

Formal verification of protocol specified in LTS for railway signalling systems

J.-H. Lee¹, J.-G. Hwang¹, Y.-G. Yoon¹ & G.-T. Park²

¹*Railway Signalling Research Group,
Korea Railroad Research Institute (KRRRI), Korea*

²*Dept. of Electrical Engineering, Korea University, Korea*

Abstract

According to the computerization of railway signalling systems, the interface link between the signalling systems has been replaced by the digital communication channel. At the same time, the importance of the communication link is more pronounced than in the past. In this research, a new standard communication protocol for Korean railway signalling has been designed and the overview of the designed protocol and the results of performance analyses are briefly represented in this paper. Using the informal method for specifying the communication protocol, a little ambiguity may be contained in the protocol. To clear the ambiguity contained in the designed protocol, we apply a formal method to the designed protocol and verify the safety and liveness properties with the model checking method. It will be expected to increase the safety, reliability and efficiency of maintenance of the signalling systems by using the designed protocol for railway signalling in Korea

1 Introduction

A few years ago, most of the signalling equipment consisted of vital relay-based systems ensure the safety of railway control systems. However, according to the computerization of railway signalling systems, lots of information is exchanged among the computerized railway signalling systems. By the systemization of railway signalling systems, the communication link is considered more significant than before. Therefore, the communication protocol has to be clearly defined and standardized for the systemized and intelligent railway signalling systems.



However, there are some problems with the railway signalling systems in Korea. First, the existing communication protocol for railway signalling has a different protocol that is applied to interfacing between signalling systems although the protocols have identical functions. It is unavoidable that disparate protocols have been introduced by different manufacturers. Therefore, there are difficulties in maintaining signalling communication equipment. The other is that the existing protocols currently used in the railway field have some illogical parts such as structure, byte formation, error correction scheme, etc. To solve these problems, essentially requires a standard communication protocol with high reliability. To overcome these problems, a new protocol for Korean railway signalling systems has designed and standardized in our research. The performance of data link control protocols for railway signalling systems is to analyze and designed protocol is more improved than existing protocols by these simulated results [1].

It is expected that the communication protocols designed by experts could have brought about some ambiguities. Provided that there were some ambiguities in the designed protocol by the experts, and that the protocols were applied to vital railway signalling systems, the ambiguities might provoke fatal flaws in the control of signalling systems or accidents. Therefore, the communication protocol for vital systems like railway signalling systems has to be correctly verified by the formal method [3]. For our research, we use LTS(Labeled Transition System) to design the communication protocol for railway signalling, LTS is an intermediate model for encoding the operational behavior of processes. And then, we verify automatically and formally the safety and liveness properties through the model checking method [4][5].

2 Review of the conventional protocols

Among many kinds of KNR(Korean National Railroad) signalling systems, we review the LDTS(Local Data Transmission System), and EIS(Electronic Interlocking System), which are representative ones of signalling systems at the KNR. LDTS equipment is located in the signalling systems room and it receives the control commands from the centralized railway signalling system for the control of the field signalling equipment such as EIS, point machines, signals, etc., then LDTS sends the commands to EIS. The LDTS equipment is collecting the state information of field signalling equipment, and then LDTS also sends these collected data to the central signalling equipment. LDTS acts as a hub link between the central control centre and local signalling facility, so the communication link is very important to railway signalling systems in Korea. Therefore, the interface link is significant from the point of view of safe railway signalling operation. Figure 1 shows the configuration of railway signalling systems for KNR.

Several protocols are used for the above-mentioned link between LDTS and EIS in Korea. One of them, the I/O protocol is widely used in Korea. Therefore, it is only concentrated on the I/O protocol among several existing protocols.



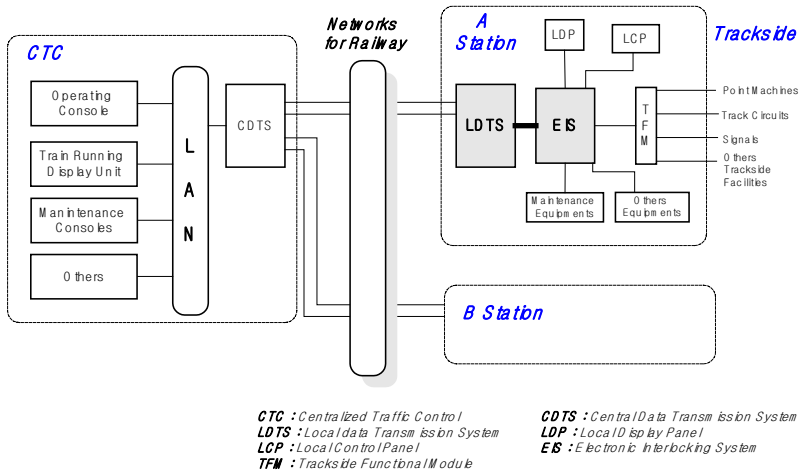


Figure 1: Configuration of railway signalling systems.

We have found some drawbacks in the I/O protocol. First, the byte formation is differs from the generic byte formation. One byte generally consists of 8 bits but one byte in an existing protocol is composed of 9 bits. The reason for this is that at the time it was developed, the Korean computing systems were able to support 9 bits of byte formation efficiently, so it did not have to use an 8-bit formation only. So, the I/O is referred to as a 9th communication protocol in the Korea railway fields. However, the computer life cycle is too rapid to catch an efficient but isolated computing system like 9 bits byte formation. Therefore, a generic 8 bits byte formation should be accepted in the standardization of protocol.

Another drawback in the I/O protocol is the existence of the 'Destination and Source Type/ID' field. In a point-to-point communication protocol, there is no need for these unusual fields to use transmission message format in a practical sense. This malformation for the transmission of message frames is inheritance that existing protocols acquired when they didn't convert to a new protocol when conventional electric interlocking equipment, communicating a multi-drop type to the I/O board, allows it to be replaced by new electronic equipment. More information for these drawbacks of existing protocol has described in [1].

3 New designed communication protocol

As the above-mentioned introduction section indicated, the present state of communication protocols for Korean railway signalling systems does contains critical defects. But the new protocol is not expected to have these problems, and it also requires the standardization of the designed protocol to improve the operation and maintenance ability. The performance of data link control protocol for railway signalling is analyzed by simulation. In this section, the designed protocol for railway signalling will be described concisely.



The designed protocol has an advanced structure and mechanism thereby removing drawbacks of the existing protocol. Furthermore, the protocol is able to be more accurate in terms of communication by a combination of the ‘STX’ and ‘ETX’ fields. These added fields provide the same role as the existing 9th scheme. The ‘STX’ field means the start of the transmission frame, and the ‘ETX’ represents the end of one. Also, the uncommon frame format of the conventional one, ‘Destination and Source Type/ID’ has been removed at the design protocol stage.

To improve the error detection performance during the transmission of the message frame, the BCC error detection code has been transferred to the CRC 16 error detection code. The application of this error detection code is expected to contribute to the decrease of the frame error rate during communication. The simulated results for those will be represented in the next section. The designed transmission message format is as follows:

Table 1: Message format.

STX	Data Length	Sequence No.	Message Type	Data	CRC	ETX
1 byte	1 byte	1 byte	1 byte	N byte	2 byte	1 byte

Where

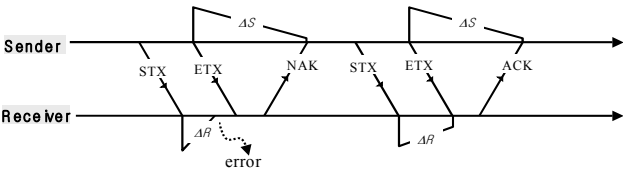
STX: start of frame,
Data Length : message length from Sequence Number to ETX (maximum 255 bytes),
Sequence Number : 0x00 ~ 0xFF,
Message Type : transmitted message types
Data : variables according to information.
CRC : CRC-16 : $X^{16} + X^{15} + X^2 + 1$
ETX : end of frame

The SAW ARQ scheme is applied to the designed protocol. An error detection code based on the CRC 16 code and the ‘ACK/NAK’ control message are used for the ARQ scheme. And a message must be retransmitted in case of error detection. The following is a description of the retransmission mechanism.

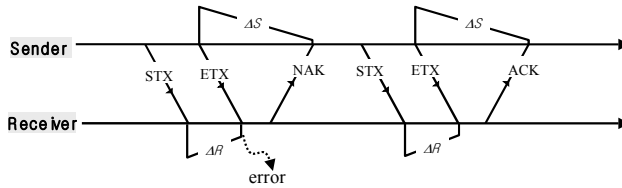
(a) If the following cases occurred to a sender, the same message must be retransmitted to the receiver up to a maximum of 3 times.

① Reception of ‘NAK’ message at sender

Case I: Error detection in transmission frame by error detection code, fault of sequence number at receiver (‘NAK’ message transmission to sender)



Case II: No reception of 'ETX' message at receiver in spite of expiration of receiver timer setting time ΔR ('NAK' message transmission to sender)



- ② If the sender could not receive any response message from the communication receiver such as 'ACK' or NAK, even though the sender timer was expired, the previous message is retransmitted to the receiver.

- (b) If the sender did not receive any response from the receiver even though the identical message was sent 3 times, the sender might regard it as a communication link error. Therefore, the sender discards the transmission message and a link error process is executed. Then the sender periodically transmits a polling message with 0x00 sequence number to the receiver for the identification of link restoration.

4 Performance analysis results

To verify the designed protocol performance concerned with data link control, the simulation is performed on existing and designed protocols under the same conditions. The performance of data link control is simulated based on the developed simulation tool in Figure 2, and frame error probability and link throughput are considered as a performance metric. This simulation tool has developed for performance analysis of data link protocol in our research. Table 2 shows the simulation conditions for the comparative performance analysis.

With parameters shown in Table 1, the simulation shows the performance characteristics of the designed protocol. Figure 3(a) shows the frame error probability characteristics through the designed communication protocol and the existing one. Comparison of the results indicates that the frame error performance of the designed protocol is superior to the conventional one. Figure 3(b) shows the link throughput characteristics by two protocols, and also the link throughput is greatly improved in the case of the designed protocol than in the existing one. These two figures demonstrate that the designed protocol has good performance by comparison to the conventional protocol. It can be seen that the designed protocol has a good performance in terms of error probability and throughput characteristics.

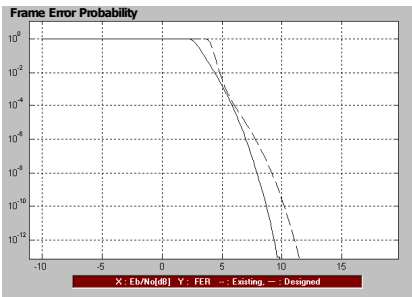




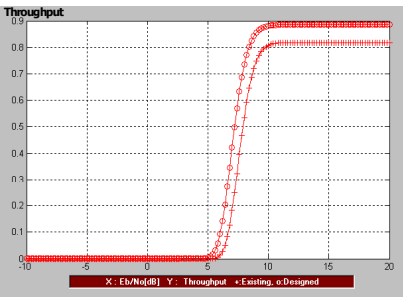
Figure 2: Main window of simulation tool for performance analysis.

Table 2: Simulation conditions.

E_b / N_0	-10 ~ 20 [dB]
Signal type	Bipolar
Data field	100 [Byte]
Physical link distance	100 [m]
Effective noise temperature	27 [°C]
Media propagation speed (copper)	2×10^8 [m/s]
ARQ scheme	SW ARQ



(a) Frame error probability



(b) Throughput

Figure 3: Comparison of data link protocols performance.



5 Verification of designed protocol specified in LTS

It is expected that the communication protocols designed by experts have some ambiguities. Provided that there are some ambiguities in the designed protocol by experts and the protocol is applied to a vital railway signalling system, these may provoke the fatal faults in the control of signalling or accidents. Therefore, the communication protocol for vital systems such as the railway signalling system has to be correctly verified by the formal method.

For our research, we use LTS (Labeled Transition System) to design the protocol for railway signalling, the LTS is an intermediate model for encoding the operational behavior of processes. And then, we verify automatically and formally the safety and the liveness properties through the model checking method. Especially, the modal mu-calculus, which is a highly expressive method of temporal logic that has been applied to the model checking method. Figure 4 also shows the LTS modeling with function model for formal specification.

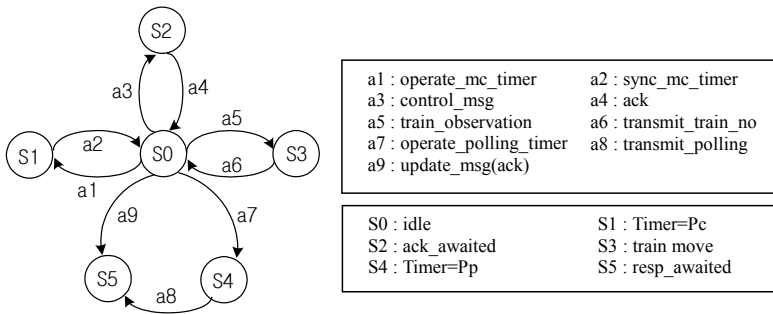


Figure 4: LTS modeling for proposed communication protocol.

5.1 Overview for verifying correctness

As a highly focused part in the development of the protocol, verifications for protocol specification are complementary techniques that are used to increase the level of confidence in the system functions as prescribed by their specifications. That is, it must verify the non-existence of deadlock and livelock states, abnormal reachability, and potential design errors in the designed protocol. The basic approach to verifying whether our designed protocol satisfies a property by using the model-checking concept involves the following steps:

- The communication protocol is expressed as a FSM and a set of labeled transition remarks.
- The protocol to verify is expressed as a LTS model from pre-worked FSM model.



An algorithm, called a model checker, is used to verifying whether the model expressed as a LTS satisfies the properties of correctness. There are two kinds of properties, which are as follows:

- Safety property is the state in which bad states and actions never happen. That is, the system never enters an unacceptable state. Some well-known examples of safety properties in communication protocol are the absence of deadlock or livelock.
- Liveness property is the state in which good states and actions eventually happen. That is, predefined states and actions necessarily take place. This is defined as reachability.

5.2 Modal mu-calculus as a model-checking

Modal mu-calculus of Kozan [4] is a powerful logic for expressing temporal properties by using the least and greatest fixed-point operators that can express the safety and liveness properties of communication protocols. In modal mu-calculus, fomulas consist of atomic propositions, $\wedge$ (conjunction), $\vee$ (disjunction), $[]$ (necessity), $\langle \rangle$ (possibility), ν (greatest fixed point) and μ (least fixed point). And generalized formulas for modal mu-calculus are as follows:

$$\phi ::= tt | ff | Z | \phi_1 \wedge \phi_2 | \phi_1 \vee \phi_2 | [k] \phi | \langle k \rangle \phi | \nu Z. \phi | \mu Z. \phi \quad (1)$$

where

ν and μ : Operators for expression of least and greatest fixed-point, respectively

$\wedge$ and $\vee$: Local connectives

$[]$ and $\langle \rangle$: Modal operators with meaning of necessity and possibility.

ϕ : Formulas for process characteristics.

Safety property is based on the exclusion of deadlock and livelock states, and liveness property is the characteristic of satisfaction of reachability and liveness in communication protocol. If the following modal mu-calculus formulas are true respectively, it means that the safety and liveness characteristics of designed communication protocols have been verified correctly.

- Safety for states : $\nu Z. \phi \wedge [-] Z$
- Safety for behavior : $\nu Z. \phi [k] ff \wedge [-] Z$
- Liveness for states : $\mu Z. \phi \vee (\langle - \rangle tt \wedge [-] Z)$
- Liveness for behavior : $\mu Z. \phi \langle - \rangle tt \wedge [k] Z$

5.3 Verification of designed protocol

In this section, we will verify the designed protocol using the modal mu-calculus formula described to equation (1), which means we will examine the correctness properties of the protocol. For example, the equation (2) modal mu-calculus formula has to be “true”, if the LTS of the designed protocol consists of the non-existence of deadlock and livelock.

$$\nu Z. (\mu Y. A \vee (\langle - \rangle tt \wedge [-] Y)) \wedge [-] Z, A = \{S_0\} \quad (2)$$



The Solve as a model-checking algorithm is applied to this equation (2). From this process the verifying results can be obtained. Figure 5 shows the max and min blocks generated from the equation (2) by using least and greatest fix-points and Figure 6 shows the relation between the variables' transitions described as an edge-labeled directed graph G.

$B_1 \equiv \min \{X_1 = X_2 \vee X_3$ $X_2 = A$ $X_3 = X_4 \wedge X_5$ $X_4 = [-]X_1$ $X_5 = <->X_6$ $X_6 = tt\}$	$B_2 \equiv \max \{X_7 = X_1 \wedge X_8$ $X_8 = [-]X_7\}$
---	--

Figure 5: Max block, min block.

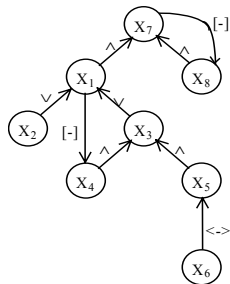


Figure 6: Edge-labeled directed graph G.

Figure 7(a) shows the bit-vector, counter and array, which are initialized by means of the solution algorithm. And Figure 7(b) shows the resulting bit-vector, counter, and array. We can decide the deadlock and livelock properties from the results.

X	X ₁	X ₂	X ₃	X ₄	X ₅	X ₆	X ₇	X ₈
S0	0	1	0	0	0	1	1	1
S1	0	0	0	0	0	1	1	1
S2	0	0	0	0	0	1	1	1
S3	0	0	0	0	0	1	1	1
S4	0	0	0	0	0	1	1	1
S5	0	0	0	0	0	1	1	1

C	X ₃	X ₄
S0	2	4
S1	2	1
S2	2	1
S3	2	1
S4	2	1
S5	2	1

X	X ₁	X ₂	X ₃	X ₄	X ₅	X ₆	X ₇
S0	1	1	1	1	1	1	1
S1	1	0	1	1	1	1	1
S2	1	0	1	1	1	1	1
S3	1	0	1	1	1	1	1
S4	1	0	1	1	1	1	1
S5	1	0	1	1	1	1	1

C	X ₁	X ₂
S0	0	0
S1	0	0
S2	0	0
S3	0	0
S4	0	0
S5	0	0

M[1]=<<S0, X2>, <S0, X6>, <S1, X6>, <S2, X6>, <S3, X6>, <S4, X6>, <S5, X6>>

M[2]=<>

M[1]=<>

M[2]=<>

(a) Initial states

(b) Resulted states

Figure 7: Bit-vector, counter and array M[i].



A deadlock can be detected at components of bit-vector. All bit-vectors from resulted bit-vector, with the exception of component X_2 relate to atomic proposition A, set to '1', so we can find the absence of a deadlock in the LTS model of the designed protocol. Therefore, the livelock property can be detected through the components of the counter. All counters from resulted counter are set to '0', so we can find the absence of livelock in the LTS model. From these results, the above described LTS model for the designed protocol is satisfied with the " $\forall Z. (\mu Y. A \vee (\neg \rightarrow tt \wedge [\neg Y])) \wedge [\neg Z, A=\{S0\}$ " formula. This means that the protocol is verified as the proper model for satisfying the correctness properties.

6 Conclusion

This paper describes the designed communication protocol structure for Korea railway signalling systems and their performance analysis results. The existing communication protocol for signalling contains considerable critical defects. The novel protocol for signalling is designed to solve these problems. To verify the designed protocol performance on data link control, the simulation is performed on two protocols under the same conditions. From the performance analysis, it is verified that the novel designed protocol exhibits good performance and also the unquestionable matters are eliminated at the designed protocol formation and mechanism. Using the informal method in specification of the communication protocol, ambiguities are generally contained in the protocol. To clear up the ambiguity contained in the designed protocol, the protocol is specified in LTS and verified through the safety and liveness properties via the model checking method. It is expected that there will be an increase in safety, reliability and efficiency in terms of the maintenance of the signalling system by using the designed novel communication protocol for Korea railway signalling systems.

References

- [1] J. G. Hwang and J. H. Lee, 'Performance analysis of data link protocol for railway signalling', Proceeding of World Congress on Railway Research, Oct. 2003.
- [2] S. Lin, D. J. Costello and M. J. Miller, 'Automatic repeat request error control schemes', IEEE Trans. Commun., vol. 22, pp. 5-17, Dec. 1984.
- [3] D. Schwabe, 'Formal Techniques for the Specification and Verification of Protocol', Ph.D Thesis, Univ. of California Los Angeles, Apr., 1981.
- [4] D. Kozen, 'Results on the prepositional mu-calculus', Theoretical Computer Science, 27:333-354, December 1983.
- [5] R. Cleaveland, 'Tableau - Based Model-Checking in the Propositional Mu-Calculus', Acta Informatica 27 : 725-727, 1990.

