

$$SegmentModification(n) \triangleq \\ \wedge nState[n] = N\_Modification$$

$\wedge$  LET  
 $p \triangleq \text{Head}(n\text{Buffer}[n])$   
 $et \triangleq \text{CHOOSE } x \in \text{NormalTxTime} : \text{TRUE}$   
 $np \triangleq [p \text{ EXCEPT } !.isrc = n, !.idst = RT[p.dst],$   
 $!.elapsed = @ + et, !.data = @ + \text{PacketMod}]$   
 IN  $\text{Send}(np)$   
 $\wedge n\text{Buffer}' = [n\text{Buffer} \text{ EXCEPT } ![n] = \text{Tail}(@)]$   
 $\wedge n\text{State}' = [n\text{State} \text{ EXCEPT } ![n] = N\_Wait]$   
 $\wedge \text{UNCHANGED } \langle \text{genVars}, \text{receiverVars}, \text{watchdogVars},$   
 $\text{blockchainVars} \rangle$

$\text{ReceiverRecv}(r) \triangleq$   
 $\wedge r\text{State}[r] = R\_Wait$   
 $\wedge \exists p \in \text{channel} :$   
 $\wedge p.idst = r$   
 $\wedge \text{Receive}(p)$   
 $\wedge r\text{Buffer}' = [r\text{Buffer} \text{ EXCEPT } ![r] = \text{Append}(@, p)]$   
 $\wedge \text{Transfer}(r, p.id, RToken, 1, \text{GetFingerprint}(p))$   
 $\wedge \text{UNCHANGED } \langle \text{genVars}, \text{nodeVars}, r\text{State}, \text{watchdogVars}, \text{txBlock},$   
 $\text{balance}, \text{malicious}, \text{benign}, fPrint, \text{malPackets} \rangle$

$\text{ReliableDelivery}(p1, p2) \triangleq$   
 $\wedge p2.elapsed - p1.elapsed \in \text{NormalTxTime}$   
 $\wedge p1.data = p2.data$

$\text{IsPacketSeenFirst}(p) \triangleq$   
 $\wedge \exists w \in \text{Watchdog} : p \in w\text{Buffer}[w]$   
 $\wedge \forall n \in \text{Segment} : p \notin \{n\text{Buffer}[n][np] : np \in \text{DOMAIN } n\text{Buffer}[n]\}$

$\text{WatchdogSeen}(w) \triangleq$   
 $\exists p \in \text{channel} :$   
 $\wedge w\text{State}[w] = W\_Working$   
 $\wedge p \notin w\text{Processed}[w]$   
 $\wedge (p.isrc \in \text{Coverage}[w] \vee p.idst \in \text{Coverage}[w])$   
 $\wedge w\text{Buffer}' = [w\text{Buffer} \text{ EXCEPT } ![w] = @ \cup \{p\}]$   
 $\wedge \text{IF } \text{IsPacketSeenFirst}(p)$   
 $\text{THEN } \text{firstSeen}' = \text{firstSeen} \cup \{p\} \text{ ELSE UNCHANGED } \text{firstSeen}$   
 $\wedge \text{UNCHANGED } \langle \text{genVars}, \text{nodeVars}, \text{commVars}, \text{receiverVars},$   
 $w\text{State}, w\text{Processed}, \text{blockchainVars} \rangle$

$\text{WatchdogCheck}(w) \triangleq$   
 $\exists p1 \in w\text{Buffer}[w] : \exists p2 \in w\text{Buffer}[w] :$   
 $\wedge p1 \neq p2$   
 $\wedge p1.idst = p2.isrc$   
 $\wedge \text{ReliableDelivery}(p1, p2)$   
 $\wedge \text{Transfer}(w, p1.idst, RToken, 1, \text{GetFingerprint}(p2))$   
 $\wedge w\text{Buffer}' = [w\text{Buffer} \text{ EXCEPT } ![w] = @ \setminus \{p1, p2\}]$   
 $\wedge w\text{Processed}' = [w\text{Processed} \text{ EXCEPT } ![w] = @ \cup \{p1, p2\}]$   
 $\wedge \text{UNCHANGED } \langle \text{genVars}, \text{nodeVars}, \text{commVars}, \text{receiverVars},$   
 $\text{firstSeen}, w\text{State}, \text{txBlock}, \text{balance}, \text{malicious}, \text{benign},$   
 $fPrint, \text{malPackets} \rangle$

$\text{WatchdogReview}(w) \triangleq$   
 $\exists p \in w\text{Buffer}[w] :$   
 $\wedge \text{IF } p.idst \in \text{Segment}$   
 $\text{THEN } \text{Transfer}(w, p.idst, PToken, 1, \text{GetFingerprint}(p))$   
 $\text{ELSE UNCHANGED } \text{txPool}$   
 $\wedge w\text{Buffer}' = [w\text{Buffer} \text{ EXCEPT } ![w] = @ \setminus \{p\}]$   
 $\wedge w\text{Processed}' = [w\text{Processed} \text{ EXCEPT } ![w] = @ \cup \{p\}]$   
 $\wedge \text{UNCHANGED } \langle \text{genVars}, \text{nodeVars}, \text{commVars}, \text{receiverVars},$   
 $\text{firstSeen}, w\text{State}, \text{txBlock}, \text{balance}, \text{malicious}, \text{benign},$   
 $fPrint, \text{malPackets} \rangle$

$\text{DecideMalicious}(n) \triangleq \text{malicious}' = \text{malicious} \cup \{n\}$   
 $\text{DecideBenign}(n) \triangleq \text{benign}' = \text{benign} \cup \{n\}$

Return FALSE if the node is malicious

$\text{JudgeDecision}(n) \triangleq$   
 LET  $\text{score} \triangleq \text{InitialBalance} - \text{balance}[n][PToken]$   
 IN  
 $\wedge (\text{score} \geq 0)$

$\text{IntegrityCheck}(fp) \triangleq$   
 LET  $id \triangleq fp[1]$   $dst \triangleq fp[2]$   $pfp \triangleq fp[3]$   
 $\text{storedFp} \triangleq fPrint[id, dst]$  IN  
 $\text{storedFp} \neq \{\} \Rightarrow pfp \in \text{storedFp}$

RECURSIVE  $\text{SumToken}(-, -, -)$   
 $\text{SumToken}(f, S, t) \triangleq$   
 IF  $S = \{\}$  THEN 0 ELSE  
 LET  $x \triangleq \text{CHOOSE } x \in S : \text{TRUE}$   
 IN  $f[x][t] + \text{SumToken}(f, S \setminus \{x\}, t)$

$\text{EvaluatorReview}(e, ty) \triangleq$   
 $\wedge \text{LET } t\text{Total} \triangleq \text{SumToken}(\text{balance}, \text{Evaluator}, ty)$  IN  
 IF  $(2 * \text{balance}[e][ty] * \text{Cardinality}(\text{Evaluator}) < t\text{Total})$

THEN  $\text{balance}' = [\text{balance} \text{ EXCEPT}$   
 $![e] = [@ \text{ EXCEPT } ![ty] = @ + \text{RegenTokenMin}]$   
 ELSE  $\text{balance}' = [\text{balance} \text{ EXCEPT}$   
 $![e] = [@ \text{ EXCEPT } ![ty] = @ + 2 * \text{RegenTokenMin}]$

$\text{ConfirmTx} \triangleq$   
 $\exists tx \in \text{txPool} :$   
 $\wedge \text{txPool}' = \text{txPool} \setminus \{tx\}$   
 $\wedge \text{IF } \text{CheckBalance}(tx.from, tx.token, tx.value) \text{ THEN}$   
 LET  $e \triangleq tx.from$   $n \triangleq tx.to$  IN  
 $\wedge \text{txBlock}' = \text{txBlock} \cup \{tx\}$   
 $\wedge \text{balance}' = [\text{balance} \text{ EXCEPT}$   
 $![e] = [@ \text{ EXCEPT } ![tx.token] = @ - tx.value],$   
 $![n] = [@ \text{ EXCEPT } ![tx.token] = @ + tx.value]$  ]  
 $\wedge \text{LET } id \triangleq tx.fingerprint[1]$   $dst \triangleq tx.fingerprint[2]$   
 $sfp \triangleq tx.fingerprint[3]$  IN  
 IF  $fPrint[id, dst] = \{\}$   
 THEN  $fPrint' = [fPrint \text{ EXCEPT } ![id, dst] = \{sfp\}]$   
 ELSE UNCHANGED  $fPrint$   
 $\wedge \text{IF } n \in \text{Segment} \cup \text{PacketObject} \Rightarrow \wedge \text{JudgeDecision}(n)$   
 $\wedge \text{IntegrityCheck}(tx.fingerprint)$   
 THEN  $\text{DecideBenign}(n) \wedge \text{UNCHANGED } \langle \text{malicious}, \text{malPackets} \rangle$   
 ELSE  $\wedge \text{DecideMalicious}(n)$   
 $\wedge \text{malPackets}' = \text{malPackets} \cup \{tx.fingerprint[1]\}$   
 $\wedge \text{UNCHANGED } \text{benign}$   
 $\wedge e \in \text{Evaluator}$   
 $\wedge \text{balance}[e][tx.token] \leq \text{TokenMin}$   
 $\Rightarrow \text{EvaluatorReview}(e, tx.token)$   
 ELSE UNCHANGED  $\langle \text{txBlock}, \text{balance} \rangle$   
 $\wedge \text{UNCHANGED } \langle \text{genVars}, \text{nodeVars}, \text{commVars}, \text{receiverVars},$   
 $\text{watchdogVars} \rangle$

$\text{SuccessfullyDelivered} \triangleq$   
 $\wedge \forall r \in \text{Receiver} :$   
 $\forall p \in \{r\text{Buffer}[r][x] : x \in \text{DOMAIN } r\text{Buffer}[r]\} :$   
 $\vee \text{checksum}[p.cksum] = \langle r, p.data \rangle$   
 $\wedge \forall \text{sentPacket} \in \text{PreGenPackets} :$   
 $\exists r \in \text{Receiver} :$   
 $\text{sentPacket.payload} \in$   
 $\{r\text{Buffer}[r][x].data : x \in \text{DOMAIN } r\text{Buffer}[r]\}$

$\text{AllDelivered} \triangleq$   
 $\wedge \forall r \in \text{Receiver} :$   
 $\forall p \in \{r\text{Buffer}[r][x] : x \in \text{DOMAIN } r\text{Buffer}[r]\} :$   
 $\vee \text{checksum}[p.cksum] = \langle r, p.data \rangle$   
 $\vee \text{checksum}[p.cksum] = \langle r, p.data - \text{PacketMod} \rangle$   
 $\wedge \forall \text{sentPacket} \in \text{PreGenPackets} :$   
 $\exists r \in \text{Receiver} :$   
 $\text{sentPacket.payload} \in$   
 $\{r\text{Buffer}[r][x].data : x \in \text{DOMAIN } r\text{Buffer}[r]\} \cup$   
 $\{r\text{Buffer}[r][x].data - \text{PacketMod} : x \in \text{DOMAIN } r\text{Buffer}[r]\}$

$\text{AllProcessed} \triangleq$   
 $\wedge \text{pendingPackets} = \{\}$   
 $\wedge \forall n \in \text{Segment} : n\text{Buffer}[n] = \{\}$   
 $\wedge \text{channel} = \{\}$

$\text{IsSecurelyDelivered}(p) \triangleq$   
 $\exists r \in \text{Receiver} :$   
 $\langle p.id, p.data \rangle \in$   
 $\{\langle r\text{Buffer}[r][rp].id, r\text{Buffer}[r][rp].data \rangle : rp \in \text{DOMAIN } r\text{Buffer}[r]\}$

$\text{WorkingProperly} \triangleq$   
 $\forall p \in \text{sentPackets} :$   
 $\text{IsPacketSeenFirst}(p) \rightsquigarrow \vee p.id \in \text{malPackets}$   
 $\vee \text{IsSecurelyDelivered}(p)$

$\text{Termination} \triangleq$   
 $\wedge \text{txPool} = \{\}$   
 $\wedge \forall w \in \text{Watchdog} : w\text{Buffer}[w] = \{\}$   
 $\wedge \text{AllProcessed}$   
 $\wedge \forall r \in \text{Receiver} : r\text{State}[r] = R\_Wait$   
 $\wedge \forall p \in \text{firstSeen} : p.id \in \text{malPackets} \vee \text{IsSecurelyDelivered}(p)$   
 $\wedge \text{UNCHANGED vars}$

$\text{TokenBalance} \triangleq$   
 LET  $\text{totalBalance} \triangleq \text{InitialBalance} * \text{Cardinality}(\text{Participant})$   
 IN  $\text{Sum}(\text{balance}, \text{DOMAIN } \text{balance}) = \text{totalBalance}$

$\text{Delivered} \triangleq$   
 $\forall p \in \text{sentPackets} :$   
 ENABLED  $\text{IsPacketSeenFirst}(p) \Rightarrow \text{IsSecurelyDelivered}(p)$

$\text{Next} \triangleq$

$\vee \textit{PacketGen}$   
 $\vee \exists n \in \textit{Segment} : \textit{SegmentRecv}(n) \vee \textit{SegmentNormalSend}(n)$   
 $\vee \textit{SegmentPacketDrop}(n) \vee \textit{SegmentModification}(n) \vee \textit{SegmentOnOffForwarding}(n)$   
 $\vee \exists r \in \textit{Receiver} : \textit{ReceiverRecv}(r)$   
 $\vee \exists w \in \textit{Watchdog} : \textit{WatchdogSeen}(w) \vee \textit{WatchdogCheck}(w)$   
 $\vee (\textit{AllProcessed} \wedge \exists w \in \textit{Watchdog} :$   
 $\quad \textit{wBuffer}[w] \neq \{\} \wedge \textit{WatchdogReview}(w))$   
 $\vee \textit{ConfirmTx}$   
 $\vee \textit{Termination}$

$\textit{Spec} \triangleq \textit{Init} \wedge \Box[\textit{Next}]_{\textit{vars}}$