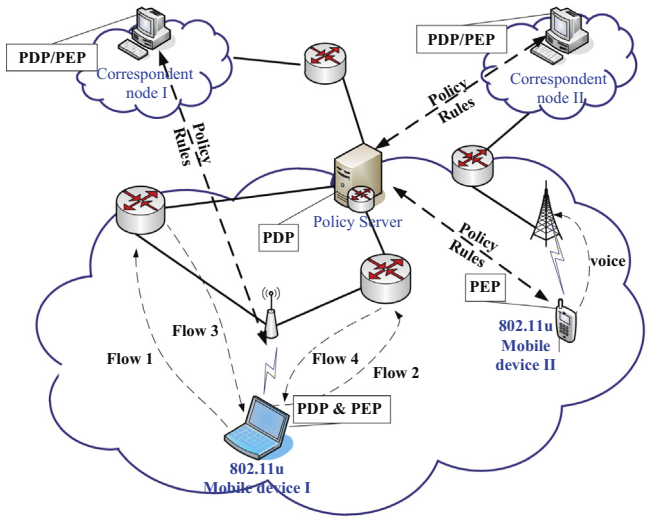


**Fig. 3.** Policy-based flow control architecture.

### 4.1. Architecture overview

In this section, we provide a more detailed description of the policy-based flow control architecture for multi-homed mobile terminals. We first introduce the key terminologies to be used in our description.

**Flow**: A flow is an unidirectional data stream identified by a set of parameters, such as the source address, destination address, source port, destination port, protocol type and so on [13]. Our paper mainly focuses on transport protocols (e.g. TCP, UDP, SCTP).

**Flow control**: Flow control is defined as a packet scheduling mechanism for multi-homed terminals in such way, those packets with different characteristics are directed to different network links.

**Policy**: Policy [15] is defined as a set of instructions triggering flow control mechanism. Policy can be divided into user policy and network policy. User policy indicates user's preferences on how to use network resources. Network policy describes the allocation and scheduling of the resources of the entire network. A policy is composed of condition part and action part, the former one describes the conditions of network resources while the latter one defines user requirements of how to use these resources or the control descriptions from network side.

**Routing rule**: Routing rule is the formalized description of policy. Each rule has a selector and an action list [13]. Selector is used to match packets according to the rules; action list indicates the path for the packets matched by the selector. Routing rule can be executed by operating system or other specific protocols after being transformed to system-specific or protocol-specific filter rules. In our work, we leverage the flow distribution rule language (FDRL) [16] to describe the routing rule.

FDRL is an OS independent rule language defining and performing per flow path selection for multi-homed terminals standardized by IETF. flow distribution policy (FDP) is defined by FDRL. FDP is a rule collection which contains several rule-sets. A rule is composed of five elements, AF, FLOW, EXTRA, ACTION and WHERE. AF, EXTRA and WHERE are optional elements. AF, FLOW and EXTRA belong to rule selector while ACTION and WHERE belong to rule action list. AF option is used to indicate whether the rule is applied to IPv4 or IPv6. FLOW option is used to match specific protocol type. EXTRA option describes some specific fields of IPv4 packets header or IPv6 packets header. ACTION option indicates operations of the packets matching previous rule items. If the packet needs to be forwarded, a path ID will be given. Otherwise, a drop instruction will be given. WHERE option is used to show where the rule will be executed. Below is an example of a rule-set.

```
ip6 tcp local port 2000-8000 on 1;
ip4 udp local 202.113.56.58 port 10000 peer port 80
drop at local;
```

The first rule indicates that all the IPv6 packets with TCP as its transport protocol and [2000,8000] as the range of its source port will be forwarded through path 1. The second rule is used to match IPv4 packets. The UDP packets with source address 202.113.56.58, source port 10000 and destination port 80 will be dropped and the rule only works at local host.

Please cite this article in press as: Y. Cui et al., Policy-based flow control for multi-homed mobile terminals with IEEE 802.11u standard, Comput. Commun. (2013), http://dx.doi.org/10.1016/j.comcom.2013.09.003

In our system implementation, we use FDRL to describe the flow control policies. Section 4 gives a detailed description of the system implementation.

Policy-based flow control mechanism is employed for mobile device I and II. The mobile device I with PDP and PEP deployed generates rules locally and synchronizes the routing rules to the correspondent node to control both up-link and down-link flows. It can generate some policies to distribute flow one and three on the Ethernet interface while flow two and four on the WiFi interface. Mobile device II with only PEP deployed requires the policy server to be responsible for policy management. Policy server generates specific policies according to the current network conditions for the mobile device. The mobile device is only responsible for receiving and executing these policies.

### 4.2. Flow control mechanism

In this section we propose a collaborative flow control mechanism. This mechanism is an extension of the approach proposed in [13]. This approach contains a policy server deployed in the network for network policy collecting, rule generating and rule dispatching. Users can also take part in policy generating in this mechanism. The user and the policy server can collaborate with each other for routing rules generation. Terminals and policy server can employ PDP and PEP simultaneously. As shown in Fig. 4, several modules are defined to achieve these functions.

**Policy Repository** is used to store policies from the user or the network side. Policies of users and network side can be exchanged by the policy management module.

**Protocols Adapter** is used to hide the differences between different underlying multi-homing support protocols. As devices may be equipped with several protocols supporting multi-homing, each protocol may use a specific identifier to define the paths of flows. Protocols Adapter is responsible for formatting various path identifiers to a uniform presentation. The paths can be described by a five-element-set path ID, interface index, protocol family, local address, remote address. The path information is notified to the Path Detector in such format.

**Path Detector** is responsible for sensing current conditions such as reachability, available bandwidth and transmission rate of each path provided by the Protocols Adapter. The output of this module is a list of path characteristics.

**Routing Rules Generator** takes user's policies and network characteristics into account to generate the formalized routing rules as the output of this module. For each user policy, the Routing Rules Generator selects a path to match the user's requirements.

**Routing Rule Receiver and Sender** synchronizes the rules to the correspondent node to ensure that they can be executed in that side.

**Rule Parser** is responsible for parsing the routing rules and stores the results into a certain data structure such as an abstract syntax tree which is processed by the Rule Executor.

**Rule Executor** translates the routing rules into filter rules according to the data structure utilized by the Rule Parser. Filter rules are some system-specific or protocol-specific packet filtering rules such as "netfilter rules" in Linux operating system. The operating system or the protocol-level multi-homing support will direct the packets according to these rules.

**Policy Merger** is responsible for merging user policy and network policy. A terminal first announces its user policies and information of multiple interfaces to the policy server. The policy then merges the user policies and network policies. Conflicts may occur during the merging process. Since network side often has more information about the entire networks, we recommend that the network side has higher priority by leading the routing rules generation when conflicts occur. Routing rules are sent to the terminal after being generated.

**Access Network Health Detector** monitors the network conditions and notifies the current network situation (e.g. the bandwidth) periodically.

In our collaborative flow control mechanism, the user and the policy server can collaborate with each other on routing rule generation, user preferences and network characteristics are smoothly combined.

## 5. System design and implementation with mobile IPv6

In this section we introduce the simultaneous multi-access system based on mobile IPv6 protocol [17,18] as a proof of the feasibility of our approach. A fraction of the functions of our entire solution is implemented in this system. It consists of two subsystems: MCoA-MIP6 Subsystem dealing with mobility management, and Policy Flow Control Subsystem responsible for policy collection, routing rule generation, transmission and execution. The MCoA-MIP6 Subsystem is implemented on the basis of the open

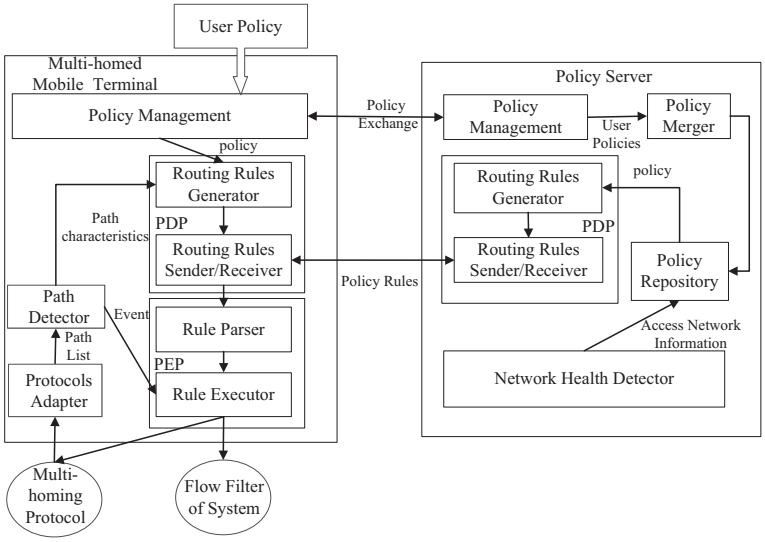


**Fig. 4.** Collaborative flow control mechanism of host and network.

source project MIPL of Helsinki University [19]. The policy control subsystem is implemented in Java. The entire system runs on Linux operating environment. We use Ubuntu 8.04 with kernel version 2.6.24 as the development platform. The specific kernel is rebuilt with modified configurations to support mobile IP function as well as policy routing. The architecture of the system is shown in Fig. 5.

### 5.1. MCoA-MIP6 Subsystem

The IP address in traditional IP protocol not only stands for the identity of the host but also presents the location of the host. Mobile IP protocols [8,20,21], change this design by separating host ID and location with a home address (HA) and a care-of address (CoA). Mobile IP protocol introduces a home agent (HA) that is responsible for receiving and sending packets for mobile nodes when they are roaming in a foreign network.

MCoA-MIP6 means mobile IPv6 with multiple care-of address registration support. Multiple interfaces of a multi-homed terminal are registered to the home agent and a tunnel will be created between each pair of home agent and a mobile node's interface (in 802.11u the interfaces are managed by AP-STA). As described in [22], a Binding Identifier (BID) is used to distinguish bindings between different interfaces of the same terminal. On mobile node, MCoA-MIP6 Subsystem gets BIDs from Policy Flow Control Subsystem when performing a binding update. It also monitors the change of the binding and sends binding update to inform home agent of the change. On home agent, when it receives a binding update with a valid BID setting in Binding Identifier mobility option [22], it should use both the home address and the BID as the search key to lookup the binding cache at first. MCoA-MIP6 Subsystem stores BIDs of each mobile node in a binding cache and provides binding information including home address, BID and care-of address to the Policy Flow Control Subsystem of home agent. The binding can be created or modified according to the result of lookup. If all the above operations are successfully completed, a Binding Acknowledgment containing the Binding Identifier mobility options must be sent to MN. When the mobile node receives a right Binding Acknowledgment a bidirectional tunnel will be created between the care-of address and the home agent address. The signaling interaction is shown in Fig. 6. After the registration, the home agent can capture all the packets sent to the home address of the mobile node and forward them through the bidirectional tunnel.

Different tunnels between the mobile node and home agent are employed as different paths. In our implementation we reuse BIDs to identify different paths and to indicate the path ID in routing rules. The management of BID in our design is done in Policy Flow Control Subsystem.

### 5.2. Policy Flow Control Subsystem

Policy Flow Control Subsystem is the core part of the system which can be divided into Connection Manager and Rule Manager. The mobile node has both two modules. The home agent only needs the Rule Manager because so far our home agent does not generate any rules for the MN. Connection Manager illustrated in Fig. 6 covers the function of Protocol Adapter, Network Detector and the Rules Generator. On the mobile node, Connection Manager collects information of interfaces and user policies to generate routing rules. Rule Manager implements the functions of Routing Rules Receiver and Sender, Rule Parser and the Rule Executor. Rule Manager is responsible for transmitting, parsing and executing rules.

Rules are mainly generated from user policy in our current implementation. In this system, we implement a GUI program for collecting users' policies. The transmission of the routing rules follows the form of generic notification messages [23] as depicted in Fig. 6. To parse the rules presented in FDRL, Rule Parser performs lexical and syntactic analysis to the rules. In our implementation, we use abstract syntax tree (AST) to store the analyzed results. The rule executor traverses the AST to obtain the information needed for policy applying.

Our implementation relies on the functions provided by netfilter framework and policy routing of Linux kernel. With the help of them, the system can support most of the functions defined in FDRL. With each BID mapped to a tunnel, a routing rule is applied as follows. First, the AST is traversed to generate a netfilter rule to mark the packets with the characteristic described in the routing rule with a certain token (BID). Second, we add a rule that directs the packet with that token to a certain routing table. Third, a routing entry is added to the corresponding routing table, which sets the tunnel related to the BID of the routing rule as the default outgoing interface. An example illustrating the entire flow control process is depicted in Fig. 7.

## 6. Testbed evaluation

We setup a lab testbed as depicted in Fig. 8 to evaluate the prototype. HP Pavilion P6515CN desktops with Linux system are configured as routers. The LAN and WLAN access consisted of such router and TP-LINK $TL_WA501G+$. Since it is difficult to find out a client with 802.11u enabled, we replace the 802.11u multi-homed client with a laptop that equipped with two network interface cards. The mobile client used in the testbed is ThinkPad T61 laptop with Gigabit Ethernet and Intel 4965AGN wireless card while the HA and CN are HP Pavilion P6515CN desktops. A tool called "iPerf" is used for testing the performance of our policy system. The

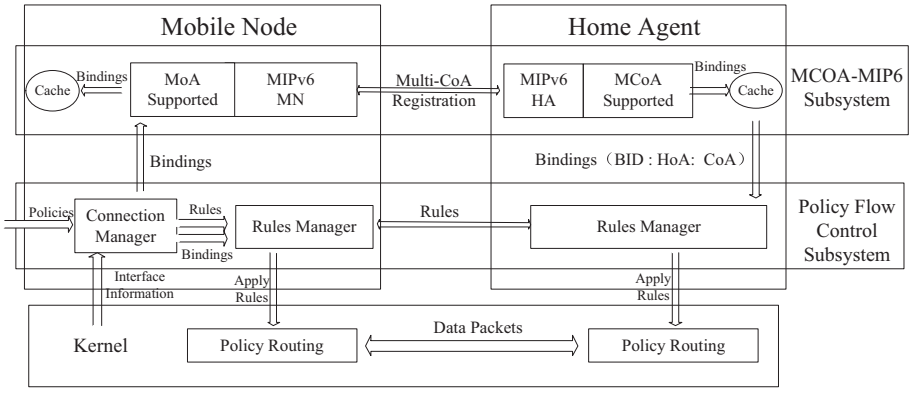


**Fig. 5.** System architecture.

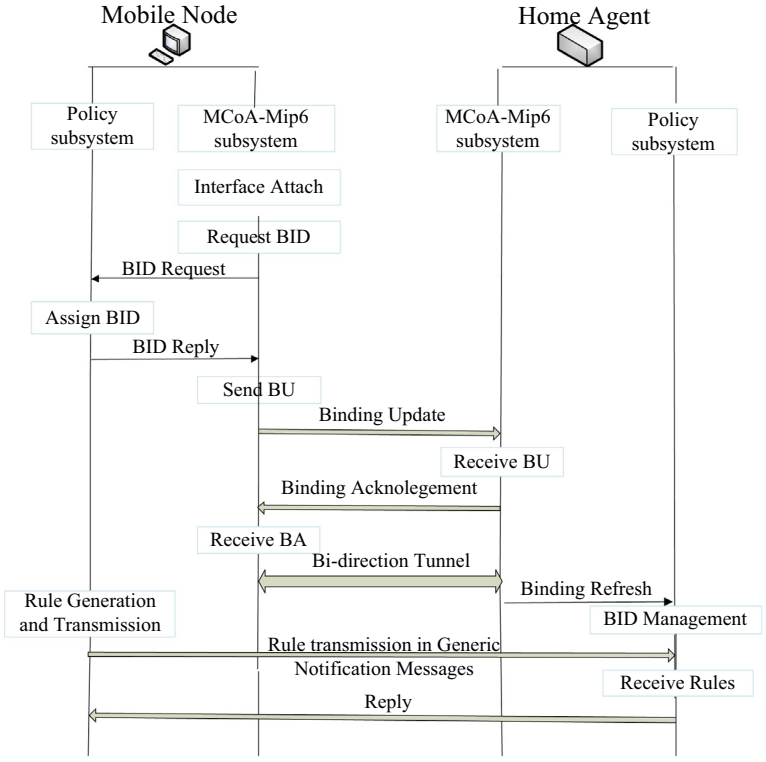


**Fig. 6.** Signaling interaction between MN and HA.

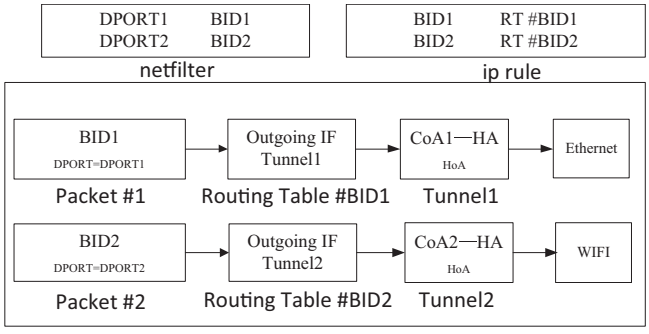


**Fig. 7.** Flow direction example.

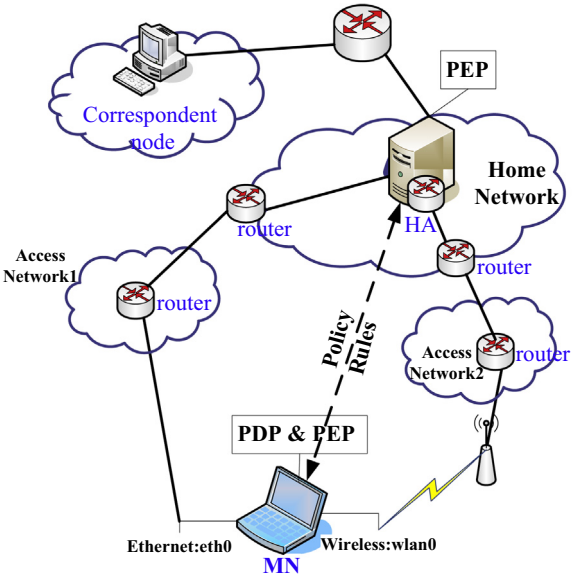


**Fig. 8.** Topology of testbed.

testing is done in a network environment with both wired LAN access and wireless LAN access. We use BID1 and BID2 to identify the two access technologies. The testing involves two scenarios. One is to test the concept of policy-based flow control described in our paper and another is fault tolerance test.

Two TCP flows with destination port 5001 and 5002 are running on the user terminal. At the beginning, only the wired network is available. The total available bandwidth of the wired LAN network is limited to 800 kb/s to simulate a congested network. Thus both two flows have to go through the LAN. Then the wireless LAN network becomes available which has higher bandwidth. Then we generate a routing rule "tcp peer port 5001 on BID2" to move one of the two TCP flows to the wireless interface.

Fig. 9 shows the result. In this graph, the horizontal axis stands for the time and the vertical axis indicates the bandwidth of the TCP flows. The two TCP flows share the bandwidth in the first 40 seconds and each of them achieves only about 250 kb/s. After the application of the routing rule, the TCP flow with destination port 5001 is directed to the wireless network. Both of the two TCP flows get higher bandwidth than before. The test verifies that policy-based flow control mechanism enables users to control and distribute different flows across multiple access technologies, allowing users to fully use the bandwidth available on heterogeneous networks.

The second test focuses on the capability of fault tolerance. TCP flows with destination port 5001 and 5002 are being transmitted through the wireless and wired interface, respectively. We then shut down the wired network to trigger a handoff. Our system

Please cite this article in press as: Y. Cui et al., Policy-based flow control for multi-homed mobile terminals with IEEE 802.11u standard, Comput. Commun. (2013), http://dx.doi.org/10.1016/j.comcom.2013.09.003

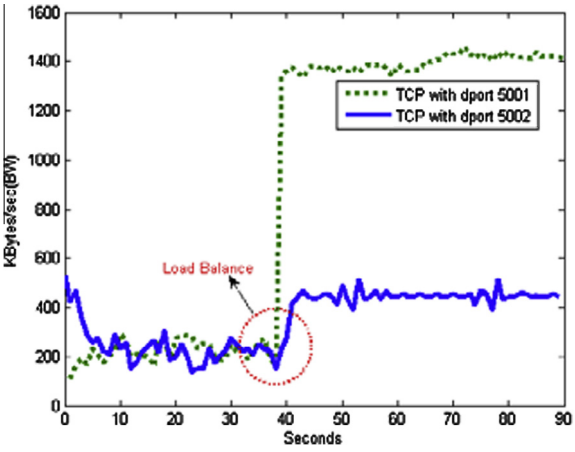


**Fig. 9.** Flow control test: bandwith-time history.

can capture this event and make a decision depending on user's current situation. In our current implementation, the system will choose one interface with the best bandwidth from the available accesses if such handoff event occurs. In this testing, the system automatically generates a routing rule "any on BID1" to redirect the TCP flow from the wired access to the wireless access. The result is shown in Fig. 10. The wired access becomes unavailable in 52 s. The dotted curve shows that the TCP rate on that interface sharply reduced to zero and then quickly recovers to about 1000 kb/s. The two flows are both running on the wireless access after the handoff. It can be observed that there is a certain degree of rate decline. In order to estimate how to quickly recover the interrupted flow during a handoff, we take a further testing. We respectively analyze how much time the interrupted flow spends on recovering to 250 kb/s and 500 kb/s. We give out ten groups of such data as depicted in Fig. 11. The testing results show that it takes about 200 and 400 ms to recover to the above rates respectively.

From the evaluation result we can see the policy-based flow control mechanism allows users and network operators to control the flows according to their preferences or network situations. Besides, the flow control mechanism has a good performance in enhancing fault tolerance and load balancing. Since most of the protocol mechanisms in our implementation (e.g. multiple CoA registration, flow distribution rule language (FDRL)) have already been standardized by IETF, and many operators all over the world (e.g. Telefonica, Sprint, China Mobile, China Unicom) have also

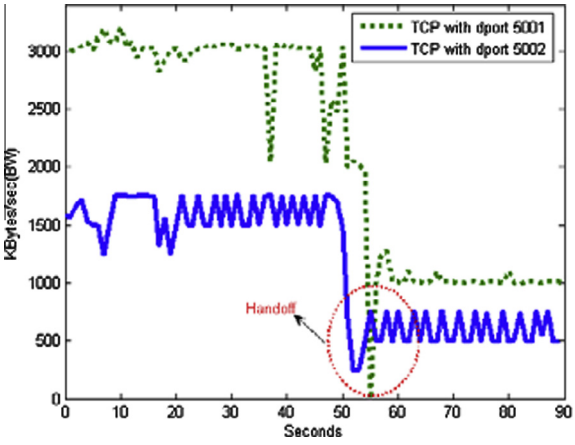


**Fig. 10.** Fault tolerance test: bandwidth-time history.

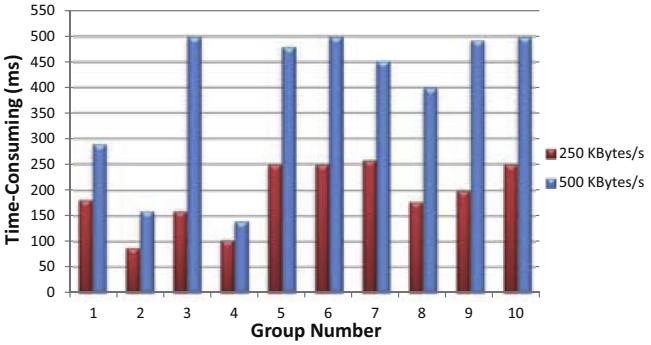


**Fig. 11.** Time-consuming statistics.

devoted themselves to develop mobile IP technology in recent years, the difficulty and complexity of the implementation for policy flow control are expected to be quite low.

It is worth noting that in our experiment we only implement a subset of our solution, which does not include the amendments to the original IEEE 802.11u with multi-homing support. The real-environment implementation and deployment of the entire solution deeply rely on deploying the modified 802.11u protocol on both STA1 and STA2, which is impractical in the experimental environment of laboratory. However, we believe the current implementation and evaluation are sufficient to verify the functions of generation, transmission and execution of flow control policy between mobile nodes and network side, which are the major contributions of the paper. IEEE 802.11u amendments are considered to be the real-network scenario instantiation of our policy flow control mechanism.

## 7. Conclusion

Current IEEE 802.11u protocol provides users with very restricted ability to control data flows among multiple access technologies. In this paper, we propose an amendment for 802.11u client to enable multi-homing support. To better utilize the available multiple paths to improve user experience, we propose a novel policy-based flow control mechanism for 802.11u multi-homed devices. Besides, we conduct a prototype system implementation and experimentation as a proof of the feasibility of our approach. The experiment result demonstrates that our policy-based flow control mechanism enables users to control and distribute different flows on different paths. It improves user experience and can effectively solve load balancing and fault tolerance issues. In the future, we intend to do more research and improvement to make the mechanism more mature.

## Acknowledgments

This work is supported by National Natural Science Foundation of China (Nos. 61120106008, 60911130511), National Major Basic Research Program of China (Nos. 2009CB320501, 2009CB320503).

## References

[1] M. Bernaschi, F. Cacace, G. Iannello, Vertical handoff performance in heterogeneous networks, in: Proceedings of the 2004 International Conference on Parallel Processing Workshops, IEEE Computer Society, 2004, pp. 100–107.
[2] X. Chen, Y. Zhao, B. Peck, D. Qiao, Sap: smart access point with seamless load balancing multiple interfaces, in: 2012 Proceedings IEEE INFOCOM, IEEE, 2012.
[3] S. Elayoubi, E. Altman, M. Haddad, Z. Altman, A hybrid decision approach for the association problem in heterogeneous networks, in: 2010 Proceedings IEEE INFOCOM, IEEE, 2010, pp. 1–5.

[4] J. Ylitalo, T. Jokikyyny, T. Kauppinen, A. Tuominen, J. Laine, Dynamic network interface selection in multihomed mobile hosts, in: Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003, IEEE, 2003, p. 10.
[5] J. Iyengar, P. Amer, R. Stewart, Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths, IEEE/ACM Transactions on Networking 14 (5) (2006) 951–964.
[6] A. Ford, C. Raiciu, M. Handley, S. Barré, J. Iyengar, Architectural guidelines for multipath TCP development, IETF, Informational RFC 6182, 2011, ISSN: 2070-1721.
[7] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson, Host identity protocol, IETF, RFC 5201, April 2008.
[8] S. Wang, Y. Cui, S. Das, Intelligent mobility support for ipv6, in: 33rd IEEE Conference on Local Computer Networks, 2008, LCN 2008, IEEE, 2008, pp. 403–410.
[9] Part 11, amendment 9: interworking with external networks, IEEE 802.11u, February 2011.
[10] Access network discovery and selection function (ANDSF) management object (MO), 3GPP TS 24.312, June 2009.
[11] C. Raiciu, S. Barre, C. Pluntke, A. Greenhalgh, D. Wischik, M. Handley, Improving datacenter performance and robustness with multipath TCP, SIGCOMM – Computer Communication Review 41 (4) (2011) 266.
[12] S. Barré, Linux kernel MPTCP project, software, <http://inl.info.ucl.ac.be/mptcp>, March 2012.
[13] K. Mitsuya, R. Kuntz, S. Sugimoto, R. Wakikawa, J. Murai, A policy management framework for flow distribution on multihomed end nodes, in: Proceedings of Second ACM/IEEE international workshop on Mobility in the evolving internet architecture, ACM, 2007, p. 10.
[14] G. Stone, B. Lundy, G. Xie, Network policy languages: a survey and a new approach, IEEE Network 15 (1) (2001) 10–21.
[15] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, S. Waldbusser, Terminology for policy-based management, Tech. Rep., RFC 3198, November 2001.
[16] C. Larsson, M. Eriksson, K. Mitsuya, K. Tasaka, R. Kuntz, Flow distribution rule language for multi-access nodes, IETF, Work in progress, draft-larsson-mext-flow-distribution-rules-02, February 2009.
[17] D. Johnson, C. Perkins, J. Arkko, Mobility support in IPv6, IETF, RFC 3775, June 2004.
[18] S. Wang, Y. Cui, S. Das, W. Li, J. Wu, Mobility in IPv6: whether and how to hierarchize the network?, IEEE Transactions on Parallel and Distributed Systems 22 (10) (2011) 1722–1729
[19] K. Sami, K. Niklas, M. Juha, N. Toni, Henrik, Petander, Mipl mobile IPv6 for linux, software, May 2003, <http://www.mipl.mediapoli.com/>.
[20] R. Hsieh, Z. Zhou, A. Seneviratne, S-mip: a seamless handoff architecture for mobile ip, 22nd Annual Joint Conference of the IEEE Computer and Communications INFOCOM, 3, IEEE, 2003, pp. 1774–1784.
[21] C. So-In, R. Jain, S. Paul, J. Pan, A policy oriented multi-interface selection framework for mobile IPv6 using the id/locator split concepts in the next generation wireless networks, The Second International Conference on Computer and Automation Engineering (ICCAE), 2010, 2, IEEE, 2010, pp. 580–584.
[22] R. Wakikawa, T. Ernst, K. Nagami, V. Devarapalli, Multiple care-of addresses registration for mobile IPv6, IETF, RFC 5648, Oct. 2009.
[23] B. Haley, S. Gundavelli, Generic notification message for mobile IPv6, IETF, Work in progress, draft-haley-mext-generic-notification-message-00, April 2008.

Please cite this article in press as: Y. Cui et al., Policy-based flow control for multi-homed mobile terminals with IEEE 802.11u standard, Comput. Commun. (2013), http://dx.doi.org/10.1016/j.comcom.2013.09.003