様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ２０ 日現在

機関番号：３４４０６
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ１１２６２

研究課題名（和文）経路保証プロトコルのモデル検査手法の開発

研究課題名（英文）A model checking method for secure routing protocols

研究代表者
小島　英春（Hideharu, Kojima）

大阪工業大学・情報科学部・准教授

研究者番号：９０６１０９４９

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究では，センサネットワークやアドホックネットワークで利用される経路保証プロトコルの形式検証を行う際に生じる状態爆発を抑制する手法の開発を行なった．基本的な考え方は，同じトポロジ形状であれば等価な状態とみなすことで走査する状態数を削減することである．また，対象とする経路保証プロトコルは，署名を用いて経路の正しさを保証するため，開発手法では，同じトポロジ形状であり等価な状態とみなしたトポロジであればそれぞれの署名も等価であるとみなす方法を組み込んでいる．この手法をモデル検査器SPINに適用し，経路保証プロトコルの検証を行ない，状態数が削減されること，実行時間の短縮を示すことができた．

研究成果の学術的意義や社会的意義
センサネットワークやアドホックネットワークが社会で展開されることを考えると，経路が構築されること，情報の通信経路が信頼できることが重要である．経路保障プロトコルは，それらを実現するものである．これを用いるにあたって，正しく動作するかどうかを事前に検証することが必要である．従来の方法では，状態爆発により検証の完了が困難である場合があることや検証に必要な実行時間が長くなることがあるが，本研究で開発した手法を用いて状態爆発を抑制することで，検証に必要な時間を削減することが可能となった．

研究成果の概要（英文）：In this research, we developed a method to suppress state explosion that occurs during formal verification of secure routing protocols used in sensor networks and ad hoc networks. The basic idea is to reduce the number of states to be traversed by regarding that states with the same network topology shape are equivalent. Since the target protocol uses signatures to guarantee the correctness of routes, the developed method incorporates a method that signatures included in the equvalent states are considered equivalent. We applied this method to the model checker SPIN to verify the secure routing protocol, and showed that the number of states is reduced and the execution time is shortened.

研究分野：情報学

キーワード：モデル検査　状態爆発抑制　経路保証プロトコル

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

IoT ネットワークは近年，政府が目指す超スマート社会において重要な役割を担うと考えられる．文献[1]では，一例として航空インダストリアル・インターネットを挙げている．この例では，飛行機や滑走路の状況という非常に重要な情報であるため，端末から届く情報は正しいのか，その通信経路は信頼できるものか，が非常に重要である．そこで，経路保証プロトコルを用いて通信経路の正しさを保証することにより，攻撃者からの偽の情報を排除することが必要となる．IoT ネットワークを構築する際に情報の送受信を行う通信経路が正しく構築されること，その通信経路が改竄されていないことを検証することの重要性がこれまで以上に増し，それらを効率よく検証する方法が必要となる．

アドホックネットワークの 1 つである IoT ネットワークでは，端末の参加・離脱・移動により無数のトポロジ変化が生じ，その全ての状況において正しく動作することを検証するために，状態の網羅を行うモデル検査は非常に適している[2]．本研究ではモデル検査を用いて，受信した情報がどのような経路を辿ってきたかを保証する経路保証プロトコルを効率的に検証する手法を開発する．経路保証プロトコルは，送信元宛先間の経路構築時に各端末が経路情報に署名を行い，経路情報と署名をパケットに載せて宛先まで届けることで，署名を通じて経路情報の正しさを保証する．経路保証プロトコルはルーティングプロトコルであるため，モデル検査では，送信元宛先間に経路を構築できることを検証する．

２．研究の目的

アドホックネットワークやセンサネットワークでは，前述した通り，端末が動的に移動，ネットワークへ参加，離脱が生じる．このようなネットワークでは，構築可能な通信経路が非常に多くなることが考えられ，端末数が増加した場合は，それが爆発的に増加することが考えられる．これは，モデル検査において状態数が爆発的に増加することを示しており，現実的な時間では，モデル検査が完了しないことが考えられる．そこで，本研究の目的は，端末数がした際にモデル検査において生じる状態爆発を抑制するための経路保証プロトコルの効率的なモデル検査手法の開発である．次の 2 点を行い，モデル検査ツールの実装を行う．

３．研究の方法

本研究を進めるにあたり，以下の 2 つの方法を開発し，対象となる経路保証プロトコルに適用する．また，状態数削減手法については，対象となる経路保証プロトコルの元となるプロトコルである DSR を対象にする．まずは，元となる DSR を対象に状態数削減手法を開発し，その後に，その手法を対象となる経路保証プロトコルである ISDSR に適用できるように，署名の扱いについての機能を追加する．

状態数削減手法の開発

状態数削減手法の 1 つとして，Symmetry Reduction がある．これは，同じ動作を行うプロセスの状態の対称性を利用して，複数の状態を等価な状態として扱うことで状態数を削減し，その中の 1 つを代表元として等価な状態を表す状態として扱う．本研究では，トポロジ形状を代表元との等価判定に用いて Symmetry Reduction を行う．トポロジ形状が同じ場合は，対応する端末が決まるため，置換の組合せを限定することが可能となる．またトポロジ同型判定を行う必要があるため，効率的な同型判定方法の開発を行う．これにより，状態数の削減を行う．

状態数削減手法を用いた場合の経路保証に用いられる署名の扱い

前述した状態数削減手法を用いた場合，等価な状態とみなす必要があるが，それらの状態におけるトポロジの端末の並びが異なるという状況が生じる．端末の並びが異なるため，それぞれの状態における署名は異なる．この場合，トポロジ形状が同じ，その時点で署名の検証が真である場合には，同じ状態とみなし，Symmetry Reduction の適用をすることで，署名を含めて状態を等価とみなすようにする手法を開発する．

４．研究成果

状態数削減手法を開発し，それをリアクティブ型のルーティングプロトコルである，DSR と AODV に適用した結果は以下のとおりである．SPIN を用いて，DSR と AODV のモデルを作成し，開発手法を適用した場合と適用しない場合において状態数と実行時間，主記憶利用量を計測した．

表．1：DSR を対象に開発手法を適用した場合としない場合の比較

	状態数		実行時間［秒］		主記憶利用量［MB］	
端末数	開発手法あり	開発手法なし	開発手法あり	開発手法なし	開発手法あり	開発手法なし
7	49305	160455	0.23	0.58	22.306	70.265
8	321720	1282087	2.00	5.48	168.958	652.511
9	2307542	12379809	22.7	72.3	1437.843	7420.864

表．2：AODV を対象に開発手法を適用した場合としない場合の比較

	状態数		実行時間［秒］		主記憶利用量［MB］	
端末数	開発手法あり	開発手法なし	開発手法あり	開発手法なし	開発手法あり	開発手法なし
4	597	1065	< 0.01	< 0.01	0.16	0.28
5	1869	8694	0.01	0.03	0.59	2.72
6	5409	88265	0.12	0.42	1.99	32.32
7	14828	1075348	1.72	13.30	6.22	451.23
8	39005	15275465	31.6	938	18.45	7225.64
9	99348	-	626	T. O.	53.06	-
10	246609	-	1.42×10^4	T. O.	144.87	-

表．1 と表．2 ともに，状態数，実行時間，主記憶利用量ともに，開発手法を適用した場合の結果が優れている．この結果より，開発した状態数削減手法は，モデル検査において状態数を大きく削減できると考えられる．また，ここでの T. O.は，指定した実行時間以上の時間が必要であったことを示している．端末数が増加すると開発手法を適用した場合も状態数が増加しているが，開発した手法を適用しない場合に比べて上昇の割合が緩やかである．

表．3：ISDSR を対象に開発手法を適用した場合としない場合の比較

	状態数		実行時間［秒］		主記憶利用量［MB］	
端末数	開発手法あり	開発手法なし	開発手法あり	開発手法なし	開発手法あり	開発手法なし
4	334	542	0.31	0.22	131	133
5	1195	4009	2.12	0.73	138	159
6	6388	29072	10.3	3.95	185	387
7	35284	213419	108	29.4	496	2348
8	191072	1665776	1.51×10^3	225	2415	19698
9	1004558	-	2.36×10^4	T. O.	13736	-

表．3 は，経路保証プロトコルである ISDSR に開発手法を適用したものである．状態数，主記憶利用量は端末数が増加すると大きく削減されているが，実行時間については，端末数 8 までは開発手法を適用した方が長くなっている．しかし，端末数が 9 になると開発手法を適用していないものは指定した実行時間内に検証が終わらなかったが，適用した場合は検証を完了している．経路保証プロトコルを対象にしているため，署名も含めた状態の等価判定に時間がかかっていることが考えられる．

これらから，本研究で開発した手法は，状態数を大きく削減するとともに，主記憶の利用量も合わせて削減することが可能である．また，実行時間に関しては，端末数が増加して開発手法を適用しない場合にはタイムアウトになるようなモデルに対しても検証が完了することを示している．

[1]:山田 直史，高島 洋典，木村 康則，“超スマート社会（Society5.0）実現に向けて：CPS／IoT とその後，” 情報管理，Vol. 60，No. 5，pp. 325-334，2017

[2]: J.Qadir et al.，“Applying Formal Methods to Networking: Theory, Techniques, and Applications，” IEEE Communications Surveys & Tutorials, 17(1), pp.256-291, 2015

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Kojima Hideharu、Yanai Naoto、Cruz Jason Paul	４．巻 7
２．論文標題 ISDSR+: Improving the Security and Availability of Secure Routing Protocol	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 74849～74868
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2916318	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Kojima Hideharu、Yanai Naoto
２．発表標題 A Model Checking Method for Secure Routing Protocols by SPIN with State Space Reduction
３．学会等名 2020 IEEE International Parallel and Distributed Processing Symposium Workshops(APDCM2020)（国際学会）
４．発表年 2020年

１．発表者名 Shinnosuke Shimizu, Hideharu Kojima, Naoto Yanai, Tatsuhiro Tsuchiya
２．発表標題 Implementation and Evaluation of ISDSR in Emulation Environments
３．学会等名 2019 IEEE Wireless Communications and Networking Conference, WCNC2019（国際学会）
４．発表年 2019年

１．発表者名 Hideharu Kojima, Naoto Yanai
２．発表標題 A State Space Reduction Method for Model Checking of Wireless Multi-hop Network Routing Protocols Focusing on Topologies
３．学会等名 Seventh International Symposium on Computing and Networking Workshops, CANDAR 2019 Workshops（国際学会）
４．発表年 2019年

１．発表者名
Hideharu Kojima, Naoto Yanai

２．発表標題
A State Space Suppression Method for Formal Verification of Secure Routing Protocols With SPIN

３．学会等名
IEEE International Symposium on Software Reliability Engineering Workshops, ISSRE Workshops 2019（国際学会）

４．発表年
2019年

１．発表者名
小島英春，矢内直人

２．発表標題
経路保証プロトコルを対象にしたSPIN を用いたモデル検査にむけて

３．学会等名
第16回電子情報通信学会ネットワークソフトウェア研究会，

４．発表年
2018年

１．発表者名
小島英春，矢内直人

２．発表標題
アドホックネットワークプロトコルのモデル検査における状態数削減手法

３．学会等名
第18回電子情報通信学会ネットワークソフトウエア研究会予稿集

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	矢内　直人 (Yanai Naoto) (30737896)	大阪大学・大学院情報科学研究科・准教授 (14401)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関