Specifying a Timestamp-based Protocol For Multi-step Transactions Using LTL

Rafat Alshorman, Walter Hussak

Abstract—Most of the concurrent transactional protocols consider serializability as a correctness criterion of the transactions execution. Usually, the proof of the serializability relies on mathematical proofs for a fixed finite number of transactions. In this paper, we introduce a protocol to deal with an infinite number of transactions which are iterated infinitely often. We specify serializability of the transactions and the protocol using a specification language based on temporal logics. It is worthwhile using temporal logics such as LTL (Linear-time Temporal Logic) to specify transactions, to gain full automatic verification by using model checkers.

Keywords—Multi-step transactions, LTL specifications, Model Checking.

I. INTRODUCTION

RECENT advances in the development of portable devices and wireless communication networks have led to the emergence of mobile computing. In mobile computing environments, users have the opportunity to access information and services regardless of their location or movement behaviour. This means that a large community of concurrent users can submit their transactions to the database to be executed [15]. Examples of these applications are mobile auctions, stock trading and electronic commerce applications. In stock trading, submitting buy or sell transactions on the Internet has existed for some time. In electronic commerce applications, customers carrying portable devices (cell phones, laptops, PDAs) may purchase flight tickets from any airlines with their credit cards. These applications involve dealing with a huge number of transactions accessing databases whose consistency must be preserved in spite of updates. The component in the database system responsible for scheduling the operations of concurrent transactions to achieve consistency is the concurrency control system (or the scheduler). The scheduler orders operations belonging to different transactions by means of a concurrency control protocol [10].

The number of transactions, in most concurrency control protocols of traditional database systems, that are allowed to be executed concurrently is finite or bounded. However, in recent database systems, especially in mobile environments, the number of possible concurrent transactions is unbounded. Therefore, the schedules produced are infinite. In order to prove correctness of such systems, a verification technique that works with this view of infinite schedules is needed. Most verification techniques of such concurrency control protocols are based on finite state representations of system behaviours. These techniques cannot be directly applied to those systems of concurrent transactions where behaviours may refer to past steps of the ongoing computation or where the number of concurrent transactions is unbounded. In such cases, even simple transactions can generate infinite state systems [11].

One of the most famous examples that refers to the importance of specifying and verifying the correctness of the protocols that are used in environments where the number of users increase beyond known bounds is the Skype\(^1\) services outage [4], [5]. This problem was caused by a massive restart of users’ computers across the globe within a very short time as they rebooted after receiving a routine set of patches through Windows update [5]. A huge number of users came to the system in a continuous stream to access and request the services in terms of login transactions. The flood of attempted Skype logins together with a lack of Skype network resources, at that time, led to an outage in services. However, this event revealed a previously unseen software bug within the network resource allocation algorithm which prevented the self-healing function from working quickly. Regrettably, as a result of this disruption, Skype was unavailable to the majority of its users for approximately two days and prevented millions of registered users from accessing and making internet telephone calls using Skype software [4]. This demonstrates the limitation of some of the current protocols to deal with huge numbers of users transactions, and shows the need for specifying and verifying the correctness of the protocols that are used in such environments.

In general, mobile users submit transactions to servers that contain databases and participate in the mobile environment for execution. Since the architecture of a mobile computing system is distributed in nature [12], transactions are decomposed into a set of subtransactions, each of which executes in a different database participating in the mobile environment. Each database in a mobile environment contains a finite set of data items and therefore, the number of different transactions is also finite. However, the database system continuously reacts with other components in the environment in terms of transactions, and so the schedule will be infinite.

This paper is organized as follows. In Section II, we shall introduce some related and previous work. The motivation and the methodology of specifying infinite histories of multi-step transactions are discussed in Sections III and IV, respectively. In Section V, we define a protocol based on timestamps that

\(^1\)Skype is a VoIP (Voice over Internet Protocols) telephony company that enables its users to make free voice calls with other Skype users and also low-cost calls to landlines and mobiles around the world. Recently, the number of Skype users exceeded 170 millions, about 10 millions of which are online at the same time [5]. For more information see [3].
aims to ensure the serializability of multi-step transactions accessing ordered set of data items. Linear-time temporal logic (LTL) syntax and semantics are given in Section VI. In Section VII, the properties of LTL structure for read and write operations and their interpretations on LTL paths are depicted. The LTL specifications of serializability condition and the protocol are given Section VIII, and the conclusions are drawn in Section IX.

II. RELATED WORK

In [1], a scenario of multi-step transactions has been introduced to access an ordered set of data items \( D \). Each transaction accessed a subset of data items of a set of \( m \) data items \( D \) and each such subset accessed data items in the same order as they occurred in \( D \). They proved the serializability condition, see Theorem 12, that represented the correctness criterion to decide whether an infinite history, composed of such transactions, is serializable by checking only all possible pairs of transactions. This results in temporal logic formulae of reduced size and scale to large number of transactions. This makes testing for serializability efficient and easy to encode into the widely used temporal logics CTL and LTL. In this paper, we shall define a protocol, based on timestamps, as a concurrency control criterion suitable for such transactions. We shall use LTL to encode the specifications for the protocol and the serializability condition. We shall introduce a method to prove that the histories produced by the timestamp-based protocol are serializable and then, we can use model checkers, such as NuSMV, to perform full automatic verifications.

III. MOTIVATION

This paper focuses on specifying and verifying infinite histories of multi-step transactions accessing a finite set of data items with different properties, using temporal logic and model checker. Much work has been done in modelling mobile environments in order to determine performance. The aim here is to model mobile environments in order to determine correctness. In mobile computing environments infinite histories are produced, by the newer technologies of web and mobile transactions, in which transactions are continuously accessing the data items of the databases. The main desired property that needs to be specified and verified is serializability. We model a protocol that produces infinite histories in order to be able to use the NuSMV model checker based on the temporal logic LTL specifications to prove or disprove that the models satisfy this property. We define a protocol, based on timestamps, to apply the technique to, and verify its correctness for serializability.

IV. METHODOLOGY

In this section, we discuss some important methodological assumptions which will be used throughout the paper. The objective of this paper is to specify the correctness of transactions executing concurrently on a database in terms of serializability using specifications written in LTL. The reason for using temporal logics such as LTL, is that the method can be extended in order to verify infinite schedules as occur in mobile environments where transactions are incoming and outgoing in a continuous stream. The importance of temporal logic in computer science is clear, especially in the specification and verification of critical reactive systems. Model checkers, such as NuSMV, of many variants of temporal logic have been developed to the extent that they can deal with a huge number of states and verify real-world systems [16].

LTL is a temporal logic where the model of time is a path in which the future is determined. LTL is used for specifying general reactive and concurrent systems [13], [14]. It is worthwhile using LTL to specify multi-step transactions to gain full automatic verification by using model checkers.

We shall model the protocol which is used to ensure the serializability of concurrent transactions as finite state transition systems for which the specifications are expressed in LTL. Then, by exploring the state space of the state transition system, it is possible to check automatically if the protocol satisfies its desired specifications or not. The multi-step transactions model is characterized by a set of properties which ensure that any model for the protocol, produced by a model checker, should meet the desired model properties of multi-step transactions. The desired properties, that the system should satisfy, are expressed in LTL. Finally, a model checker will produce true if specification of the desired property satisfies all possible system behaviours. Otherwise, a counterexample will be produced to show the source of the error.

V. A TIMESTAMP-BASED PROTOCOL FOR MULTI-STEP TRANSACTIONS

Assume that we have an ordered set of data items \( D \), where \( D_i \subseteq D \), accessed by transaction \( T_i \in T = \{ T_j : j \in \mathbb{N}_1 \} \) such that \( D_i = \{ x_1, x_{i+1}, \ldots, x_p \} \), see Section II of [1]. At any point in time, let \( F(T_i) \) equal the first data item in \( D_i \) that is still to be accessed (the value of \( F(T_i) \) will keep changing during the execution time). For any transaction \( T_i \) and data item \( x_a \), we shall denote by \( TS(T_i, x_a) \) the timestamp when \( T_i \) accesses the data item \( x_a \) (for the read operation). We assume that every timestamp value is unique and accurately represents an instant in time. No two timestamps can be the same. A higher-valued timestamp occurs later in time than a lower-valued timestamp. Initially, for all \( x_a \in D_i \) and \( T_i \in T \), \( TS(T_i, x_a) = 0 \). Thereafter, when \( T_i \) accesses the data item \( x_a \), \( TS(T_i, x_a) = \text{System Timestamp} \). Then, the value of \( TS(T_i, x_a) \) remains unchanged until the last operation in the transaction \( T_i \) (\( w_i(x_p) \)) has executed. Finally, when \( w_i(x_p) \) has executed, the value of \( TS(T_i, x_a) \) is reset to zero. Formally, we define \( TS(T_i, x_a) \) as follows:

\[
\begin{align*}
TS(T_i, x_a) &= \begin{cases} 
0, & x_a \notin D_i; \\
0, & \text{when } T_i \text{ has executed } w_i(x_p); \\
\text{STS} & \text{when } T_i \text{ accesses } x_a; \\
TS(T_i, x_a), & \text{if } T_i \text{ has not executed } w_i(x_p) \text{ yet}; 
\end{cases}
\end{align*}
\]

where STS denotes the System TimeStamp. In order to execute read and write operations of transaction \( T_i \) on data item \( x_a \), we shall compare \( TS(T_i, x_a-1) \) with the remaining transactions (on the same data item \( x_a-1 \)). If \( TS(T_i, x_a-1) \) has the
minimum positive time stamp among all transactions that have executed \( x_{a-1} \) and are waiting to execute \( x_a \), then \( T_i \) can access \( x_a \). Otherwise, the transaction should suspend until it satisfies the condition (as we will see in the next subsection).

A. Accessing rules

1) There is no transaction has read \( x_a \) and has not written to \( x_a \) iff, for all \( T_j \in T \).
   (a) \( TS(T_j, x_a) = 0 \) or
   (b) \( TS(T_j, x_a) \neq 0 \) and \( w_j(x_a) \) has been executed.

2) \( T_i \) may access the first data item \( x_j \) in \( D_i \), if \( x_i \) satisfies rule 1.

3) \( T_i \) may access a data item \( x_i \), \( 2 \leq l \leq p \), if \( F(T_i) = x_i \). Otherwise, the transaction \( T_i \) will be suspended.

4) \( F(T_i) = x_i \) iff
   (a) \( x_1 \) satisfies rule 1
   (b) \( TS(T_i, x_{l-1}) = min\{TS(T_j, x_{l-1}) \mid 1 \leq j \leq n \text{ and } TS(T_j, x_{l-1}) > 0 \text{ and } TS(T_j, x_l) = 0\} \)
   (c) \( x_l \in D_l \)

For example, assume that we have 4 ordered sets of data items:

- \( D_1 = \{x_1, x_2, x_3\} \)
- \( D_2 = \{x_1, x_2\} \)
- \( D_3 = \{x_2, x_3, x_4, x_5\} \)
- \( D_4 = \{x_3, x_4\} \)

and suppose that \( T_1 \) precedes \( T_2 \) and \( T_2 \) precedes \( T_3 \). Hence, \( T_1 \) can access \( x_1 \) before \( T_2 \). Then, \( T_2 \) can access \( x_2 \) before \( T_3 \). Also, \( T_1 \) can access \( x_3 \) after \( T_2 \) has accessed \( x_3 \). Therefore, the TSM matrix will be as follows:

The entry that lies in the \( i^{th} \) row and the \( j^{th} \) column of the matrix (TMS) is typically referred to as \( TS(T_i, x_j) \), and it represents the value of the timestamp for transaction \( T_i \) when it has accessed \( x_j \). The matrix entries keep changing during the execution time. This change depends on the transactions nature (number of consecutive data items they access) and number of active transactions in any point in time. Initially, TSM will be as follows

\[
TS(T, D) = \begin{pmatrix}
0 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 0
\end{pmatrix}
\]

Now, assume that the schedule (history) \( h \) and TSM at some point in time are such that

\[
h = r_1(x_2)r_2(x_1)w_2(x_1), \quad TS(T, D) = \begin{pmatrix}
0 & 1 & \ldots & 0 \\
2 & 0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 0
\end{pmatrix}
\]

and that the transaction \( T_3 \) tries to access its first data item \( x_2 \). Then, \( T_3 \) can not access the data item \( x_2 \) because it has been read by \( T_1 \) but not written yet, as by accessing rule 1. Thus, we can know whether a data item \( x_a \) has been accessed by any transaction \( T_j \in T \) and also which transactions, by applying accessing rule 1. Subsequently, assume that the history \( h \) is such that

\[
h = r_1(x_2)r_2(x_1)w_2(x_1)w_1(x_2), \quad TS(T, D) = \begin{pmatrix}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 0 & \ldots & 0 \\
0 & 4 & 0 & \ldots & 0 \\
0 & 5 & 0 & \ldots & 0 \\
0 & 0 & 0 & \ldots & 0
\end{pmatrix}
\]

and transactions \( T_1, T_2 \) and \( T_3 \) are contending to access \( x_3 \). According to accessing rule 3, any one of them that satisfies the conditions of accessing rule 4 can access \( x_3 \). Hence, all of them satisfy conditions (a) and (c) of rule 4. But, only \( T_1 \) satisfies also condition (b) because it has the minimum timestamp of \( x_2 \). This means that \( T_1 \) accessed \( x_3 \) first, and it should also access \( x_3 \) first. It can be easily seen that for transaction \( T_2 \), timestamps \( TS(T_2, x_1) \) and \( TS(T_2, x_2) \) are reset to zero. This occurs when any transaction finishes its execution on all its data items.

VI. LINEAR TEMPORAL LOGIC SPECIFICATIONS

In this section, we present LTL as a logic that can be used to specify and verify infinite histories composed of \( n \) transactions each accessing contiguous subsets of \( m \) ordered data items, and repeating infinitely often. The aggregate of all the repetitions of the \( n \) transactions gives an infinite number of transactions \( T = \{ T_i : i \in N \} \). Infinite histories are produced by executing the accessing protocol of Section V, on an unlimited number of these kinds of transactions. The reason for using LTL as a specification language in this context, is that LTL formulae are interpreted over both finite and
infinite sequence of states [17], as we will see in the next sections, which is useful for the histories that are produced from executing the accessing protocol. Also, LTL is used for specifying general reactive and concurrent systems [13], [14]. We will encode the specifications of the accessing protocol, which is timestamp-based, and the serializability condition, which is introduced in Theorem 12 of [1], into LTL.

A. Syntax of LTL

The alphabet of LTL consists of a set of propositions symbols p₀, p₁, . . . , distinguished read/write step propositional symbols r₁(x_j), w₁(x_j), where i ≥ 1 and j ≥ 1, booleans ¬, ∨, ∧, T, ⊥, and temporal operators F, G, U. Formulae in LTL are thus generated by:

\[ \phi ::= p_i \mid r_i(x_j) \mid w_i(x_j) \mid \neg \phi \mid \phi_1 \lor \phi_2 \mid \phi_1 \land \phi_2 \mid X \phi \mid F \phi \mid G \phi \mid \phi U \phi_2 \]

The symbols ⊥ and T will also be used to denote the truth values false and true respectively and the abbreviations ⇒ and ⇔ will have their usual logical meaning.

B. Semantics of LTL

An interpretation for LTL, I(s₀), at a given state s₀ ∈ S, where S is a set of states, assigns truth values \( p_i^{I(s_0)} \), r₁(x_j)\.\( I(s_0) \) and w₁(x_j).\( I(s_0) \) to propositional symbols p₁, r₁(x_j) and w₁(x_j), respectively. A Kripke structure M, as it is defined in [2], is a triple < S, R, I >, where S is a set of states, R ⊆ S × S a transition relation such that, for all s ∈ S, there exists s' ∈ S with (s, s') ∈ R. A path in M is an infinite sequence of states, \( \pi = s_0, s_{a+1}, . . . \), such that, for every b ≥ a, (s_b, s_{b+1}) ∈ R. We use \( \pi^a \) to denote the suffix of \( \pi \) starting at s₀. As each state in a Kripke structure is required to have at least one successor, it follows that \( \pi^a \neq \) for any state \( s_a \). The semantics of a LTL formula \( \phi \) is given by the truth relation \( M, s_a \models \phi \) which means that \( \phi \) holds at state \( s_a \) in the Kripke structure M. Similarly, if \( \phi \) is a path formula, \( M, \pi \models \phi \) means that \( \phi \) holds along path \( \pi \) in the Kripke structure M. The relation \( \models \) is defined inductively as follows:

\[
\begin{align*}
M, s_0 &\models p_i^{I(s_0)} \Rightarrow T \\
M, s_0 &\models r_i(x_j)^I(s_0) \Rightarrow r_i(x_j)^I(s_0) \\
M, s_0 &\models w_i(x_j)^I(s_0) \Rightarrow w_i(x_j)^I(s_0) \\
M, s_a &\models \neg \phi \text{ if } M, s_a \not\models \phi \\
M, s_a &\models \phi_1 \lor \phi_2 \text{ if } M, s_a \not\models \phi_1 \text{ or } M, s_a \not\models \phi_2 \\
M, s_a &\models \phi_1 \land \phi_2 \text{ if } M, s_a \not\models \phi_1 \text{ and } M, s_a \not\models \phi_2 \\
M, s_a &\models X \phi \text{ if } M, s_{a+1} \models \phi \\
M, s_a &\models \phi U \phi_2 \text{ iff there exists } k \geq a \text{ such that } M, s_k \models \phi \\
M, s_a &\models G \phi \text{ iff for all } k \geq a \text{ such that } M, s_k \models \phi \\
M, s_0 &\models \phi U \phi_2 \text{ iff there exists } c \geq a, M, s_c \not\models \phi_2 \text{ and, for all } a \leq b < c, M, s_b \models \phi_1 \\
\end{align*}
\]

VII. PROPERTIES OF READ AND WRITE PROPOSITIONS

Assume that we have a Kripke structure M and that the following properties, relating to \( r_i(x_j) \) and \( w_i(x_j) \) propositions, hold in M:

(P1) Read/write alternation
A transaction \( T_i \) cannot have read two distinct data items (in \( D_s \)) without having written to one of them, i.e. if \( x_j < D \) \( x_j' \), \( < D \) denotes to irreflexive totally order relation on a set \( D, r_i(x_j) \) cannot be executed until \( w_i(x_j) \) has been executed.

(P2) Write implies read
A transaction \( T_i \) can only have written to \( x_j \) if it has read \( x_j \), i.e. if \( w_i(x_j) \) executes, then \( r_i(x_j) \) must have executed before.

(P3) Read/write step proposition remains true until the next operation, belonging to the same transaction, becomes true
If a read/write step has taken place, the corresponding proposition remains true until the next operation in \( T_i \) becomes true, i.e. \( r_i(x_j) / w_i(x_j) \) is true, remains true until the next step \( w_i(x_j) / r_i(x_j) \), where \( x_j < D x_j' \), becomes true.

(P4) At most one step occurs at each successive state
No two distinct steps can both be false in a state, and then both true in a next state.

(P5) A transaction \( T_i \) accesses each data item \( x \in D_s \) exactly once for both read and write operations
For all \( x \in D_s \), a transaction \( T_i \) can have exactly one read operation (\( r_i(x) \)) and exactly one write operation (\( w_i(x) \)) for the data item \( x \).

The semantics of formula \( \phi \) is now given by a truth relation \( M, s_a \models \phi \), where M is a structure for LTL satisfying the additional properties (P1)-(P4). Given a state \( s_a \) and a path \( \pi \), there corresponds a sequence of read and write step propositions that become true in \( s_a, s_{a+1}, . . . \). In this way, \( \pi \) yields a history of the transactions \( T_1, T_2, . . . \) produced by the protocol and starting their execution at \( s_a \). We illustrate this correspondence between paths and histories as follows:

\[
\begin{align*}
\begin{array}{cccccccc}
\mathcal{R}_1(x_1) & \mathcal{R}_2(x_2) & \mathcal{R}_3(x_3) & \mathcal{W}_1(x_1) & \mathcal{W}_2(x_2) & \mathcal{W}_3(x_3) \\
\mathcal{B}_1 & \mathcal{B}_2 & \mathcal{B}_3 & \mathcal{B}_4 & \mathcal{B}_5 & \mathcal{B}_6 \\
\mathcal{S}_0 & \mathcal{S}_1 & \mathcal{S}_2 & \mathcal{S}_3 & \mathcal{S}_4 & \mathcal{S}_5 \\
\begin{array}{cccccc}
\mathcal{S}_6 & \mathcal{S}_7 & \mathcal{S}_8 & \mathcal{S}_9 & \mathcal{S}_{10} & \mathcal{S}_{11} \\
\mathcal{S}_{12} & \mathcal{S}_{13} & \mathcal{S}_{14} & \mathcal{S}_{15} & \mathcal{S}_{16} & \mathcal{S}_{17} \\
\end{array} \\
\end{array}
\end{align*}
\]
In the depiction above, we have:

\[ D_1 = \{x_1, x_2, x_3\} \]
\[ D_2 = \{x_2, x_3, x_4\} \]
\[ D_3 = \{x_1, x_2, x_3, x_4, x_5\} \]

and the corresponding transactions as follows:

\[ T_1 = r_1(x_1) w_1(x_1) r_1(x_2) w_2(x_2) r_1(x_3) w_3(x_3) \]
\[ T_2 = r_2(x_2) w_2(x_2) r_2(x_3) w_3(x_3) r_2(x_4) w_4(x_4) \]
\[ T_3 = r_3(x_3) w_3(x_3) r_3(x_4) r_3(x_5) w_5(x_5) \]

The read and write propositions that are given for each successive state represent the propositions that are true in those states. The top of each column displays the unique proposition that becomes true in the particular state. This represents the read and write operations that has been scheduled by the protocol. In order to make it easier to follow the structure which has a large number of propositions which are false, only the values of propositions that are true in the states of the trace are shown. The corresponding history \( h \) is:

\[ h = r_1(x_1) r_2(x_2) w_1(x_1) w_2(x_2) r_3(x_3) w_3(x_3) r_1(x_2) w_1(x_2) \]
\[ r_3(x_3) w_2(x_3) r_2(x_3) w_3(x_3) r_1(x_3) w_1(x_3) r_3(x_3) w_3(x_3) r_3(x_4) w_3(x_4) r_3(x_5) w_5(x_5) \]

We make use of additional propositions begin\(_i\) and end\(_i\) to refer to the begin and the end of each transaction.

**VIII. Encoding the Accessing Protocol and Serializability Condition into LTL**

Firstly, we encode, using temporal operators, the properties (P1)-(P5) of the read and write propositions in the LTL structures (as in the previous section) as \( \sigma_0 \), \( \sigma_1 \), \( \sigma_2 \), \( \sigma_3 \) and \( \sigma_4 \) respectively, as follows:

**(P1) Read/Write alternation**

A transaction \( T_i \) cannot have read two distinct data items (in \( D_i \)) without having written to one of them, i.e. if \( x < D \ y \), \( r_i(y) \) cannot be executed until \( w_i(x) \) has been executed.

\[ \sigma_0 = \bigwedge_{i \geq 1} \bigwedge_{x,y \in D_i, x < D y} G[r_i(x) \Rightarrow F(w_i(x) \land F(r_i(y)))] \]

**(P2) Write implies read**

A transaction \( T_i \) can only have written to \( x \) if it has read \( x \), i.e. if \( w_i(x) \) executes, then \( r_i(x) \) must have executed before.

\[ \sigma_1 = \bigwedge_{i \geq 1} \bigwedge_{x \in D_i} G[r_i(x) \Rightarrow F(w_i(x))] \]

**(P3) Read/write step proposition remains true until the next operation, belonging to the same transaction, becomes true**

If a read/write step has taken place, the corresponding proposition remains true until the next operation in \( T_i \) becomes true, i.e. if \( r_i(x)/w_i(x) \) is true, it remains true until the next step \( w_i(x)r_i(y) \), where \( x < D \ y \), becomes true.

\[ \sigma_2 = \bigwedge_{i \geq 1} \bigwedge_{x \in D_i} G[w_i(x) \Rightarrow \neg r_i(x)] \land \bigwedge_{i \geq 1} \bigwedge_{x,y \in D_i, x < D y} G[r_i(y) \Rightarrow \neg w_i(x)] \]

**(P4) At most one step occurs at each successive state**

No two distinct steps can both be false in a state, and then both true in a next state.

\[ \sigma_3 = \bigwedge_{i,j \geq 1, i \neq j} \bigwedge_{\forall k} G[\neg (w_i(x_j) \land w_j(x_i)) \land X[r_i(x_j) \land F_{r_i}(x_j))] \land \neg (r_i(x_j) \land \neg w_i(x_j)) \land X(r_i(x_j) \land F_{w_i}(x_j))] \land \neg (\neg w_i(x_j) \land \neg w_j(x_i)) \land X(w_i(x_j) \land F_{w_i}(x_j)) \]

**(P5) A transaction \( T_i \) accesses each data item \( x \in D_i \) exactly once for both read and write operations**

For all \( x \in D_i \), a transaction \( T_i \) can have exactly one read operation \( (r_i(x)) \) and exactly one write operation \( (w_i(x)) \) for the data item \( x \), i.e we can not have \( T_i \) such that:

\[ T_i = r_i(x_1)w_1(x_1)\ldots r_i(x_1)\ldots w_i(x_p) \]

or

\[ T_i = r_i(x_1)w_1(x_1)\ldots w_i(x_1)\ldots w_i(x_p) \]

where \( D_i = \{x_1, x_2, \ldots, x_p\} \). This is defined in \( \sigma_5 \) as follows:

\[ \sigma_4 = \bigwedge_{i \geq 1} \bigwedge_{x \in D_i} G[\neg F(r_i(x)] \land F(r_i(x))] \land \bigwedge_{i \geq 1} \bigwedge_{x \in D_i} G[\neg F(w_i(x)] \land F(w_i(x))] \]

Next, we encode the serializability condition of Theorem 12 (see [1]). This is defined in terms of \( \sigma_5 \) and \( \sigma_6 \):

\[ \sigma_5 = \bigwedge_{i,j \geq 1, i \neq j} \bigwedge_{\forall k} G[\neg (w_i(x) \land F(r_i(x)) \land F_{w_i}(x))] \land (w_i(x) \land F_{w_i}(x) \land \neg F(r_i(x)) \land F_{r_i}(x)) \land \neg (F(r_i(x)) \land \neg F_{w_i}(x)) \land (\neg F_{w_i}(x) \land \neg F_{r_i}(x)) \]

\[ \sigma_6 = \bigwedge_{i,j \geq 1, i \neq j} \bigwedge_{x \in D_i \cap D_j} G[\neg r_i(x) \land r_i(x)] \]
The serializability condition of Theorem 12 says if we choose any two transactions \((T_i, T_j)\) participating in a history \(h\) and we take the history that containing only the operations that belonging to \(T_i\) and \(T_j\) (denoted by \(h(T_i, T_j)\)), where \(D_i \cap D_j = \{x_1, \ldots, x_p\}\). Then, \(h(T_i, T_j)\) will be of the form

\[
h_{(T_i, T_j)} = \ldots r_i(x_1) \ldots w_i(x_1) \ldots r_i(x_p) \ldots w_i(x_p) \ldots r_j(x_1) \ldots w_j(x_1) \ldots r_j(x_p) \ldots w_j(x_p) \ldots
\]

then the the history \(h\) is serializable. In \(\sigma_6\), we encode that if a transaction \(T_i\) begins executing a read operation on data item \(x\), no read operation on data item \(x\) by any other transactions occurs (executes) until the write operation of \(T_i\) completes its execution on data item \(x\), i.e.:

\[
\ldots r_i(x_1), \ldots, r_i(x_p) \ldots w_i(x_1) \ldots
\]

Therefore, if we avoid the situation above, there is no cycle in the precedence graph \(G\) of a history \(h(T_i, T_j)\) (denoted by \(G(h(T_i, T_j))\) as in [1], [2], [10]) between \(T_i\) and any other transaction \(T_j\) on the same data item; see Figure 1(a). Now, the serializability condition, of Theorem 12, is to hold for each \(x \in D_i \cap D_j\). It is possible to make a cycle of length two in a precedence graph \(G(h(T_i, T_j))\) on different data items, i.e. if \(T_i\) precedes \(T_j\) in accessing data item \(x\) and \(T_j\) precedes \(T_i\) in accessing data item \(y\), or \(T_j\) precedes \(T_i\) in accessing data item \(x\) and \(T_i\) precedes \(T_j\) in accessing data item \(y\), see Figure 1(b) and Figure 1(c). Therefore, we encode in \(\sigma_5\) that these two situations do not occur. The formulae \(\sigma_5\) and \(\sigma_6\) together represent the encoding of the serializability condition into LTL denoted by \(\sigma_T\):

\[
\sigma_T = \sigma_5 \land \sigma_6
\]

(a) Cycle on the same data item

(b) Cycle on different data items

(c) Cycle on different data items

Fig. 1. Cycle of length two

Next, we encode the accessing protocol, which defines in section V, in \(\sigma_{10}\) as follows:

\[
\sigma_{10} = \bigwedge_{i,j,k \geq 1} \left( w_i(x_1) \land F(w_j(x_1) \land F(w_k(x_1)))\right) \lor \left( w_j(x_1) \land F(w_k(x_1) \land F(w_j(x_1)))\right) \lor \left( w_k(x_1) \land F(w_i(x_1) \land F(w_j(x_1)))\right).
\]

In \(\sigma_8\), we model an unbounded number of transactions, that may come to the scheduler \(S\), which uses the protocol that is defined in section V, by three transactions \(T_i, T_j\) and \(T_k\). Transactions \(T_i\) and \(T_j\) represent any two particular transactions satisfying the accessing rules of the protocol and \(T_k\) represents any other transaction in the schedule \(S\). Transaction \(T_k\) could execute any data item \(x \in D_i \cap D_j \cap D_k\) as follows

- Case 1: \(T_k\) could execute \(x\) after \(T_i\) and \(T_j\)

\[
\ldots w_i(x_1) \ldots w_j(x_1) \ldots w_k(x_1) \ldots
\]

- Case 2: \(T_k\) could execute \(x\) after \(T_i\) and before \(T_j\)

\[
\ldots w_j(x_1) \ldots w_k(x_1) \ldots w_j(x_1) \ldots
\]

- Case 3: \(T_k\) could execute \(x\) before \(T_i\) and \(T_j\)

\[
\ldots w_k(x_1) \ldots w_i(x_1) \ldots w_j(x_1) \ldots
\]

In the depiction above, we assume that \(T_i\) executes the data item \(x\), where \(x \in D_i \cap D_j\), before \(T_j\) does. Therefore, we can say that, \(T_i\) and \(T_j\) satisfy the accessing rules of the protocol if and only if for all \(x \in D_i \cap D_j\), \(TS(T_i, x) < TS(T_j, x)\) or \(TS(T_j, x) < TS(T_i, x)\) regardless of when the transaction \(T_k\) could access the data item \(x\). We can illustrate this in the LTL structure as follows:

\[
\begin{align*}
& w_i(x_1) \quad r_j(x_1) \quad w_j(x_1) \quad w_i(x_{i+1}) \\
& \vdots \quad \vdots \quad \vdots \quad \vdots \\
& r_j(x_{i+1}) \quad w_j(x_{i+1}) \quad w_i(x_p) \quad r_j(x_p) \\
& \vdots \quad \vdots \quad \vdots \quad \vdots \\
& w_i(x_{i+1}) \quad r_j(x_{i+1}) \quad w_j(x_{i+1}) \quad w_i(x_p) \quad w_j(x_{i+1}) \quad r_j(x_p)
\end{align*}
\]
\( w_j(x_p) \)

\[ \bullet \]

\( w_i(x_p) \)

\( w_j(x_p) \)

\( \vdots \)

where \( D_i \cap D_j = \{ x_i, x_{i+1}, \ldots, x_p \} \). We notice, from the depiction above, that transaction \( T_i \) has executed \( w_i(x) \) and \( T_j \) has not executed both \( r_j(x_i) \) and \( w_j(x_j) \) yet, regardless of when/where the transaction \( T_k \) executes read and write operations on the data item \( x_i \) and similarly for \( x_{i+1} \) up to \( x_p \).

Transaction \( T_j \) will execute both \( r_j(x_i) \) and \( w_j(x_j) \) after \( T_i \) does and this will keep \( T_i \) and \( T_j \) serializable. In other words, execution of any operations belonging to other transactions will not affect the serializability of the transactions \( T_i \) and \( T_j \).

The access rules of the protocol (see subsection V.A) say that if a transaction \( T_i \) has executed \( r_i(x) \) but not \( w_i(x) \), no other transaction \( T_j \) can execute \( r_j(x) \). This can be encoded into LTL as follows:

\[
\sigma_9 = \bigwedge_{i,j \geq 1, i \neq j} \bigwedge_{x \in D_i \cap D_j} G[r_i(x) \implies \neg r_j(x)]
\]

Therefore \( \sigma_{10} \), which represents the access protocol, is defined as follows:

\[
\sigma_{10} = \sigma_8 \land \sigma_9.
\]

This means that any history \( h \) produced by the access protocol should satisfy both \( \sigma_8 \) and \( \sigma_9 \), if we model the read and write operations in the history \( h \) by an LTL structure.

Now, the future in LTL is seen as a sequence of states, so the future is a path. Therefore, if we consider the states in the LTL path as instants of time, we can assign a truth value to each proposition at each time instant so that the interpretation maps to each instant of time a set of propositions that hold at that instant. As a consequence of this, we can assign a truth value to each read/write proposition belonging to any active transaction, at any given time, that is scheduled by the protocol. As we are dealing with a protocol based on timestamps, our interpretation will, therefore, map each timestamp to a set of propositions that hold at that timestamp. Thus, the interpretation \( I \) is a function

\[
I : \mathbb{N} \rightarrow 2^{\text{prop}}
\]

where \( \mathbb{N} \) is a set of timestamps (natural number) and \( \text{prop} \) is a set of all propositions. This means that we can specify infinite histories generated by a protocol based on timestamps using LTL specifications. Now, as \( \sigma_{10} \) represents the histories produced (or generated) by the protocol and \( \sigma_7 \) represents the serializability condition then, we can prove that the histories are serializable by proving the following formula:

\[
\sigma_{10} \implies \sigma_7.
\]

IX. CONCLUSION

We have given an approach, using LTL, to specify and verify a scheduler uses a protocol, based on timestamp, to schedule an unlimited number of transactions incoming and outgoing from a system. This approach allows for the systems and their properties to be specified using temporal logics. The verification part can be performed by model checkers, such as NuSMV or Spin, to check exhaustively the state space of the system behaviours against the specifications. If the system does not satisfy its properties, counterexamples to pinpoint the errors are automatically produced by the model checker.

We have assumed serializability to be the correctness criterion for concurrent transactions executing in a transactions processing system. Also, we have shown that the serializability condition and the scheduler can be encoded into LTL. Then, an automatic verification can be performed using a model checker, to see whether the scheduler satisfies the serializability condition or not.

We have found that LTL is a good choice to specify a protocol based on timestamps because any state in LTL path could implicitly represent a timestamp. Actually, we encoded the behaviour of the protocol in terms of three transactions. Two of them represent any two transactions satisfying the accessing rules of the protocol, and the remaining one represents any other transaction in the schedule. This means that we can prove that the schedules, produced by the protocol, are serializable if

\[
\sigma_{10} \implies \sigma_7
\]

is satisfied, where \( \sigma_{10} \) represents the LTL formula that specifies the behaviour of the protocol in LTL structure, that we have given above, and \( \sigma_7 \) represents the LTL formula that specifies the serializability condition. This gives us an automatic verification approach that can overcome the disadvantages of the traditional approaches such as human error and may not cover all possible system behaviours.

ACKNOWLEDGMENT

We would like to thank ZPU (Zarqa Private University) for its support in making this work possible.

REFERENCES


