# Verification of Session Initiation Protocol Using Petri Nets

Benju Xie

***Abstract*—The Session Initiation Protocol (SIP) is one of the leading protocols for multimedia control over the Internet, On the basis of the process of Session Initiation Protocol's service, Petri net model of SIP was established. In this paper, we use Petri Nets (PNs) to model and analyze SIP, in terms of properties of Petri net and the analysis of reachability tree, the protocol was proved to be security.**

***Index Terms*—Session initiation protocol, petri nets, protocol verification, reachability tree**

## I. Introduction

SIP has been widely used for establishing, maintaining and tearing down multimedia sessions over the Internet, and it has become increasingly popular in Voice over IP applications [1]. SIP is developed by the Internet Engineering Task Force (IETF) and is specified in Request for Comments (RFC) 3261. Currently work is still being carried out within IETF, to maintain and continue the development of this protocol. Modelling and analyzing SIP specification using formal methods can help in assuring that the contents of RFC 3261 are correct, unambiguous, and easy to understand. A well-defined and verified protocol specification will reduce the cost for its implementation and maintenance, therefore from the point of view of protocol engineering, verification is also an important step of the lifecycle of protocol development. We use Petri Nets (PNs) [2] as the modelling and analyzing technique, due to many successful applications of PNs in verifying communication protocols.

## II. Procedure for Paper Submission

### A. SIP

SIP is a signalling protocol for establishing, modifying and terminating a multimedia session between two or more participants. These services are provided by SIP components (entities), including user agent, proxy server, redirect server, and registration server.

SIP has a layered architecture, comprising the syntax and encoding, transport, transaction, and transaction user (TU) layers [3], which is shown as Fig. 1:

The second layer of SIP is the transport layer. It defines the behaviour of SIP entities in sending and receiving messages over the network.

Two types of SIP transactions are defined for the transaction layer, the INVITE and the non-INVITE transactions. An INVITE transaction is initiated when an INVITE request is sent; and a non-INVITE transaction is initiated when a request other than INVITE or ACK is sent. Each of the transactions consists of a client transaction sending requests and a server transaction responding to requests.

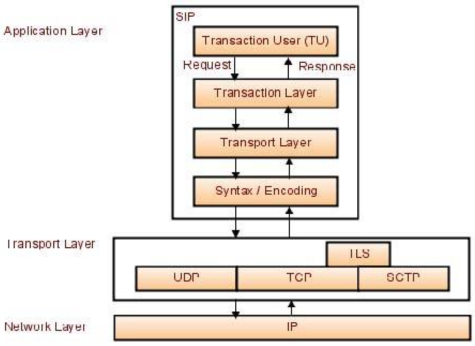

Fig. 1. Layered structure of SIP.

The top layer holds the Transaction Users (TUs), which can be any SIP entity except a stateless proxy.

SIP is a transaction-oriented protocol that carries out tasks through different transactions. So among the four SIP layers, the transaction layer is the most important one. It is responsible for request-response matching, retransmission handling with unreliable transport medium, and timeout handling. To accomplish a transaction, the transaction (such as the INVITE transaction) in the transaction layer is required to interact with the TU and the SIP transport layer.

### B. Petri Nets

Petri nets (PNs) are one of the graphical and mathematical tools widely used in modelling discrete event systems. System designers communicate with users through a PN graph for validation, and use PN based analysis methods for verification. Thus, the PN model of a system can be represented by a directed bipartite graph, i.e., consisting of two different types of nodes, called places and transitions. Places are usually drawn as circles and model conditions. Transitions are usually drawn as bars and model events. A state of the system is modelled by amarking of the PN, which is indicated by places holding some tokens. The PN model can also be represented mathematically, by an incidence matrix, which is used for structural and behavioral analysis. The system behavior can also be analyzed through a reachability tree generated by the token game.

A reachability tree shows all markings (states) reached, as well as the transition firings to reach these states. These firings drive the token game. If an enabled transition fires, its input places lose tokens and its output places deposit tokens. This means that for an event to occur, the preconditions of the event should be satisfied, and after the occurrence, the post-conditions of the event come about. The number of the tokens lost and deposited is determined by the input and output arc weights of the transition, respectively.

Manuscript received June 8, 2012; revised July 10, 2012.

Benju Xie is with the Qingdao University of Science and Technology (e-mail: qd_xbj@yeah.net)

## III. Petri Nets Model of SIP

Fig. 2 is Petri Nets model of SIP in safe state.

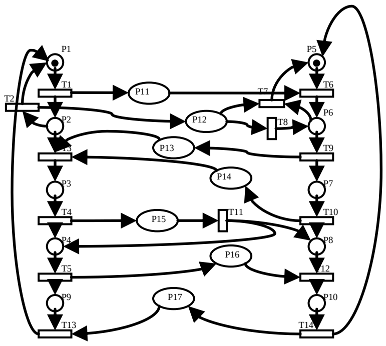

Fig. 2. Petri Nets model of SIP in safe state.

Fig. 3 is Petri Nets model of SIP in BREAK attack state.

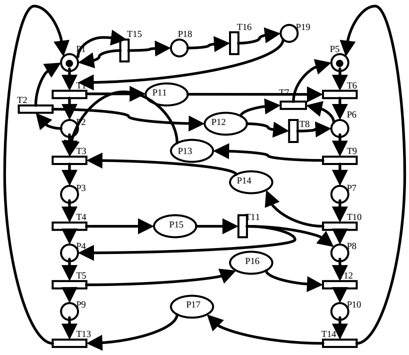

Fig. 3. Petri Nets model of SIP in BREAK attack state.

State space analysis is a main analysis technique for PNs [4], [5]. The state space of a PN is a directed graph comprising all reachable markings (states) and state changes of the PN model. By generating and querying the state space using supporting tools, we can verify the properties of a modelled system, such as absence of deadlocks (undesirable terminal states), whether or not a given state can be reached or a required service can be delivered.

## IV. Reachability Tree of SIP

The reachability problem for Petri nets is to decide, given a Petri net N and a marking M [6], whether $M \in R(N)$ .

Clearly, this is a matter of walking the reachability graph defined above, until either we reach the requested marking or we know it can no longer be found. This is harder than it may seem at first: the reachability graph is generally infinite, and it is not easy to determine when it is safe to stop.

Reachability graph tree of SIP is shown as Fig. 4.

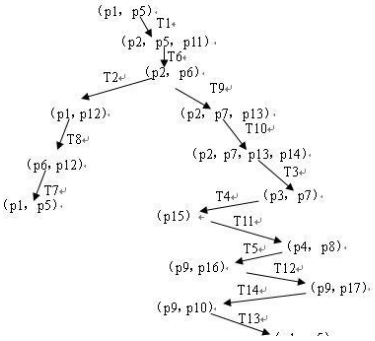

Fig. 4. Reachability graph tree of SIP.

Reachability graph tree of SIP When BREAK attack is shown as Fig. 5.

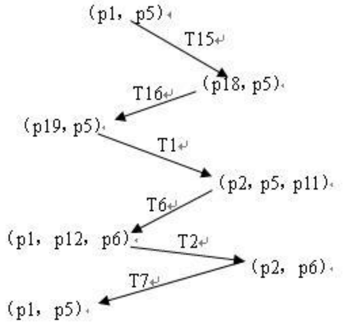

Fig. 5. Reachability graph tree of SIP When BREAK attacking.

## V. Conclusion

The Session Initiation Protocol is a core protocol of internet. In this paper we have discussed the security threats that SIP is facing and the importance of conducting formal security analysis of SIP specification. We have presented a Petri Net-based approach for assessing SIP security threats.

## References

[1] L. G. Ding and L. Liu, "Modelling and Analysis of the INVITE Transaction of the Session Initiation Protocol Using Coloured Petri Nets," *Proc. of 29th Int. Conf. on Applications and Theory of Petri Nets and Other Models of Concurrency*. LNCS, 2008, pp. 132-151, Springer.

[2] K. Jensen, "Coloured Petri nets: Basic Concepts," *Analysis Methods and Practical Use*, 2nd edition, Springer.

[3] Y. Peng, Z. Yuan, and J. Wang, "Petri Net Model of Session Initiation Protocol and Its Verification," *Proc. of Wireless Communications, Networking and Mobile Computing*. 2007, pp. 1861-1864, IEEE.

[4] D. Geneiatakis, "Survey of security vulnerabilities in session initiation protocol," *IEEE Communications Surveys & Tutorials*, 2006, vol. 8, no. 3, pp. 68-81. IEEE.

[5] K. Jensen, L. Kristensen, and L. Wells, "Coloured Petri nets and CPN tools for modelling and validation of concurrent systems," *Int. J. of Software Tools for Technology Transfer*, 2007, vol. 9, no. 3, pp. 213-254. Springer.

[6] B. B. Nieh and S. E. Tavares, "Modelling and analyzing cryptographic protocols using Petri nets," *In Advances in Cryptology - AUSCRYPT'92*, LNCS 718, pp. 275-295. Springer.