Compositional Modelling and Verification of IPv6 Mobility*

Peng Wu¹ and Dongmei Zhang²

¹ Lab of Computer Science, Institute of Software, Chinese Academy of Sciences,
Graduate School of the Chinese Academy of Sciences, Beijing 100080, China
wp@ios.ac.cn

² School of Computer Science & Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China
zhangdm@bupt.edu.cn

Abstract. An enhanced compositional framework is presented for modelling network protocols with symbolic transition graphs. In the context of the modelling framework, a sufficient condition for deadlock freedom of network protocols, namely interoperability, is reconstructed in a more concise way with an advantage that it allows for symbolic verification without referring to protocol states. Furthermore, a case study with Mobile IPv6 illustrates the effectiveness of the improved modelling framework and also discloses some infrangibilities of Mobile IPv6 in the sense that it can not maintain the binding coherency all the time, which may result in unreachable or unstable routes.

1 Introduction

Internet Protocol version 6 (IPv6), as a backbone of the Next Generation Internet, supports mobility as one of its fundamental features, which aims to make the global mobile Internet possible [1,2]. Research efforts have been devoted to analyze Mobile IPv6 quantitatively with respect to its performance. However, qualitative analysis of Mobile IPv6, with respect to its functionality, is of little concern.

This paper presents an enhanced version of modelling framework for network protocols using symbolic transition graphs with assignment (STGA), and extends our case study on Mobile IPv4 [3] to analyze the inherent mobility of IPv6 from a viewpoint of a complete network topology. The case study discloses some infrangibilities in the routing capability of Mobile IPv6, that is, it can not maintain the binding coherency all the time, which may result in unreachable or unstable routes. Such defects have not been reported before, even in Mobile IPv6 testing [4].

* The work is supported by grants 60223005 and 60242002 from the National Natural Science Foundation of China, a grant from the Chinese Academy of Sciences and a grant from the EYTT of MOE.

2 Model Checking Mobile IPv6

Formally, Mobile IPv6 can be described as a tuple $MIP6^{n_{ha}, n_{mh}} = (\mathbb{E}_6, \mathbb{C}_6^e, \mathbb{C}_6^p)$ with $\mathbb{E}_6 = \{HA6[0..n_{ha}-1], MH6[0..n_{mh}-1]\}$. $HA6$ and $MH6$ are STGA models of home agents and mobile hosts in Mobile IPv6, respectively; n_{ha} and n_{mh} are the number of home agents and mobile hosts, respectively. $\mathbb{C}_6^e$ is a finite set of channel connecting protocol entities with the external environment of $MIP6$. $\mathbb{C}_6^p$ is a finite set of channel connecting protocol entities with each other.

From the viewpoint of functionality, Mobile IPv6 should always be able to route IP datagrams to mobile nodes roaming outside of their home networks, which can be described as the conjunction of μ -calculus formulae: DF , AR_h , AR_f and ToD . DF means the protocol can always evolve. $AR_h(AR_f)$ means whenever a mobile host becomes stable at its home network(a foreign network), all datagrams destined for the mobile host should be forwarded without a tunnel(via a tunnel). ToD means a tunnel should be used only when the mobile host is roaming.

For details of the definitions of $MIP6$ and formulae mentioned above, one can refer to [5]. Especially, $MIP6$ can be easily proved to be interoperable. With Theorem 2.3 and 2.4 in [5], the deadlock freedom of $MIP6^{1,1}$ can be concluded without explicitly enumerating its state space exhaustively.

As far as AR and ToD are concerned, the model checking experiments end unexpectedly with negative results, which disclose the infrangibility of Mobile IPv6 in its routing capability.

2.1 Adaptive Routing

Fig. 1(a) illustrates a counterexample for the property AR_f , where a mobile host is to register its binding information. Although having acknowledged the mobile host with OK , the home agent updates its local binding list after it has forwarded a datagram received previously to the mobile host according to its current binding list, where the mobile host is supposed to be still home. Therefore the datagram will never reach the mobile host. Similarly one can find a corresponding counterexample for the property AR_h .

One way to avoid the case of datagram loss illustrated above is to switch the order between actions *reg_rep_hm* and *set_hbinding*. A model checking experiment shows the resulted model does still not satisfy AR_h , with a counterexample illustrated in Fig. 1(b), where a mobile host has moved out of its home network. Before the mobile host becomes stable at the foreign network, that is, receives a Binding Acknowledgement from its home agent, a datagram has been forwarded to its new care-of address *coa* that is not yet enabled. In such case, the behavior of the mobile host is undefined in the specification of Mobile IPv6. Similarly one can find a corresponding counterexample for the property AR_f with respect to the modified model.

2.2 Tunnel on Demand

The binding incoherency also ruins the property ToD . Fig. 2(a) illustrates a counterexample for ToD , where a mobile host is to deregister its binding in-

Fig. 1. Counterexamples for Adaptive Routing

Fig. 2. Counterexamples for Tunnel-On-Demand

formation. Although having acknowledged the mobile host with *OK*, the home agent updates its local binding list after it has forwarded a datagram received previously to the mobile host according to its current binding list, where the mobile host is supposed to be out of its home network. In such case, the behavior of the mobile host is undefined in the specification of Mobile IPv6.

The modified model resulted by switching the order between actions *reg_rep_hm* and *set_hbinding* does still not satisfy *ToD*. A counterexample is illustrated in Fig. 2(b), where a mobile host is to register its binding information. Before receiving a Binding Acknowledgement from its home agent, it receives a datagram via a tunnel, which has not yet been enabled. In such case, the behavior of the mobile host is undefined in the specification of Mobile IPv6.

3 Conclusion

An enhanced compositional framework was presented in this paper for modelling network protocols using STGA. It inherits the reactive nature of network protocols and render interoperability checking static on symbolic transition graphs. A case study on Mobile IPv6 has been conducted, respecting the deadlock-free design paradigm of the modelling framework. The case study not only shows the effectiveness of the modelling framework, but also detects some infrangibilities of Mobile IPv6 in its binding incoherency, which may make a datagram unreachable to its destination or being forwarded to an unstable mobile host.

As future work, the framework can be extended for parameterized verification. The inherent parameterized nature of the modelling framework can help verify concrete network protocols or other reactive systems in a more cost-effective way.

References

1. Johnson, D., Perkins, C.: Mobility support in IPv6. In: Second ACM International Conference On Mobile Computing And Networking (MobiCom'96), ACM (1996) 27–37
2. Johnson, D., Perkins, C., Arkko, J.: Mobility support in IPv6. Internet-Draft, IETF Mobile IP Working Group (2003)
3. Wu, P., Zhang, D.: Compositional analysis of mobile IP with symbolic transition graphs. In: 16th International Conference on Computer Communication. (2004) 1481–1488
4. ZHANG, Y.J., TIAN, J., LI, Z.C.: Mobile IPv6 and its conformance testing (2002)
5. Wu, P., Zhang, D.: Compositional analysis of mobile network protocols. Technical Report ISCAS-LCS-05-02, Lab of Computer Science, Institute of Software, Chinese Academy of Sciences (2005)