Linking Operational Semantics and Algebraic Semantics for Wireless Networks

Xiaofeng Wu and Huibiao Zhu*

Shanghai Key Laboratory of Trustworthy Computing,
Software Engineering Institute, East China Normal University, Shanghai, China
{xfwu,hbzhu}@sei.ecnu.edu.cn

Abstract. Wireless technology has achieved lots of applications in computer networks. To model and analyze wireless systems, a calculus called CWS and its operational semantics have been investigated. This paper considers the linking between the algebraic semantics and the operational semantics for this calculus. Our approach is to derive the operational semantics from the algebraic semantics. Firstly we present the algebraic semantics and introduce the concept of head normal form. Secondly we present the strategy of deriving the operational semantics from the algebraic semantics. Based on the strategy, an operational semantics is derived, which shows that the operational semantics is sound with respect to the algebraic semantics. Then the equivalence between the derivation strategy and the derived transition system is proved. This shows the completeness of the derived operational semantics. Finally, we investigate the mechanical approach to our linking method using the equational and rewriting logic system Maude. We mechanize the algebraic laws, the derivation strategy and the derived operational semantics.

1 Introduction

Wireless technology has achieved a wide range of applications in computer networks. To model and analyze wireless systems, various process calculi have been introduced, like CBS [12], CBS# [9], CMN [7], CMAN [2], CWS [6], etc. Some calculi employ special constructs to represent the topology and the behavior of network. With concepts like device location and transmission range, broadcast can be local, i.e., broadcasted messages can only be received by nodes within the transmission range. Most calculi treat broadcast as an atomic action to abstract away from collisions due to simultaneous transmissions from different sources. While interference is an essential aspect in CWS, which gives rise to complex situations on interactions in wireless systems. For CWS, the operational semantics has been developed including a reduction semantics and a labelled transition system. The main technical result of this approach is the equivalence between the two operational semantics [6].

In this paper, we consider the algebraic semantics for CWS as well as the consistency between its algebraic semantics and operational semantics. In order

* Corresponding Author

to prove the consistency, we explore the linking between the two semantics. The exploration can be achieved by deriving the operational semantics from the algebraic semantics. The linking theories between different semantic models (operational semantics, algebraic semantics and denotational semantics) [5,11,13] for a language provide the correct understanding for one semantics based on the viewpoint of another, which is advocated in Hoare and He's Unifying Theories of Programming [4].

To support the linking from the algebraic semantics to the operational semantics, we first introduce several typical types of guarded choices and a set of algebraic laws. They are used to construct the head normal form of networks. The derivation of the operational semantics from the algebraic semantics is based on the head normal form. Then we define the derivation strategy. Based on the strategy, a set of transition rules can be achieved by strict proof. This can be regarded as the soundness consideration of the operational semantics from the viewpoint of the algebraic semantics. Furthermore, we explore the equivalence between the derivation strategy and the derived transition system to show the completeness of the operational semantics from the viewpoint of the algebraic semantics. Besides the above theoretical approach, we also investigate the practical aspect of the linking. We mechanize the algebraic semantics, the head normal form, the derivation strategy and the derived operational semantics. The mechanized results indicate that the transition system of the derived operational semantics is the same as the one based on the derivation strategy.

The remainder of this paper is organized as follows. Section 2 recalls the core language of CWS. Section 3 investigates the algebraic semantics by introducing four types of guarded choices and a collection of parallel expansion laws. Section 4 defines the head normal form of networks based on the algebraic laws. Section 5 is devoted to the derivation of operational semantics from the algebraic semantics. The derivation strategy is defined and a set of transition rules is generated. Also, the equivalence between the derivation strategy and the derivation operational semantics is proved. Section 6 mechanizes our linking method. Section 7 concludes this paper.

2 Overview of CWS

The Calculus for Wireless Systems (abbreviated as CWS) has been introduced in [6]. This language contains categories of syntactic elements as follows.

$$P ::= \mathbf{out}\langle e\rangle.P \mid \langle v\rangle.P \mid \mathbf{in}(x).P \mid (x).P \mid \mathbf{0}$$

$$N ::= n[P]^{c}_{l,r} \mid N|N \mid \mathbf{0}$$

- $\mathbf{out}\langle e\rangle.P$ is a begin-transmission process willing to broadcast the value of e. It evolves to $\langle v\rangle.P$ when the broadcast is initiated, where $[\![e]\!] = v$.
- $\langle v\rangle.P$ is an end-transmission process. It indicates that the value v is currently broadcasting. It becomes P if the transmission is terminated.
- $\mathbf{in}(x).P$ is a begin-reception process willing to receive. It becomes $(x).P$ if it is activated by a transmission.

- $(x).P$ is an end-reception process. It is receiving and evolves to P if the transmission is terminated successfully or a collision happens due to another transmission. In the former case the received value is bound to x in process P. In the latter case a special value $\perp$ is bound to x denoted as $P\{\perp/x\}$ indicating failure of receiving caused by interference.
- $\mathbf{0}$ represents an inactive process, which cannot perform any actions.

The process part describes the behavior of a node. A transmission is modeled by two boundary events which introduces interference explicitly.

- $n[P]^c_{l,r}$ denotes a node owning a network address n, located at physical location l with dissemination radius r and using communication channel c. Within the node, process P executes sequentially.
- $N|N$ indicates that a network is composed of two subnetworks.
- $\mathbf{0}$ represents an empty network, defined as $n[\mathbf{0}]^c_{l,r} =_{df} \mathbf{0}$. For any network N, it satisfies $\mathbf{0}|N{=}N{=}N|\mathbf{0}$.

The network part indicates that a wireless system is modelled as a collection of nodes running in parallel. Each node is assumed to occupy a unique identifier and two nodes cannot share the same physical location. A distance function $d(\cdot,\cdot)$ is used [6,7] to return the distance between two locations.

Example 2.1 Let $N_1 =_{df} n_1[\mathbf{out}\langle e_1\rangle.P]^{c_1}_{l_1,r_1}$ and $N_2 =_{df} n_2[\mathbf{out}\langle e_2\rangle.Q]^{c_2}_{l_2,r_2}$ be two nodes. Assume that $d(l_1,l_2) \leqslant r_1$ and $d(l_2,l_1) > r_2$, then N_2 is in the transmission range of N_1, but not vice versa. □

According to the prefix of a process inside a node, all nodes can fall into four categories:

(1) transmitter, in the form $n[\mathbf{out}\langle e\rangle.P]^c_{l,r}$, is willing to start a transmission if its environment is not occupied by communication from other nodes.
(2) active transmitter, in the form $n[\langle v\rangle.P]^c_{l,r}$, is currently broadcasting.
(3) receiver, in the form $n[\mathbf{in}(x).P]^c_{l,r}$, is waiting for being activated.
(4) active receiver, in the form $n[(x).P]^c_{l,r}$, is currently receiving.

Node status of a node $n[P]^c_{l,r}$ is defined as a triple $s =_{df} (l,r,c)$, whose elements are the node's location, radius, and channel respectively.

Active transmitters T is a set of nodes (represented by their node status) which are currently transmitting in the network, i.e., (l,r,c) is an element of set T iff the node $n[P]^c_{l,r}$ is an active transmitter.

Active neighbours of a node $n[P]^c_{l,r}$ is a subset of active transmitters T, denoted as $T|(l,r,c)$. It contains the nodes which are currently transmitting and whose transmissions can be received by the node with status (l,r,c). Formally,

$$T|(l,r,c) =_{df} \{\ (l',r',c') \mid (l',r',c') \in T\ \wedge\ d(l',l) \leqslant r'\ \wedge\ c' = c\ \}$$

Example 2.2 Let $N_1 =_{df} n_1[\mathbf{out}\langle e\rangle.P]^c_{l_1,r_1}$, $N_2 =_{df} n_2[\mathbf{out}\langle f\rangle.Q]^c_{l_2,r_2}$, $N_3 =_{df} n_3[\mathbf{in}(x).R]^c_{l_3,r_3}$ and $N_4 =_{df} n_4[\mathbf{in}(y).S]^c_{l_4,r_4}$ be four nodes. Assume that N_3 is in the transmission range of N_1 and N_2 (i.e., $d(l_1,l_3) \leqslant r_1$ and $d(l_2,l_3) \leqslant r_2$), N_2 and N_4 are in the transmission range of N_1 and N_2 respectively (i.e., $d(l_1,l_2) \leqslant r_1$ and $d(l_2,l_4) \leqslant r_2$).

Then $Net = N_1|N_2|N_3|N_4$ is a network composed of four nodes using the same channel c. Initially, the active transmitters of this network is the empty

set. So N_1 and N_2 can begin their own transmissions. We consider the transition initiated by N_2 with N_3 and N_4 activated. Before the termination of transmission from N_2, N_1 is free to start its transmission as it is out of the transmission range of N_2. Hence, interference occurs at N_3 but not at N_4 which is out of the transmission range of N_1. We present this transition as following.

$$\begin{aligned}
& n_1[\mathbf{out}\langle e\rangle.P]^c_{l_1,r_1} \mid n_2[\mathbf{out}\langle f\rangle.Q]^c_{l_2,r_2} \mid n_3[\mathbf{in}(x).R]^c_{l_3,r_3} \mid n_4[\mathbf{in}(y).S]^c_{l_4,r_4} \\
\longrightarrow\ & n_1[\mathbf{out}\langle e\rangle.P]^c_{l_1,r_1} \mid n_2[\langle[\![f]\!]\rangle.Q]^c_{l_2,r_2} \mid n_3[(x).R]^c_{l_3,r_3} \mid n_4[(y).S]^c_{l_4,r_4} \\
\longrightarrow\ & n_1[\langle[\![e]\!]\rangle.P]^c_{l_1,r_1} \mid n_2[\langle[\![f]\!]\rangle.Q]^c_{l_2,r_2} \mid n_3[R\{\perp/x\}]^c_{l_3,r_3} \mid n_4[(y).S]^c_{l_4,r_4} \\
\longrightarrow\ & n_1[\langle[\![e]\!]\rangle.P]^c_{l_1,r_1} \mid n_2[Q]^c_{l_2,r_2} \mid n_3[R\{\perp/x\}]^c_{l_3,r_3} \mid n_4[S\{[\![f]\!]/y\}]^c_{l_4,r_4}
\end{aligned}$$

3 Algebraic Semantics

3.1 Guarded Choice

In order to linearize the parallel composition and to model the scheduling of interactions among nodes, we introduce a transmission tag t to record currently scheduled node, which is one of the following three forms.

(1) *none*, which indicates that no node is scheduled now.
(2) $\mathbf{out}\langle e\rangle@s$, which indicates that node s is scheduled to start its transmission.
(3) $\langle v\rangle@s$, which indicates that node s is scheduled to finish its transmission.

Now we introduce the concept of the guarded choice, which enriches the language to support the algebraic laws. The guarded choice is expressed in the form:

$$\{H_1 \to (N_1\langle T_1, t_1\rangle)\} \,[]\, ... \,[]\, \{H_n \to (N_n\langle T_n, t_n\rangle)\}$$

Each element $H \to (N\langle T, t\rangle)$ of the guarded choice is a guarded component, where

- H can be a guard in one of the following five forms: $\mathbf{out}\langle e\rangle@s$, $\langle v\rangle@s$, $\mathbf{in}(x)@s$, $(x)@s$, or **idle**. The last form indicates that the network is waiting for actions performed by its environment. Other forms indicate the performance of the corresponding action by node s.
- $N\langle T, t\rangle$ reflects the network after H is fired. If H is performed or fired, the subsequent network is N and its network status is $\langle T, t\rangle$. T is all the transmitting nodes in network N and t is the scheduled node.

To represent a network in the form of the guarded choice, we introduce four typical types of guarded choices as following.

The first type of guarded choice is composed of a set of begin transmission components and a set of end transmission components, called transmission selection guarded choice.

(form-1) $[]_{i\in I}\{\mathbf{out}\langle e_i\rangle@s_i \to (M_i\langle T_i, t_i\rangle)\} \,[]\, []_{j\in J}\{\langle v_j\rangle@s_j \to (N_j\langle T_j, t_j\rangle)\}$

The second type of guarded choice is composed of a set of begin reception guard components. The guard can be fired if the receiver s_i can receive the transmission from the scheduled node.

(form-2) $[]_{i\in I}\{\mathbf{in}(x_i)@s_i \to (M_i\langle T_i, t_i\rangle)\}$

The third type of guarded choice is composed of a set of end reception guard components. It can be fired by a transmitter or corresponding active transmitter. The former case causes interference as the receiver is currently communicating with another transmitter while in the latter case the reception terminates successfully.

(form-3) $[]_{i\in I}\{(x_i)@s_i \rightarrow (M_i\langle T_i, t_i\rangle)\}$

The fourth type of guarded choice is the idle guarded choice. It is introduced to represent the situation that no action is allowed to perform, for instance, a transmitter exposed to other transmissions. If no action can be performed in the whole network, the idle guard is fired.

(form-4) $[]_{i\in I}\{\mathbf{idle} \rightarrow (M_i\langle T_i, t_i\rangle)\}$

3.2 Algebraic Laws

In this section, we explore a collection of parallel expansion laws, which are used to derive the operational semantics.

In this work, we consider the algebraic laws for networks expressed in the form $(N\langle T, t\rangle) = (M\langle T, t\rangle)$, where N and M stand for networks, T stands for the set of active transmitters, and t stands for the transmission tag. It indicates that the behavior of network N and M are equivalent under the active transmitters set T and transmission tag t. We write $N =_{\langle T,t\rangle} M$ for $(N\langle T, t\rangle) = (M\langle T, t\rangle)$.

We define a function to reduce the number of parallel expansion laws by covering several cases at the same time. Let

$$\mathbf{par}(M, N, T, t) =_{df} \begin{cases} (N\langle T, t\rangle) & \text{if } M = \mathbf{0} \\ (M\langle T, t\rangle) & \text{if } N = \mathbf{0} \\ (M|N\ \langle T, t\rangle) & \text{otherwise} \end{cases}$$

Here we only consider half of the laws since the commutativity of parallel composition is considered, i.e., $N|M = M|N$. Our exploration for the algebraic laws is based on the four typical types of guarded choices.

We first consider the case that two parallel components are transmission selection guarded choices with a transmission tag *none*. The tag indicates that no node is scheduled. So any nodes from both parallel branches can be scheduled. In the result of parallel composition, the network status of the selected branch is applied to the **par** function. Law (par-1) reflects this case as below.

(par-1) Let $M =_{\langle T,none\rangle} []_{i\in I}\{\mathbf{out}\langle e_i\rangle@s_i \rightarrow (M_i\langle T_i, t_i\rangle)\}\ []\ []_{k\in K}\{\langle v_k\rangle@s_k \rightarrow (W_k\langle T_k, t_k\rangle)\}$

$N =_{\langle T,none\rangle} []_{j\in J}\{\mathbf{out}\langle e_j\rangle@s_j \rightarrow (N_j\langle T_j, t_j\rangle)\}\ []\ []_{o\in O}\{\langle v_o\rangle@s_o \rightarrow (V_o\langle T_o, t_o\rangle)\}$

Then $M|N =_{\langle T,none\rangle} []_{i\in I}\{\mathbf{out}\langle e_i\rangle@s_i \rightarrow \mathbf{par}(M_i, N, T_i, t_i)\}$

$[]\ []_{k\in K}\{\langle v_k\rangle@s_k \rightarrow \mathbf{par}(W_k, N, T_k, t_k)\}$

$[]\ []_{j\in J}\{\mathbf{out}\langle e_j\rangle@s_j \rightarrow \mathbf{par}(M, N_j, T_j, t_j)\}$

$[]\ []_{o\in O}\{\langle v_o\rangle@s_o \rightarrow \mathbf{par}(M, V_o, T_o, t_o)\}$

Next we explore the case that both parallel components are the second type of guarded choice with a tag $\mathbf{out}\langle e\rangle@s$. This indicates that s is scheduled to begin a transmission and all nodes in both branches can be activated by the

scheduled node shown as below.

(par-2) Let $M =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{i\in I}\{\mathbf{in}(x_i)@s_i \to (M_i\langle T_i,t_i\rangle)\}$ and
$N =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{j\in J}\{\mathbf{in}(x_j)@s_j \to (N_j\langle T_j,t_j\rangle)\}$

Then $M|N =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{i\in I}\{\mathbf{in}(x_i)@s_i \to \mathbf{par}(M_i,N,T_i,t_i)\}$
$[\!]\,[\!]_{j\in J}\{\mathbf{in}(x_j)@s_j \to \mathbf{par}(M,N_j,T_j,t_j)\}$

If both parallel components are the third type of guarded choice, the parallel result is related to the transmission tag. Cases are shown in law (par-3) and law (par-4) respectively. The tag $\langle v\rangle@s$ represents that node s is scheduled to terminate its transmission of value v. Hence the corresponding active receivers of the scheduled node can receive the value v successfully. $M_i\{v/x_i\}$ represents that the value v is bound to the variable x_i.

(par-3) Let $M =_{\langle T,\langle v\rangle@s\rangle} [\!]_{i\in I}\{(x_i)@s_i \to (M_i\langle T_i,t_i\rangle)\}$ and
$N =_{\langle T,\langle v\rangle@s\rangle} [\!]_{j\in J}\{(x_j)@s_j \to (N_j\langle T_j,t_j\rangle)\}$

Then $M|N =_{\langle T,\langle v\rangle@s\rangle} [\!]_{i\in I}\{(x_i)@s_i \to \mathbf{par}(M_i\{v/x_i\},N,T_i,t_i)\}$
$[\!]\,[\!]_{j\in J}\,\{(x_j)@s_j \to \mathbf{par}(M,N_j\{v/x_j\},T_j,t_j)\}$

The tag $\mathbf{out}\langle e\rangle@s$ indicates that node s is scheduled to start its transmission. Collisions occur for active receivers which are in the transmission range of the scheduled node. A special value is bound to the corresponding variable. Law (par-4) reflects this case as below.

(par-4) Let $M =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{i\in I}\{(x_i)@s_i \to (M_i\langle T_i,t_i\rangle)\}$ and
$N =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{j\in J}\{(x_j)@s_j \to (N_j\langle T_j,t_j\rangle)\}$

Then $M|N =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{i\in I}\{(x_i)@s_i \to \mathbf{par}(M_i\{\perp/x_i\},N,T_i,t_i)\}$
$[\!]\,[\!]_{j\in J}\{(x_j)@s_j \to \mathbf{par}(M,N_j\{\perp/x_j\},T_j,t_j)\}$

Law (par-5) shows that we deal with interference first when a node is scheduled to begin a transmission.

(par-5) Let $M =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{i\in I}\{\mathbf{in}(x_i)@s_i \to (M_i\langle T_i,t_i\rangle)\}$ and
$N =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{j\in J}\{(x_j)@s_j \to (N_j\langle T_j,t_j\rangle)\}$

Then $M|N =_{\langle T,\mathbf{out}\langle e\rangle@s\rangle} [\!]_{j\in J}\{(x_j)@s_j \to \mathbf{par}(M,N_j\{\perp/x_j\},T_j,t_j)\}$

If one parallel component is an idle guarded choice while another parallel component is not an idle guarded choice, the parallel result follows the behaviour of the branch which is not in the **idle** form. This case is shown by law (par-6) as below, where the guard H_i is not in the form of **idle**.

(par-6) Let $M =_{\langle T,t\rangle} [\!]_{i\in I}\{H_i \to (M_i\langle T_i,t_i\rangle)\}$ and
$N =_{\langle T,t\rangle} [\!]_{j\in J}\{\mathbf{idle} \to (N_j\langle T_j,t_j\rangle)\}$

Then $M|N =_{\langle T,t\rangle} [\!]_{i\in I}\{H_i \to \mathbf{par}(M_i,N,T_i,t_i)\}$

If both parallel components are idle guarded choices, the parallel result is still an idle guarded choice. We apply the network status from the left branch to the function **par** in the result. This case is expressed as below.

(par-7) Let $M =_{\langle T,t\rangle} [\!]_{i\in I}\{\mathbf{idle} \to (M_i\langle T_i,t_i\rangle)\}$ and
$N =_{\langle T,t\rangle} [\!]_{j\in J}\{\mathbf{idle} \to (N_j\langle T_j,t_j\rangle)\}$

Then $M|N =_{\langle T,t\rangle} [\!]_{i\in I}\{\mathbf{idle} \to \mathbf{par}(M,N,T_i,t_i)\}$

4 Head Normal Form

In order to support the derivation of the operational semantics from the algebraic semantics, we introduce the head normal form. The head normal form is expressed in the form of one step forward based on four typical types of guarded choices. We use the notation $\mathcal{HF}(N\langle T,t\rangle)$ to stand for the head normal form of the network N with its corresponding network status $\langle T,t\rangle$.

The head normal form of a single node is directly defined according to the corresponding network status. For a network which composed of non-empty subnetworks, its head normal form can be calculated by using the parallel expansion laws.

We first consider the cases for a transmitter with a transmission tag *none*. If it is not exposed to other transmissions (ensured by $T|(l,r,c)=\emptyset$), its head normal form is defined as the first type of guarded choice. Meanwhile the network status of the subsequent network is updated shown as below.

(1-1) $\mathcal{HF}(n[\mathbf{out}\langle e\rangle.P]^c_{l,r}\langle T,none\rangle)$

$=_{df}(\llbracket\{\mathbf{out}\langle e\rangle@(l,r,c)\rightarrow(n[\langle v\rangle.P]^c_{l,r}\langle T\cup\{(l,r,c)\},\mathbf{out}\langle e\rangle@(l,r,c)\rangle)\}\langle T,none\rangle)$ if $T|(l,r,c)=\emptyset$

Otherwise, the transmitter is not allowed to perform any action. Hence the head normal form is defined as an idle guarded choice without updating the network status of the subsequent network shown as below.

(1-1′) $\mathcal{HF}(n[\mathbf{out}\langle e\rangle.P]^c_{l,r}\langle T,none\rangle)$

$=_{df}(\llbracket\{\mathbf{idle}\rightarrow(n[\mathbf{out}\langle e\rangle.P]^c_{l,r}\langle T,none\rangle)\}\langle T,none\rangle)$ if $T|(l,r,c)\neq\emptyset$

When the transmission tag is not *none*, the head normal form is defined as an idle guarded choice with the tag reset to *none*.

(1-2) $\mathcal{HF}(n[\mathbf{out}\langle e\rangle.P]^c_{l,r}\langle T,t\rangle)$

$=_{df}(\llbracket\{\mathbf{idle}\rightarrow(n[\mathbf{out}\langle e\rangle.P]^c_{l,r}\langle T,none\rangle)\}\langle T,t\rangle)$ if t$\neq$ *none*

Next we present the head normal form for an active transmitter. If the transmission tag is *none*, the head normal form is expressed as the first type of guarded choice with the network status of the subsequent network updated.

(2-1) $\mathcal{HF}(n[\langle v\rangle.P]^c_{l,r}\langle T,none\rangle)$

$=_{df}(\llbracket\{\langle v\rangle@(l,r,c)\rightarrow(n[P]^c_{l,r}\langle T\setminus\{(l,r,c)\},\langle v\rangle@(l,r,c)\rangle)\}\langle T,none\rangle)$

Otherwise, similar to definition (1-2), the head normal form is defined as an idle guarded choice.

(2-2) $\mathcal{HF}(n[\langle v\rangle.P]^c_{l,r}\langle T,t\rangle)=_{df}(\llbracket\{\mathbf{idle}\rightarrow(n[\langle v\rangle.P]^c_{l,r}\langle T,none\rangle)\}\langle T,t\rangle)$ if t$\neq$ *none*

Then we present the head normal form for a receiver. When the transmission tag is *none* or in the form of $\langle v\rangle@s$, the head normal form is expressed as an idle guarded choice shown as (3-1) and (3-2) respectively. Definition (3-1) indicates that the receiver is listening and waiting for a transmission from its environment. Definition (3-2) expresses the case that an end transmission action has no effort on a receiver.

(3-1) $\mathcal{HF}(n[\mathbf{in}(x).P]^c_{l,r}\langle T,none\rangle)=_{df}(\llbracket\{\mathbf{idle}\rightarrow(n[\mathbf{in}(x).P]^c_{l,r}\langle T,none\rangle)\}\langle T,none\rangle)$

(3-2) $\mathcal{HF}(n[\mathbf{in}(x).P]^c_{l,r}\langle T, \langle v\rangle@s\rangle) =_{df} ([]\{\mathbf{idle} \rightarrow (n[\mathbf{in}(x).P]^c_{l,r}\langle T, none\rangle)\}\langle T, \langle v\rangle@s\rangle)$

When the tag is in the form $\mathbf{out}\langle e\rangle@s$, the head normal form is related to whether the receiver is in the transmission range of the scheduled node. If the receiver is not exposed to other transmissions and in the transmission range of the scheduled node s (ensured by $T|(l,r,c) = \{s\}$), the head normal form is expressed as the second type of guarded choice. Otherwise, it is an idle guarded choice. These cases are shown by (3-3) and (3-3′) respectively.

(3-3) $\mathcal{HF}(n[\mathbf{in}(x).P]^c_{l,r}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$

$=_{df} ([]\{\mathbf{in}(x)@(l,r,c) \rightarrow (n[(x).P]^c_{l,r}\langle T, \mathbf{out}\langle e\rangle@s\rangle)\}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$ if $T|(l,r,c) = \{s\}$

(3-3′) $\mathcal{HF}(n[\mathbf{in}(x).P]^c_{l,r}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$

$=_{df} ([]\{\mathbf{idle} \rightarrow (n[\mathbf{in}(x).P]^c_{l,r}\langle T, none\rangle)\}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$ if $T|(l,r,c) \neq \{s\}$

The head normal form of an active receiver involves more cases than other kinds of nodes because it is vulnerable to interference. When the tag is *none*, the head normal form is defined as an idle guarded choice. This indicates that the active receiver is receiving.

(4-1) $\mathcal{HF}(n[(x).P]^c_{l,r}\langle T, none\rangle) =_{df} ([]\{\mathbf{idle} \rightarrow (n[(x)P]^c_{l,r}\langle T, none\rangle)\}\langle T, none\rangle)$

When the transmission tag is not *none*, the head normal form is related to whether the active receiver is within the transmission range of the scheduled node. Definition (4-2) and (4-2′) show the cases with a transmission tag in the form $\mathbf{out}\langle e\rangle@s$, which indicates that a transmitter is scheduled to begin its transmission. If the active receiver is in the range of the scheduled node, the head normal form is expressed as the third type of guarded choice indicating the occurrence of a collision. Otherwise there is no effort on the receiver, the head normal form is an idle guarded choice.

(4-2) $\mathcal{HF}(n[(x).P]^c_{l,r}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$

$=_{df} ([]\{(x)@(l,r,c) \rightarrow (n[P]^c_{l,r}\langle T, \mathbf{out}\langle e\rangle@s\rangle)\}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$ if $\#T|(l,r,c) = 2$

(4-2′) $\mathcal{HF}(n[(x).P]^c_{l,r}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$

$=_{df} ([]\{\mathbf{idle} \rightarrow (n[(x)P]^c_{l,r}\langle T, none\rangle)\}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$ if $\#T|(l,r,c) \neq 2$

where # returns the number of elements of a finite set.

Definition (4-3) and (4-3′) show the cases with a tag in the form $\langle v\rangle@s$. If the active receiver is in the transmission range of node s, the head normal form is expressed as the third type of guarded choice indicating that it terminates the communication successfully. Otherwise the active receiver keeps receiving and its head normal form is an idle guarded choice.

(4-3) $\mathcal{HF}(n[(x).P]^c_{l,r}\langle T, \langle v\rangle@s\rangle)$

$=_{df} ([]\{(x)@(l,r,c) \rightarrow (n[P]^c_{l,r}\langle T, \langle v\rangle@s\rangle)\}\langle T, \langle v\rangle@s\rangle)$ if $T|(l,r,c) = \emptyset$

(4-3′) $\mathcal{HF}(n[(x).P]^c_{l,r}\langle T, \langle v\rangle@s\rangle)$

$=_{df} ([]\{\mathbf{idle} \rightarrow (n[(x).P]^c_{l,r}\langle T, none\rangle)\}\langle T, \langle v\rangle@s\rangle)$ if $T|(l,r,c) \neq \emptyset$

(5) $\mathcal{HF}(M \mid N\ \langle T, t\rangle)$ can be defined as the result of applying the corresponding parallel expansion laws for $\mathcal{HF}(M\langle T, t\rangle) \mid \mathcal{HF}(N\langle T, t\rangle)$.

5 Deriving Operational Semantics from Algebraic Semantics

In this section we investigates the derivation of the operational semantics from the algebraic semantics, aiming for the consistency between the two semantics.

5.1 Derivation Strategy

The transitions are written in a special notation Structural Operational Semantics (SOS) [11], which are of the two types:

$$C \longrightarrow C' \qquad \text{or} \qquad C \xrightarrow[s]{\theta} C'$$

where C and C' are the configurations representing the states before and after an execution of a step. The first type is used to model the update of the network status. The second type models a θ transition performed by node s, where θ is in one of the following forms: $\mathbf{out}\langle e\rangle$, $\langle v\rangle$, $\mathbf{in}(x)$, v, and $\perp$.

The configuration can be expressed as $\langle N, \sigma, T, t\rangle$, where

(1) The first component N is a network defined according to the syntax of CWS.
(2) The second component σ is the state of all the variables. We assume that each node owns its local variables which are distinct from variables of others.
(3) The third component T is the set of active transmitters.
(4) The forth component t is the transmission tag.

Now we consider the derivation strategy for deriving the operational semantics from the algebraic semantics. For the network N with the network status $\langle T, t\rangle$, the derivation strategy is based on its head normal form $\mathcal{HF}(N\langle T, t\rangle)$.

Definition 5.1 Derivation Strategy

(1) If $\mathcal{HF}(N\langle T, none\rangle) = (\ [\!]_{i\in I}\{\mathbf{out}\langle e_i\rangle@s_i \to (M_i\langle T \cup \{s_i\}, \mathbf{out}\langle e_i\rangle@s_i\rangle)\}$
$[\!]\ [\!]_{j\in J}\ \{\langle v_j\rangle@s_j \to (N_j\langle T \setminus \{s_j\}, \langle v_j\rangle@s_j\rangle)\}\langle T, none\rangle)$

then (1.a) $\langle N, \sigma, T, none\rangle \xrightarrow[s_i]{\mathbf{out}\langle e_i\rangle} \langle M_i, \sigma, T \cup \{s_i\}, \mathbf{out}\langle e_i\rangle@s_i\rangle$

(1.b) $\langle N, \sigma, T, none\rangle \xrightarrow[s_j]{\langle v_j\rangle} \langle N_j, \sigma, T \setminus \{s_j\}, \langle v_j\rangle@s_j\rangle$

(2) If $\mathcal{HF}(N\langle T, t\rangle) = ([\!]_{i\in I}\{\mathbf{in}(x_i)@s_i \to (N_i\langle T, t\rangle)\}\langle T, t\rangle)$

then $\langle N, \sigma, T, t\rangle \xrightarrow[s_i]{\mathbf{in}(x_i)} \langle N_i, \sigma, T, t\rangle$

(3) If $\mathcal{HF}(N\langle T, \langle v\rangle@s\rangle) = ([\!]_{i\in I}\{(x_i)@s_i \to (N_i\langle T, \langle v\rangle@s\rangle)\}\langle T, \langle v\rangle@s\rangle)$

then $\langle N, \sigma, T, \langle v\rangle@s\rangle \xrightarrow[s_i]{v} \langle N_i, \sigma[v/x_i], T, \langle v\rangle@s\rangle$

(4) If $\mathcal{HF}(N\langle T, \mathbf{out}\langle e\rangle@s\rangle) = ([\!]_{i\in I}\{(x_i)@s_i \to (N_i\langle T, \mathbf{out}\langle e\rangle@s\rangle)\}\langle T, \mathbf{out}\langle e\rangle@s\rangle)$

then $\langle N, \sigma, T, \mathbf{out}\langle e\rangle@s\rangle \xrightarrow[s_i]{\perp} \langle N_i, \sigma[\perp/x_i], T, \mathbf{out}\langle e\rangle@s\rangle$

(5) If $\mathcal{HF}(N\langle T, t\rangle) = ([\!]_{i\in I}\{\mathbf{idle} \to (N\langle T, none\rangle)\}\langle T, t\rangle)$ and $t \neq none$

then $\langle N, \sigma, T, t\rangle \longrightarrow \langle N, \sigma, T, none\rangle$

If the head normal form of a network is expressed as a transmission selection guarded choice, then it can perform a transition of item (1.a) or a transition of item (1.b). If the head normal form is expressed as the second type of guarded choice, then the network can perform a transition shown as (2) above. If the head normal form of a network is expressed as the third type of guarded choice, the transition it can perform depends on the transmission tag. When the tag is in the form $\langle v\rangle@s$, the network can perform a transition shown as (3) above. The corresponding variable of the receiver is updated by the received value and other variables keep unchanged, denoted as $\sigma[v/x_i]$. When the tag is in the form $\mathbf{out}\langle e\rangle@s$, the network must perform a collision transition and a special value is bound to the corresponding variable shown as (4) above. If the head normal form is expressed as an idle guarded choice, then the network should perform an idle transition resetting the tag to *none* in order to proceed the next scheduling.

5.2 Deriving Operational Semantics

In this section we derive the operational semantics according to the derivation strategy. This procedure shows the soundness of our operational semantics, i.e., all transition rules in the operational semantics can be generated from the algebraic semantics. The derived operational semantics is expressed as theorems to be proved. Theorem 5.1 to Theorem 5.4 are achieved directly from the definition of the head normal form and the derivation strategy. Theorem 5.5 explores the rules for parallel composition of networks.

Theorem 5.1

(1) $\langle n[\mathbf{out}\langle e\rangle.P]^c_{l,r},\sigma,T,none\rangle \xrightarrow[(l,r,c)]{\mathbf{out}\langle e\rangle} \langle n[\langle v\rangle.P]^c_{l,r},\sigma,T\cup\{(l,r,c)\},\mathrm{out}\langle e\rangle@(l,r,c)\rangle$ if $T|(l,r,c)=\emptyset$

(2) $\langle n[\mathbf{out}\langle e\rangle.P]^c_{l,r},\sigma,T,t\rangle \longrightarrow \langle n[\mathbf{out}\langle e\rangle.P]^c_{l,r},\sigma,T,none\rangle$ if $t\neq none$

The above theorem illustrates the transition rules for a node willing to start a broadcast. The first rule shows that a transmitter can start its transmission if it is not exposed to other transmissions. The second rule indicates that the transmitter cannot be scheduled when another node is scheduled.

Theorem 5.2

(1) $\langle n[\langle v\rangle.P]^c_{l,r},\sigma,T,none\rangle \xrightarrow[(l,r,c)]{\langle v\rangle} \langle n[P]^c_{l,r},\sigma,T\setminus\{(l,r,c)\},\langle v\rangle@(l,r,c)\rangle$

(2) $\langle n[\langle v\rangle.P]^c_{l,r},\sigma,T,t\rangle \longrightarrow \langle n[\langle v\rangle.P]^c_{l,r},\sigma,T,none\rangle$ if $t\neq none$

The above theorem illustrates the transition rules for an active transmitter. It can be scheduled to finish its transmission without any additional conditions if the transmission tag is *none*. Otherwise it performs an idle transition.

Theorem 5.3

(1) $\langle n[\mathbf{in}(x).P]^c_{l,r},\sigma,T,\mathbf{out}\langle e\rangle@s\rangle \xrightarrow[(l,r,c)]{\mathbf{in}(x)} \langle n[(x).P]^c_{l,r},\sigma,T,\mathbf{out}\langle e\rangle@s\rangle$, if $T|(l,r,c)=\{s\}$

(2) $\langle n[\mathbf{in}(x).P]^c_{l,r},\sigma,T,\mathbf{out}\langle e\rangle@s\rangle \longrightarrow \langle n[\mathbf{in}(x).P]^c_{l,r},\sigma,T,none\rangle$, if $T|(l,r,c)\neq\{s\}$

(3) $\langle n[\mathbf{in}(x).P]^c_{l,r},\sigma,T,\langle v\rangle@s\rangle \longrightarrow \langle n[\mathbf{in}(x).P]^c_{l,r},\sigma,T,none\rangle$

The above theorem illustrates the transition rules for a receiver. The receiver is activated if the scheduled node starts a transmission that can reach it and

it is not exposed to other transmissions. Otherwise it keeps waiting for being activated and performs an idle transition.

Theorem 5.4

(1) $\langle n[(x).P]^c_{l,r}, \sigma, T, \mathbf{out}\langle e\rangle@s\rangle \xrightarrow[(l,r,c)]{\perp} \langle n[P]^c_{l,r}, \sigma[\perp/x], T, \mathbf{out}\langle e\rangle@s\rangle$, if $\#T|(l,r,c)=2$

(2) $\langle n[(x).P]^c_{l,r}, \sigma, T, \mathbf{out}\langle e\rangle@s\rangle \longrightarrow \langle n[(x).P]^c_{l,r}, \sigma, T, none\rangle$, if $\#T|(l,r,c)\neq 2$

(3) $\langle n[(x).P]^c_{l,r}, \sigma, T, \langle v\rangle@s\rangle \xrightarrow[(l,r,c)]{v} \langle n[P]^c_{l,r}, \sigma[v/x], T, \langle v\rangle@s\rangle$, if $T|(l,r,c)=\emptyset$

(4) $\langle n[(x).P]^c_{l,r}, \sigma, T, \langle v\rangle@s\rangle \longrightarrow \langle n[(x).P]^c_{l,r}, \sigma, T, none\rangle$, if $T|(l,r,c)\neq\emptyset$

The above theorem illustrates the transition rules for an active receiver. When a node is scheduled to begin a transmission that can reach the active receiver, a collision occurs. The first rule expresses this case. If the corresponding active transmitter is scheduled, then the active receiver can terminate successfully.

Theorem 5.5

(1) If $\langle N, \sigma, T, t\rangle \xrightarrow[s]{\beta} \langle N', \sigma', T', t'\rangle$, then

$$\langle N|M, \sigma, T, t\rangle \xrightarrow[s]{\beta} \langle N'|M, \sigma', T', t'\rangle, \quad \langle M|N, \sigma, T, t\rangle \xrightarrow[s]{\beta} \langle M|N', \sigma', T', t'\rangle$$

where β is in one of the following forms: $\mathbf{out}\langle e\rangle$, $\langle v\rangle$, v, and $\perp$.

(2) If $\langle N, \sigma, T, t\rangle \xrightarrow[s]{\mathbf{in}(x)} \langle N', \sigma, T, t\rangle$ and $\langle M, \sigma, T, t\rangle \xrightarrow[s]{\perp}\!\!\!\!\!\!/\;\;$, then

$$\langle N|M, \sigma, T, t\rangle \xrightarrow[s]{\mathbf{in}} \langle N'|M, \sigma, T, t\rangle, \qquad \langle M|N, \sigma, T, t\rangle \xrightarrow[s]{\mathbf{in}} \langle M|N', \sigma, T, t\rangle$$

where $\xrightarrow[s]{\perp}\!\!\!\!\!\!/\;\;$ represents that the network cannot perform a collision transition.

(3) If $\langle N, \sigma, T, t\rangle \longrightarrow \langle N, \sigma, T, t'\rangle$ and $\langle M, \sigma, T, t\rangle \longrightarrow \langle M, \sigma, T, t'\rangle$, then

$$\langle N|M, \sigma, T, t\rangle \longrightarrow \langle N|M, \sigma, T, t'\rangle, \qquad \langle M|N, \sigma, T, t\rangle \longrightarrow \langle M|N, \sigma, T, t'\rangle$$

The above theorem illustrates the transition rules for the parallel composition of networks. The first rule considers all θ transitions except the begin reception transition. The second rule describes that a begin reception transition can be fired if no collision transition can be performed. The third rule indicates that an idle transition can be fired if all parallel components can perform an idle transition.

5.3 Equivalence of Derivation Strategy and Transition System

The collection of the transition rules derived from the derivation strategy in the previous subsection can be viewed as an operational semantics of CWS. The derivation approach shows the soundness of the operational semantics, but there remains another issue about the equivalence between the derivation strategy and the transition system, i.e., the set of transition rules derived from the derivation strategy should be the same as the set of transitions generated from the transition systems.

In order to prove the equivalence, we need to prove that the transition exists in the transition system if and only if it exists in the derivation strategy, which can be divided as the following two items:

(1) If the transition $\langle N, \sigma, T, t\rangle \xrightarrow{\alpha} \langle N', \sigma', T', t'\rangle$ exists in the transition system, then it also exists in the derivation strategy.

(2) If the transition $\langle N, \sigma, T, t\rangle \xrightarrow{\alpha} \langle N', \sigma', T', t'\rangle$ exists in the derivation strategy, then it also exists in the transition system.

Here "$\xrightarrow{\alpha}$" stands for the two types of transitions defined in section 5.1.

As our transition system is derived from the derivation strategy, the item (1) should be correct. So we consider item (2) as a theorem to be proved.

Theorem 5.6 If the transition $\langle N, \sigma, T, t\rangle \xrightarrow{\alpha} \langle N', \sigma', T', t'\rangle$ exists in the derivation strategy, then it also exists in the transition system.

Proof First, we give the proof for a single node. Here we consider the proof for a transmitter and the proof of others are similar. We know that this node has two kinds of head normal form with different network status. Assume

$$\mathcal{HF}(N\langle T, t\rangle) = ([]\{\mathbf{out}\langle e\rangle@(l, r, c) \to (n[\langle v\rangle.P]^c_{l,r}\langle T', \mathbf{out}@(l, r, c)\rangle)\}\langle T, t\rangle)$$

where t is in the form of *none*, $T' = T \cup \{(l, r, c)\}$ and $T|(l, r, c) = \emptyset$.

According to item (1) in Definition 5.1, N can perform the transition as below:

$$\langle n[\mathbf{out}\langle e\rangle.P]^c_{l,r}, \sigma, T, none\rangle \xrightarrow[(l,r,c)]{\mathbf{out}\langle e\rangle} \langle n[\langle v\rangle.P]^c_{l,r}, \sigma, T \cup \{(l, r, c)\}, \mathbf{out}\langle e\rangle@(l, r, c)\rangle$$

This exists in the transition systems (i.e., rule (1) in Theorem 5.1). Assume

$$\mathcal{HF}(N\langle T, t\rangle) = ([]\{\mathbf{idle} \to (N\langle T, none\rangle)\}\langle T, t\rangle)$$

According to Definition 5.1(5) in derivation strategy, N can perform the transition as below:

$$\langle n[\mathbf{out}\langle e\rangle.P]^c_{l,r}, \sigma, T, t\rangle \longrightarrow \langle n[\mathbf{out}\langle e\rangle.P]^c_{l,r}, \sigma, T, none\rangle \quad \text{if} \quad \mathrm{t} \neq none$$

This transition is in accordance with the transition rule (2) in Theorem 5.1. So it also exists in the transition system.

Further, we give the proof for a network composed of two nonempty subnetworks. Here we consider the situation in which the head normal form of both subnetworks are in the first type of guarded choice, the proof of others are similar. Assume

$$\mathcal{HF}(N_1\langle T, t\rangle) = ([]_{i\in I}\{\mathbf{out}\langle e_i\rangle@s_i \to (M_i\langle T_i, t_i\rangle)\} \,[]\, []_{j\in J}\{\langle v_j\rangle@s_j \to (W_j\langle T_j, t_j\rangle)\}\langle T, t\rangle)$$

$$\mathcal{HF}(N_2\langle T, t\rangle) = ([]_{k\in K}\{\mathbf{out}\langle e_k\rangle@s_k \to (U_k\langle T_k, t_k\rangle)\}[][]_{o\in O}\{\langle v_o\rangle@s_o \to (V_o\langle T_o, t_o\rangle)\}\langle T, t\rangle)$$

According to the derivation strategy, N_1 can perform transitions as following:

$$\langle N_1, \sigma_{N_1}, T, t\rangle \xrightarrow[s_i]{\mathbf{out}\langle e_i\rangle} \langle M_i, \sigma_{N_1}, T_i, t_i\rangle, \quad \langle N_1, \sigma_{N_1}, T, t\rangle \xrightarrow[s_j]{\langle v_j\rangle} \langle W_j, \sigma_{N_1}, T_j, t_j\rangle$$

N_2 can perform transitions as following:

$$\langle N_2, \sigma_{N_2}, T, t\rangle \xrightarrow[s_k]{\mathbf{out}\langle e_k\rangle} \langle U_k, \sigma_{N_2}, T_k, t_k\rangle, \quad \langle N_2, \sigma_{N_2}, T, t\rangle \xrightarrow[s_o]{\langle v_o\rangle} \langle V_o, \sigma_{N_2}, T_o, t_o\rangle$$

The head normal form of $N_1|N_2$ can be achieved by applying expansion law (par-1) and the result is shown as below.

$$\begin{aligned}&\mathcal{HF}(N_1|N_2\langle T, t\rangle)\\ &= ([]_{i\in I}\{\mathbf{out}\langle e_i\rangle@s_i \to (M_i|N_2\langle T_i, t_i\rangle)\}[]\,[]_{j\in J}\,\{\langle v_j\rangle@s_j \to (W_j|N_2\langle T_j, t_j\rangle)\}[]\\ &\quad []_{k\in K}\{\mathbf{out}\langle e_k\rangle@s_k \to (N_1|U_k\langle T_k, t_k\rangle)\}[]\,[]_{o\in O}\,\{\langle v_o\rangle@s_o \to (N_1|V_o\langle T_o, t_o\rangle)\}\langle T, t\rangle)\end{aligned}$$

According to the derivation strategy, $N_1|N_2$ can perform transitions as below:

$$\langle N_1|N_2,\sigma,T,t\rangle \xrightarrow[s_i]{\mathbf{out}\langle e_i\rangle} \langle M_i|N_2,\sigma,T_i,t_i\rangle,\ \ \langle N_1|N_2,\sigma,T,t\rangle \xrightarrow[s_j]{\langle v_j\rangle} \langle W_j|N_2,\sigma,T_j,t_j\rangle$$

$$\langle N_1|N_2,\sigma,T,t\rangle \xrightarrow[s_k]{\mathbf{out}\langle e_k\rangle} \langle N_1|U_k,\sigma,T_k,t_k\rangle,\ \ \langle N_1|N_2,\sigma,T,t\rangle \xrightarrow[s_o]{\langle v_o\rangle} \langle N_1|V_o,\sigma,T_o,t_o\rangle$$

These transitions also exist in the transition system and can be directly proved by applying the first rule in Theorem 5.5. □

6 Mechanical Approach to Linking Algebraic Semantics and Operational Semantics

In this section, we apply the mechanical method to link the algebraic semantics and the operational semantics for wireless systems by using the equational and rewriting logic system Maude [1].

6.1 Mechanizing Algebraic Semantics and Head Normal Form

To mechanize the algebraic semantics and the head normal form, we implement guarded components $\mathbf{out}\langle e\rangle@s$ as `Guard1` and $\langle v\rangle@s$ as `Guard2` respectively in Maude. Similarly, $\mathbf{in}(x)@s$, $(x)@s$ and **idle** are implemented as `Guard3`, `Guard4` and `Guard5` respectively. Then different kinds of guarded components are implemented according to the type of guards. All the guarded components are declared as type `GComponent`. Below is the declarations of guarded components in Maude.

```
subsort GComp1 GComp2 GComp3 GComp4 GComp5 < GComponent .
subsort Guard1 Guard2 Guard3 Guard4 Guard5 < GuardPrefix .
op `(_<_,_>`) : Network Act Tag -> GuardPostfix [ctor] .
op _->>_ : GuardPrefix GuardPostfix -> GComponent [ctor] .
op _->>_ : Guard1 GuardPostfix -> GComp1 [ctor] .
...
op _->>_ : Guard5 GuardPostfix -> GComp5 [ctor] .
```

Based on the five kinds of guarded components, we can define the guarded choice (i.e., `GChoice`) by implementing guarded component as its element.

```
subsort SelectGChoice < GChoice .
op {_} : GComponent -> GChoice [ctor] .
op {_} : GComp1 -> SelectGChoice [ctor] .
op {_} : GComp2 -> SelectGChoice [ctor] .
op _[]_ : SelectGChoice SelectGChoice -> SelectGChoice [ctor] .
```

In above definitions, `SelectGChoice` is the implementation of the first type of guarded choice, which is declared as a subsort of `GChoice`. It is composed of `GComp1` and `GComp2` separated by `[]`. Definitions of other types of guarded choices are similar.

The head normal form is declared as equations using the keyword `eq` (or `ceq` for conditional one) in Maude. We use `HF(N<T,t>)` to represent the head normal form $\mathcal{HF}(N\langle T,t\rangle)$ introduced in section 4.

```
eq HF(n[<v>.P](l,r,c)<T,none>) =
    ({<v>@(l,r,c)->>(n[P](l,r,c)<T\(l,r,c),<v>@(l,r,c)>)}<T,none>) .
ceq HF(n[<v>.P](l,r,c)<T,out<f>@s>) =
    ({idle->>(n[<v>.P](l,r,c)<T,none>)}<T,out<f>@s>) if t=/=none .
```

Above are the declarations of the head normal form of an active transmitter with different types of transmission tags. They are expressed in perfect accordance with the head normal form definition (2-1) and (2-2) respectively.

For parallel composition of networks, the head normal form is calculated by using parallel expansion laws according to the type of guarded choice of each parallel branch. Below is the case where the head normal form of both branches are of the first type of guarded choice.

```
ceq HF(M|N<T,t>) = (comp1(M-Select,N)[]comp2(N-Select,M)<T,t>)
    if (M-Select<T,t>) := HF(M<T,t>)/\(N-Select<T,t>) := HF(N<T,t>) .
```

The head normal form of `M` and `N` with network status `<T,t>` are expressed as `M-Select` and `N-Select` respectively. Both of them are transmission selection guarded choice. Hence, the head normal form is calculated by using parallel expansion law (par-1) as `comp1(M-Select,N)[]comp2(N-Select,M)`, where `comp1(M-Select,N)` indicates that node in M is scheduled.

Example 6.1 Let Net be the network in Example 2.2. The head normal of this network under the network status $\langle \emptyset, none \rangle$ is calculated in Maude by using the command `reduce` as below, which shows the two possible choices of its first transition step.

```
reduce in NORMAL-FORM :
   (  {out<e>@(l1,r1,c)->>(n1[<[[e]]>.P](l1,r1,c)|n2[out<f>.Q](l2,r2,c)|
                    n3[in(x).R](l3,r3,c)|n4[in(y).S](l4,r4,c)<(l1,r1,c),out<e>@(l1,r1,c)>)}

    []{out<f>@(l2,r2,c)->>(n1[out<e>.P](l1,r1,c)|n2[<[[f]]>.Q](l2,r2,c)|
                    n3[in(x).R](l3,r3,c)|n4[in(y).S](l4,r4,c)<(l2,r2,c),out<f>@(l2,r2,c)>)}
      <empty,none> )
```

6.2 Mechanizing the Derivation of Operational Semantics from Algebraic Semantics

The derivation strategy is declared as rules by keyword `crl` (i.e., conditional rule). Each rule is defined as a transition of configurations based on the head normal form. We give the declaration of the item (1.a) in Definition 5.1 below.

```
crl [1.a]:.<N,env,T,none> => <Ni,env,T U s,out<e>@s>
  if (hgc-sl<T,none>):=HF(N<T,none>)/\(hgc[]
  {out<e>@s->>(Ni<T U s,out<e>@s>)}[]hgc'<T,none>):=(hgc-sl<T,none>) .
```

From the condition of this rule, we know that the head normal form of `N` under the network status `<T,none>` is `hgc-sl` and `hgc-sl` has a component `out<e>@s->> (Ni<T U s,out<e>@s>)`. Hence, the network can perform a transition reflecting that the transmitter `s` is scheduled to start a transmission and the active transmitters set is updated from `T` to `T U s`.

Example 6.2 We use the network Net in Example 2.2 to illustrate the effectiveness of our derivation strategy. Assume that the initial network status is `<empty,none>`. We use the command `search` to generate its transitions in Maude. And one of the transition paths is shown below.

```
    < n1[out<e>.P](l1,r1,c)|n2[out<f>.Q](l2,r2,c)|n3[in(x).R](l3,r3,c)|n4[in(y).S](l4,r4,c),
      init,empty,none >
==> < n1[out<e>.P](l1,r1,c)|n2[<[[f]]>.Q](l2,r2,c)|n3[(x).R](l3,r3,c)|n4[(y).S](l4,r4,c),
      init,(l2,r2,c),none >
==> < n1[<[[e]]>.P](l1,r1,c)|n2[<[[f]]>.Q](l2,r2,c)|n3[R](l3,r3,c)|n4[(y).S](l4,r4,c),
      (x,interf),(l1,r1,c)U(l2,r2,c),none >
==> < n1[<[[e]]>.P](l1,r1,c)|n2[Q](l2,r2,c)|n3[R](l3,r3,c)|n4[S](l4,r4,c),
      (x,interf)u(y,[[f]]),(l1,r1,c),none >
```

Initially, the state of variables is set to the initial state `init`. According to the head normal of this network shown in Example 6.1, N_1 and N_2 can start their transmissions. After N_2 begins its transmission, a collision occurs in N_3 caused by N_1 and a special value `interf` (stands for $\perp$) is bound to `x`. When N_2 finishes its broadcast transmission, N_4 receives the value `[[f]]` successfully by updating the state of variable `y` to `[[f]]`.

6.3 Mechanizing the Derived Operational Semantics

This section is devoted to mechanize the derived operational semantics. The operational semantics is declared by rules or conditional rules. We can implement transition rules in Theorem 5.1 to Theorem 5.5 into Maude system directly. We use the first transition in Theorem 5.5 (with β in the form of $\mathbf{out}\langle e\rangle$) to illustrate the mechanization as below. Others are similar.

```
crl[Theorem5.5-1.1]:.<M|N,env,T,none> => <M'|N,env,T',out<e>@s>
          if .<M,env,T,none> => <M',env,T',out<e>@s> .
crl[Theorem5.5-1.2]:.<M|N,env,T,none> => <M|N',env,T',out<e>@s>
          if .<N,env,T,none> => <N',env,T',out<e>@s> .
```

From the conditions of the two rules, we know that one parallel branch can perform a begin transmission transition. Hence, the two rules show that the whole network can also perform the begin transmission transition regardless of another branch.

Consider the network Net in Example 2.2 again. Its transitions can be generated in Maude by applying the transition rules of the derived operational semantics directly. The generated transitions are exactly the same as those generated by using derivation strategy in Example 6.2 in the previous subsection. This result supports the claim of the equivalence between the derivation strategy and the derived transition system.

7 Conclusion

In this paper we have explored the linking theories between the algebraic semantics and the operational semantics of CWS. This approach starts from the algebraic laws. Our consideration is to derive the operational semantics from the algebraic semantics.

Our approach is new to a calculus of wireless systems. We first introduced the algebraic laws based on four typical forms of guarded choices and gave the parallel expansion laws. Then we defined the head normal form and presented the derivation strategy for deriving the operational semantics from the algebraic semantics. Finally an operational semantics was derived. This exploration shows the soundness of the operational semantics with respect to the algebraic semantics. Further, the equivalence between the derivation strategy and the derived operational semantics is investigated, which shows the completeness of the operational semantics from the viewpoint of the algebraic semantics. We also

mechanized the linking between the algebraic semantics and the operational semantics. The mechanical results support that the derived operational semantics is the same as the derivation strategy.

For the future, we are continuing to explore the semantics and the unifying theories for wireless systems. The denotational semantics and the deduction method [3] for wireless systems are very challenging.

Acknowledgement This work was partly supported by the Danish National Research Foundation and the National Natural Science Foundation of China (Grant No. 61061130541) for the Danish-Chinese Center for Cyber Physical Systems. And, it is also supported by National Basic Research Program of China (Grant No. 2011CB302904), National High Technology Research and Development Program of China (Grant Nos. 2011AA010101 and 2012AA011205), National Natural Science Foundation of China (Grant Nos. 61021004 and 91118008), Shanghai STCSM Project (No. 12511504205), and Shanghai Knowledge Service Platform Project (No. ZF1213).

References

1. Clavel, M., Durán, F., Eker, S., Lincoln, P., Martí-Oliet, N., Meseguer, J., Talcott, C. L.: The Maude 2.0 System. RTA 2003. LNCS, Vol. 2706, pp. 76–87. Springer, Berlin (2003)
2. Godskesen, J. C.: A Calculus for Mobile Ad Hoc Networks. COORDINATION 2007, pp. 132–150 (2007)
3. Hoare, C. A. R.: Algebra of Concurrent Programming. In Meeting 52 of WG 2.3 (2011)
4. Hoare, C. A. R., He, J.: Unifying Theories of Programming. Prentice Hall International Series in Computer Science. (1998)
5. Hoare, C. A. R., Hayes, I. J., He, J., Morgan, C. C., Roscoe, A. W., Sanders, J. W., Sorenson, I. H., Spivey, J. M., Sufrin, B. A.: Laws of Programming. Commun. ACM 30(8), pp. 672–686 (1987)
6. Lanese, I., Sangiorgi, D.: An Operational Semantics for a Calculus for Wireless Systems. Theor. Comput. Sci. 411(19), pp. 1928–1948 (2010)
7. Merro, M.: An Observational Theory for Mobile Ad Hoc Networks (full version). Inf. Comput. 207(2), pp. 194–208 (2009)
8. Mezzetti, N., Sangiorgi, D.: Towards a Calculus for Wireless Systems. Electr. Notes Theor. Comput. Sci. Vol. 158, pp. 331–353 (2006)
9. Nanz, S., Hankin, C.: A Framework for Security Analysis of Mobile Wireless Network. Theor. Comput. Sci. 367(1-2), pp. 203–227 (2006)
10. Ostrovsky, K., Prasad, K. V. S., Taha, W.: Towards a Primitive Higher Order Calculus of Broadcasting Systems. PPDP2002, pp. 2–13 (2002)
11. Plotkin, G.: A Structural Approach to Operational Semantics. J. Log. Algebr. Program. Vol. 60–61, pp. 17–139 (2004)
12. Prasad, K. V. S.: A Calculus of Broadcasting Systems. Sci. Comput. Program. 25(2–3), pp. 285–327 (1995)
13. Scott, D., Strachey, C.: Toward a Mathematical Semantics for Computer Languages. Technical report PRG-6, Oxford University Computer Laboratory (1971)