A BSP algorithm for on-the-fly checking LTL formulas on security protocols
Frédéric Gava, Michael Guedj, Franck Pommereau

To cite this version:
Frédéric Gava, Michael Guedj, Franck Pommereau. A BSP algorithm for on-the-fly checking LTL formulas on security protocols. 11th International Symposium on Parallel and Distributed Computing (ISPDC 2012), Jun 2012, Munich/Garching, Bavaria, Germany. pp.11–18, 10.1109/ISPDC.2012.10. hal-00868689

HAL Id: hal-00868689
https://hal.archives-ouvertes.fr/hal-00868689
Submitted on 16 Feb 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A BSP algorithm for on-the-fly checking LTL formulas on security protocols

Frédéric Gava  
University of Paris-East  
LAACL  
Créteil, France  
frederic.gava@univ-paris-est.fr

Michaël Guedj  
University of Paris-East  
LAACL  
Créteil, France

Franck Pommereau  
University of Évry  
IBISC  
Évry, France  
franck.pommereau@ibisc.univ-evry.fr

Abstract—This paper presents a Bulk-Synchronous Parallel (BSP) algorithm to compute on-the-fly whether a structured model of a security protocol satisfies a LTL formula. Using the structured nature of the security protocols allows us to design a simple and efficient parallelisation of an algorithm which constructs the state-space under consideration in a need-driven fashion. A prototype implementation has been developed, allowing to run benchmarks.

Keywords-BSP; LTL; Security Protocols;

I. INTRODUCTION

Designing secure protocols is a challenging problem [1]. In spite of their apparent simplicity, they are notoriously error-prone. Unfortunately, checking if a cryptographic protocol is secure or not is not decidable in general and NP-complete for bounded numbers of agents and sessions [2]. Model-checking is however well-adapted to find flaws [3]. In this paper, we consider the problem of checking an LTL formula over labelled transition systems (LTS) that model security protocols. Checking a LTL formula over a protocol is not new [4] and has the advantage over dedicated tools for protocols to be easily extensible to non standard behaviour of honest principals (e.g., contract-signing protocols: participants required to make progress) or to check some security goals that cannot be expressed as reachability properties, e.g., fair exchange.

But checking an LTL formula may be expensive both in terms of memory and execution time: this is the so-called state explosion problem. This is especially true when complex data-structures are used in the model as the knowledge of an intruder in security protocols. Because this checking can cause memory crashing on single or multiple processor systems, it has led to consider exploiting the larger memory space available in distributed systems [5], which also gives the opportunity to reduce the overall execution time. One of the main technical issues is to partition the state space, i.e., each state is assigned to a machine. Each subset of states is thus “owned” by a single machine. While it has been shown that a pure static hashing for the partition function can effectively balance the workload [24] and achieve reasonable execution time as well, this method suffers from an obvious drawbacks: it causes too much cross transitions, i.e., successor states that need to be exchanged over the network thus impairing computation locality.

Also, it is rarely necessary to compute the entire state space before finding a path that invalidates the logic formula (notably a flaw in a protocol): on-the-fly (local) algorithms are designed to build the state space and check the formula at the same time. Two approaches are generally used: Nested Depth First Search (NDFS) and Strongly Connected Components (SCC) algorithms for detecting on-the-fly a reachable accepting cycle in the underlying graph — mainly of a Büchi automaton. The former are known to be memory efficient and the latter to be time efficient [6] and both are hard to parallelize [7].

In this paper, we exploit the well-structured nature of security protocols and match it to a model of parallel computation called BSP [8]. This allows us to simplify the writing of an efficient BSP algorithm for checking on-the-fly an LTL formula for finite protocol sessions. It is based on the algorithm of [9] which mainly combines the construction a proof-structure (a graph whose nodes states of the underlying Kripke structure together with sets of logical formulas) with a Tarjan’s depth-first-search based SCC algorithm. The structure of the protocols is exploited to partition the state space and reduce cross transitions while increasing computation locality. At the same time, the BSP model allows to simplify the detection of the algorithm termination and to load balance the computations.

II. CONTEXT AND DEFINITIONS

A. The BSP model

A BSP computer is a set of uniform processor-memory pairs connected through a communication network allowing the inter-processor delivery of messages [8]. A BSP program is executed as a sequence of super-steps (see Fig. 1), each one divided into three successive disjoint phases: (1) each processor only uses its local data to perform sequential computation and to request data transfers to other nodes; (2) the network delivers the requested data; (3) a global synchronisation barrier occurs, making the transferred data available for the next super-step.
EXCHANGE

there exists a function and it is enough to assume that the following properties
approach is largely independent of the chosen formalism (a measure) such that if
informations (possible messages from newly as well as previously learnt
the key to do so is known. Then, the attacker forges all
is captured by the attacker that tries to learn from it by
agent sends a message on the network. (2) This message
is thus a series of message exchanges as follows. (1) An
resides on the network [11]. An execution of such a model
system (LTS). We also consider a Dolev-Yao attacker that
reception accept some of the messages forged by the
on the network. (3) The agents waiting for a message
messages (including the original one) are made available
intruder) receives information (and stores it), and to all
other transitions; (P2) there is an initial state $s_0$ and
there exists a function slice from states to natural numbers
(a measure) such that if $s' \in \text{succ}_R(s)$ then there is no
path from $s'$ to any state $s''$ such that slice$(s) = \text{slice}(s'')$ and
slice$(s') = \text{slice}(s) + 1$ (it is often call a sweep-line
progression [13]); (P3) there exists a function cpu from
states to natural numbers (a hashing) such that for all state
if $s' \in \text{succ}_R(s)$ then cpu$(s) = \text{cpu}(s')$; mainly,
the knowledge of the intruder is not taken into account to
compute the hash of a state; (P4) if $s_1, s_2 \in \text{succ}_R(s)$ and
$\text{cpu}(s_1) \neq \text{cpu}(s_2)$ then there is no possible path from $s_1$
to $s_2$ and vice versa.

On concrete models, it is generally easy to distinguish
syntactically the transitions that correspond to a message
reception in the protocol with information storage. Thus, is
easy to partition succ as above and, for most protocol
models, it is also easy to check that the above properties
are satisfied. This is the case in particular for us using the
ABCD formalism.

B. State space of security Protocols [10]

In this paper, we consider models of security protocols,
involving a set of agents, given as a labelled transition
system (LTS). We also consider a Dolev-Yao attacker that
resides on the network [11]. An execution of such a model
is thus a series of message exchanges as follows. (1) An
agent sends a message on the network. (2) This message
is captured by the attacker that tries to learn from it by
recursively decomposing the message or decrypting it when
the key to do so is known. Then, the attacker forges all
possible messages from newly as well as previously learnt
(i.e., attacker’s knowledge). Finally, these
messages (including the original one) are made available
on the network. (3) The agents waiting for a message
reception accept some of the messages forged by the
attacker, according to the protocol rules.

As a concrete formalism to model protocols, we have used
an algebra of coloured Petri nets called ABCD [12, Sec. 3.3]
allowing for easy and structured modelling. However, our
approach is largely independent of the chosen formalism
and is enough to assume that the following properties
hold: (P1) LTS function succ can be partitioned into two
successor functions $\text{succ}_R$ and $\text{succ}_L$ that correspond
respectively to transitions upon which an agent (except the
intruder) receives information (and stores it), and to all
other transitions; (P2) there is an initial state $s_0$ and
there exists a function slice from states to natural numbers
(a measure) such that if $s' \in \text{succ}_R(s)$ then there is no
path from $s'$ to any state $s''$ such that slice$(s) = \text{slice}(s'')$
and slice$(s') = \text{slice}(s) + 1$ (it is often call a sweep-line
progression [13]); (P3) there exists a function cpu from
states to natural numbers (a hashing) such that for all state
if $s' \in \text{succ}_R(s)$ then cpu$(s) = \text{cpu}(s')$; mainly,
the knowledge of the intruder is not taken into account to
compute the hash of a state; (P4) if $s_1, s_2 \in \text{succ}_R(s)$ and
$\text{cpu}(s_1) \neq \text{cpu}(s_2)$ then there is no possible path from $s_1$
to $s_2$ and vice versa.

On concrete models, it is generally easy to distinguish
syntactically the transitions that correspond to a message
reception in the protocol with information storage. Thus, is
easy to partition succ as above and, for most protocol
models, it is also easy to check that the above properties
are satisfied. This is the case in particular for us using the
ABCD formalism.

C. BSP Computing of the state space [10]

Based on the following properties, we have designed in
[10] a BSP algorithm (in a SPMD fashion) for computing
the state space of security protocols as shown in Fig. 3.
In this algorithm, “BSP\_EXCHANGE” is a primitive that
allows processors to globally exchange data: a set of pairs
(pid,value) is used to define values to be sends. Mainly:
(1) states are distributed across the processors using the
cpu function; (2) the algorithm finishes when no states are
exchanged; (3) function \text{Successor} is called to compute the
successors of the states, then all new states from $\text{succ}_L$
are added in $\text{todo}$ (states to be proceeded) and states from

\begin{verbatim}
def bsp_state_space() is
todo,known←0,∅
total←1
if cpu(s) = mypid
todo←todo∪\{s\}
while total>0
tosend←Successor(known,todo)
todo,total←Exchange(known,tosend)
return known

def Successor(known,todo) is
tosend←∅
while todo≠∅
pick s from todo
known←known∪\{s\}
todo←todo∪\{cpu(s)\} \m
do for s'∈\text{succ}_R(s)
tosend←tosend∪\{(cpu(s'),s')\}
return tosend

def Exchange(known,tosend) is
dump(known)
return BSP\_EXCHANGE(Balance(tosend))

def Balance(tosend) is
histoL←\{i,♯(i,s)∈tosend\}
compute histoG from BSP\_EXCHANGE(histol)
return BinPack(tosend,histoG)
\end{verbatim}

Figure 3. BSP computing the state space of protocols

\begin{figure}
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{A BSP super-step.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{fig2.png}
\caption{Syntax and informal semantics of LTL.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{fig3.png}
\caption{Syntax of LTL:
\[\phi ::= a | \neg a | \phi \land \phi | \phi \lor \phi | X\phi | \phi U \phi | \phi V \phi\]
Informal semantics of LTL:
\[X\phi : \cdot \rightarrow \bullet \rightarrow \cdot \rightarrow \bullet \rightarrow \cdot \rightarrow \cdots\]
\[\phi_1 U \phi_2 : \phi_1 \rightarrow \bullet \phi_1 \rightarrow \bullet \phi_2 \rightarrow \bullet \phi_2 \rightarrow \bullet \phi_2 \rightarrow \cdot \rightarrow \cdots\]
or
\[\phi_1 V \phi_2 : \bullet \phi_2 \rightarrow \bullet \phi_2 \rightarrow \bullet \phi_2 \rightarrow \phi_2 \rightarrow \bullet \phi_2 \rightarrow \cdot \rightarrow \cdots\]
\end{verbatim}

Figure 2. Syntax and informal semantics of LTL. 

\begin{verbatim}} \end{verbatim}
succe are sent to be treated at the next super-step, enforcing
an order of exploration of the state space that match the
progression of the protocol. (4) It thus becomes possible
at the beginning of each super-step, to dump from the main
memory all the known states because they cannot be reached
anymore due to the sweep-line progression. (5) States to
be sent are first balanced across the processors using an
histogram histoG (which is first totally exchanged to be the
same on each processor and enforce consistent decisions
on all the processors: each processor send its own local
histoL) and according to a simple heuristic for the bin
packing problem, classes of states (consistent with hash) are grouped on processors so there is no possibility of
duplicated computation.

This algorithm gives better performances (less cross tran-
sitions) than a naive distributed one [10] and is able to dump
all the known states at the beginning of each super-step
allows to use less memory. Partial-order reductions [14] can
also be introduced without really changing the algorithm.

D. Proof-structure and LTL checking [9]

Considerable attention has been devoted to the develop-
ment of automatic techniques, or model-checking pro-
cedures, for verifying finite-state systems against specifications
expressed using various temporal logics and notably the
linear (LTL) subset. This logic permits users to characterize
many properties, including safety and liveness. One may
identify two basic approaches to model checking. The first
uses global analysis to determine if a system satisfies a for-
mula; the entire state space (mainly a Kripke structure) of the
system is given on Fig 2) and concentrate on the notion of proof-
structures and LTL logic (an informal semantics
attempts to take advantage of this observation by constructing
in order to determine whether or not the system satisfies a
formula. On-the-fly , or local, approaches to model checking
in many cases (especially when a system does not satisfy a
property) are grouped on processors so there is no possibility of
duplicated computation.

We define $M = (S, R, L)$ to be a Kripke structure where
$S$ is the set of states, $R \subseteq S \times S$ the relation which is
assumed to be total (thus all paths in $M$ are infinite) and
$L \subseteq S \rightarrow 2^A$ the labelling. The proof-rules appear in Fig 4
[9] and they operate on assertions of the form $s \vdash A\Phi$ where
$s \in S$ and $\Phi$ is a set of path formulas. Semantically, $s \vdash A\Phi$
holds if $s \vdash A(\phi_1, \ldots, \phi_n)$ where $A(\phi_1, \ldots, \phi_n)$ to
represent a formula of the form $A(\Phi \cup \{\phi_1, \ldots, \phi_n\})$.

To denote that $\phi \in \Phi$. Proof-rules are used to build proof-
structures that are defined as follows:

**Definition 1.** Let $\Sigma$ be a set of nodes, $\Sigma' = \Sigma \cup true$, $V \subseteq
\Sigma'$, $E \subseteq V \times V$ and $\sigma \in V$. Then $(V, E)$ is a proof structure
for $\sigma$ if it is a maximal directed graph such that for every
$\sigma'\in V$, $\sigma'$ is reachable from $\sigma$, and the set $\{\sigma'' | (\sigma', \sigma'') \in E\}$
results from applying some rule to $\sigma'$.

Intuitively, a proof structure for $\sigma$ is a directed graph that
is intended to represent an (attempted) “proof” of $\sigma$. In what
follows, we speak of a directed graph and use traditional
graph notations when speaking of proof structures. Note
that in contrast with traditional definitions of proofs, proof
structures may contain cycles. In order to define when a
proof structure represents a valid proof of $\sigma$, we use:

**Definition 2.** Let $(V, E)$ be a proof structure. Then: (1) $\sigma \in V$ is a leaf
iff there is no $\sigma'$ such that $(\sigma, \sigma') \in E$. A leaf $\sigma$ is
successful iff $\sigma \equiv true$; (2) an infinite path $\pi = \sigma_0, \sigma_1, \ldots,
in (V, E)$ is successful iff for some assertion $\sigma_i$ infinitely
repeated on $\pi$ there exists $\sigma_1\sigma_2 \in \sigma_i$ such that for all
$j \ge i, \phi_2 \notin \sigma_j$; (3) $(V, E)$ is successful iff all its leaves and
infinite paths are successful.

Roughly speaking, an infinite path is successful if at
some point a formula of the form $\phi_1\neg\phi_2$ is repeatedly
“regenerated” by application of rule R6; that is, the right
subgoal (and not the left one) of this rule application appears
each time on the path. Note that after $\phi_1\neg\phi_2$ occurs on the
path $\phi_2$ should not, since, intuitively, if $\phi_2$ would be true
then the success of the path would not depend on $\phi_1\neg\phi_2$, while
if it would be false then $\phi_1\neg\phi_2$ would not hold. Note
also that if no rule can be applied (i.e., $\Phi = \emptyset$) then the
proof-structure and thus the formula is unsuccessful.

**Theorem 1.** Let $M$ be a Kripke structure with $s \in S$ and
$A\phi$ an LTL formula, and let $(V, E)$ be a proof structure for
$s \vdash A\phi$. Then $s \vdash A\phi$ iff $(V, E)$ is successful.
One consequence of this theorem is that if $\sigma$ has a successful proof structure, then all proof structures for $\sigma$ are successful. Thus, in searching for a successful proof structure for an assertion no backtracking is necessary. It also turns out that the success of a finite proof structure may be determined by looking at its strongly connected components for any accepting cycle. An obvious solution to this problem would be to construct the proof structure for the assertion and then check if the proof structure is successful. Of course, this algorithm is not on-the-fly as it does not check the success of a proof structure until after it is built. An efficient algorithm, on the other hand, combines the construction of a proof structure with the process of checking whether the structure is successful. A Tarjan’s like algorithm was used in [9] but a NDFS one could also be used.

### III. BSP ON-THE-FLY LTL CHECKING

As explained in the previous section, we use two LTL successors functions for constructing the Kripke structure: $\text{succ}_C$ ensures a measure of progression slice that intuitively decomposes the Kripke structure into a sequence of slices $S_0, \ldots, S_n$ where transitions from states of $S_i$ to states of $S_{i+1}$ come only from $\text{succ}_R$ and there is no possible path from states of $S_i$ to states $S_j$ for all $i < j$. Also after $\text{succ}_R$ transitions (with different hashing), there is no possible common paths which is due to different knowledge of the agents. In this way, if we assume, as in Fig 3, a distribution of the Kripke structure across the processors using the cpu function, then the only possible accepting cycles or SCCs are locals to each processor. Thus, because proof-structures follow the Kripke structure (rule R7), accepting cycles or SCCs are also only locals. This fact ensures that any sequential algorithm to check cycles or SCCs can be used for the parallel computation.\(^1\) Call this generic algorithm $\text{SeqChkLTL}$ which takes an assertion $\sigma = s \vdash \Phi$, a set of assertions to be sent (for the next super-step), and $(V, E)$ the sub-part of the proof-graph (a set of assertions as vertices and a set of edges) that has been previously proceed (this sub-part can grow during this computation). Now, in the manner of [10], we can design our BSP algorithm which is mainly an iteration over the independent slices, one slice per super-step and, on each processor, working on independent sub-parts of the slice by calling $\text{SeqChkLTL}$. This algorithm is given in Fig 5.

The main function is $\text{ParChkLTL}$, it first calls an initialisation function in which only the one processor that owns the initial state saves it in its $\text{todo}$ list. The variable $\text{total}$ stores the number of states to be processed at the beginning of each super step; $V$ and $E$ store the proof graph: $\text{super\_step}$ stores the current super step number; $\text{dfn}$ is used for the SCC algorithm; finally, $\text{flag}$ is used to check whether the formula has been proved false ($\text{flag = } \bot$) or not ($\text{flag = } \emptyset$).

\(^1\)It is mainly aired that SCC computation gives smaller traces than NDFS. Both methods are equivalent for our purpose.

![Figure 5. A BSP algorithm for LTL checking](image-url)
which indicates that the local exploration succeeded (P2) and allows to proceed to the next super step in the main loop. When all the local states have been processed, states are exchanged, which leads to the next slice (i.e., the next super step). In order to terminate the algorithm as soon as one processor discovers a counterexample, each locally computed flag is sent to all the processors and the received values are then aggregated using function filter_flag that selects the non-⊥ flag with the lowest dfn value computed on the processor with the lowest number, which allows to ensure that every processor chooses the same flag and then computes the same trace. If no such flag is selectable, filter_flag returns ⊥. To balance the computation, we use the number of states as well as the size of the formula (on which the number of subgoals directly depends).

Notice also that at each super step, each processor dumps \( \sigma \) to its local disk, recording the super step number, in order to be able to reconstruct a trace. When a state \( \sigma \) that invalidates the formula is found, a trace from the initial state to \( \sigma \) is constructed. The data to do so is distributed among processors into local files, one per super step. We thus use exactly as many steps to rebuild the trace as we have used to reach \( \sigma \). The algorithm is presented in Fig. 6: a trace \( \pi \) whose “oldest” state is \( \sigma \) is reconstructed following the proof graph backward. The processor that owns \( \sigma \) invokes Local_trace to find a path from a state \( \sigma' \), that was in todo at the beginning of the super state, to \( \sigma \). Then it sends \( \sigma' \) to its owner to let the reconstruction continue. To simplify things, we print parts of the reconstructed trace as they are locally computed. Among the predecessors of a state, we always choose those that are not yet in the trace \( \pi \) (\text{set_of_trace}(\pi) \) returns the set of states in \( \pi \)) and selects one with the minimal dfn value (using function \text{min_dfn}), which allows to select shorter traces.

### IV. Experimental Results

In order to evaluate our algorithm, we have used two formulas of the form \( \phi \cup \text{deadlock} \), where \text{deadlock} is an atomic proposition that holds iff state has no successor and \( \phi \) is a formula that checks for an attack on the considered protocol: Fml1 is the classical “secrecy” and Fml2 is “aliveness” [15] – which are the most common formulas for verifying security protocols. The chosen formulas globally hold so that the whole proof graph is computed. Indeed, on several instances with counterexamples, we have observed that the sequential algorithm can be faster than the parallel version when a violating state can be found quickly: our parallel algorithm uses a global breadth-first search while the sequential exploration is depth-first, which usually succeeds earlier. But when all the exploration has to be performed, which is widely acknowledged as the hardest case, our algorithm is always much faster. Moreover, we sometimes could not compute the state space sequentially while the distributed version succeeded, thanks to the distribution of states and sweep-line strategy — which is also used for sequential computing.

We have implemented a prototype version in Python, using SNAKES [16] for the Petri net part (which also allowed for a quick modelling of the protocols, including the Dolev-Yao attacker) and a Python BSP library [17] for the BSP routines (which are close to an MPI “alltoall”). We actually used the MPI version (with MPICH) of the BSP-Python library. While largely suboptimal (Python programs are interpreted and there is no optimisation about the representation of the states in SNAKES and the implementation of the attacker is not optimal at all), this prototype nevertheless allows an accurate comparison for acceleration. The benchmarks presented below have been performed using a cluster with 20 PCs connected through a 1 Gigabyte Ethernet network. Each PC is equipped with a 2GHz Intel® Pentium® dual core CPU, with 2GB of physical memory. This allowed to simulate a BSP computer with 40 processors equipped with 1GB of memory each.

Our case studies involved the following four protocols:

1. Needham-Schroeder public key protocol for mutual authentication;
2. Yahalom key distribution and mutual authentication using a trusted third party;
3. Otway-Rees
Figure 7. Benchmark results for the four protocols where Fml1 is "secrecy" and Fml2 "aliveness".

V. RELATED WORKS

A. Verification of security protocols

There are many tools dedicated to the modelling and verification of security protocols as [3], [19]. Most of them limit possible kinds of attacks or limit in their model language how addresses of agents can be manipulated in ad-hoc protocols (using arithmetic operations). Paper [20] presents different cases study of verifying security protocols with various standard tools. To summarise, there is currently no tool that provides all the expected requirements.

A distributed memory algorithm with its tool for verification of security protocols is described in [21]. The authors use buffering principle and employ a cache of recently sent states in their implementation to decrease the number of messages sent. Unfortunately, the verification of temporal properties is not supported due to the difficulties of combining the parallel checking with the symmetry reduction. [22] allows to verify some properties about some classes of protocols for an infinite number of sessions and with some possibility of replay using a process algebra. But no logic can be used here and each time a new property is needed, a new theorem needs to be proved. That can be complicated for the maintenance of the method. Also, the method cannot be applied to, e.g., the Yahalom protocol. On the contrary, our approach is based on a modelling framework with explicit state space construction, that is not tied to any particular application domain and our implementation using Python allows us to manipulate any kind of data-structures are used for the modelling protocols. Using Python has been shown a good trade-off between quick modelling and performance [12] and model compilation approaches can be successfully applied to compete with state-of-the-art tools as shown in [23]. So, instead of using a dedicated framework, our approach mainly relies on the particular structure of security protocols.

B. Distributed LTL checking

The main idea of most known approaches to the distributed memory state space generation is similar to the naive algorithm [24]. More references can be found in [5] and in [25] for high-level Petri nets. Close to our hashing technique, [26] presents a hashing function that ensures
that most of the successors are local. For load balancing, [27] presents a new dynamic partition function scheme that builds a dynamic remapping, based on the fact that the state space is partitioned into more pieces than the number of involved machines. When load on a machine is too high, the machine releases one of the partitions it is assigned and if it is the last machine owning the partition it sends the partition to a less loaded machine.

Very close to our idea, we can cite [28] which used a partition function that enables cycles for a parallel DFS algorithm to be local only (as for us) using SCC in the formula Büchi automata. The limits of the method are the cost of this function and furthermore the number of SCCs which is not enough to scale. [29] presents a distributed algorithm for SCC computation. In our work, all SCC are purely local, which is easier and more efficient to handle.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

There are now many tools that check the security of cryptographic protocols. But none is sufficient and adaptable for complicated scenarios. Using LTL for such applications is not new but we have exploited characteristics of these models to structure the parallel computations accordingly. Our solution is to use the well-structured nature of security protocols to choose which part of the state and formulas is really needed for the partition function and to empty the data-structure at each super-step of the parallel computation. Our solution also entails automated classification of states and dynamic mapping of classes to processors. We find that our method ensures good acceleration and allows to find small counterexamples due to its breadth-first search global strategy but DFS stategy on each processor. Furthermore, we find that our method to balance states does indeed achieve better network use, memory balance and runs faster than methods based on direct states exchanges.

The common method for LTL checking is using a Büchi automaton. Using proof-structures instead theoretically has the same worst-case time but it ensures to distinguish easily local and global successors for the distribution. We have demonstrated techniques that prove the feasibility of this approach and showed its potential. Key elements to our success were (1) an automated states classification that reduces cross transitions and memory footprint, while improving the locality of computation (2) using global barriers (which is a low-overhead method) to compute a global remapping of states and thus improve balancing workload, achieving a good scalability.

B. Future work

For future work we think about extending the logic and increasing the performances. First, proof-structures were used to check CTL* formula in [9]. We are currently working to extend our algorithm for this logic and we may also consider Past operators (in the manner of [30]) that proved to be useful for protocols [4]. Second, and more practical: we want to have a tool that could translate HSPSL models [4] into ABCD ones since HPSL is mainly used by the community; It will also allow us to test our algorithm on different attackers than the Dolev-Yao one. To optimize the performance, using a specific library as Divine [31] and model-compilation [23] will also be considered.

We are also working on the formal proof of our algorithm. Proving a verification algorithm is highly desirable in order to certify the truth of the delivered diagnostics. Such a proof is possible because, thanks to the BSP model, our algorithm remains simple in its structure which allows us to use a specific tool for checking BSP algorithms using Hoare logic [32]. Finally, we would like to generalise our present results by extending the application domain. In the security domain, we will consider more complex protocols with branching and looping structures, as well as complex data types manipulations. In particular, we will consider protocols for secure storage distributed through peer-to-peer communication [33], [34] because it is currently modeled using ABCD and generates large state spaces.

REFERENCES


