http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (23): 7185-7192, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.7185.7192

Improvement of CMP1 Protocol and Analysis of Petri Net

[1]Junmin Zhao, [1]Yi He and [2]Bei Lu
[1]Institute of Computer Science and Engineering, Henan University of Urban Construction, Pingdingshan, China
[2]Jiao Zuo Tian Yi Technology Co. Ltd, Jiaozuo, China

Abstract: In this study, the author conducts an in-depth research of the electronic commerce protocol CMP1 and finds the problem of redundant design of CMP1 protocol. Besides, the CMP1 protocol does not meet the requirements of fairness and timeliness and it is likely to suffer replay attack and problems like that. In view of the insufficiency of CMP1 protocol, this study puts forward the corresponding improvement scheme and put modifications on the protocol. The improved CMP1 protocol makes up for the previous flaws. Then, the color Petri net protocol analysis method is adopted to model and simulate the modified CMP1 protocol and the properties of the new protocol are analyzed as well. The simulation results prove that the improved protocol can not only meet the requirements of accountability, fairness and timeliness but also avoid the possibility of replay attack.

Key words: CMP1 protocol, color petri net, CPN tools, state analysis

INTRODUCTION

With the rapid development of Internet, e-commerce also has sprung up and expanded rapidly, which has become an indispensable part of our daily life. However, the existing unsafe factors of the Internet makes people doubt the reliability of e-commerce and e-commerce security has become a very important issue. Therefore, a series of security measures must be taken to ensure the healthy development of e-commerce. Among the current ways to solve the security problems in e-commerce, protocols based on passwords are of the most effective ways to solve the problems existing in e-commerce security. Nonetheless, the design process of electronic commerce protocols is complex and easy to get wrong; more or less bugs exist in the current comparative mature e-commerce protocols, which to some extent restrict the development of e-commerce. E-commerce protocols are security protocols for electronic trading, which run in the open internet environment. Therefore, e-commerce protocols must not only possess the functions of safety agreement but also meet the requirements of accountability, fairness, timeliness and other special requirements in order to ensure the effectiveness of the trading (Bolignano, 1997). The requirement of accountability means that if there is a trade dispute or either party intentionally denies after the agreement operation, each side can take out the evidences which could prove that the other party is involved in the agreement and sends some news as well as receives some. The sender owns the non-repudiation evidence POR (proof of receipt) or EOR (evidence of receipt) of the receiver, the receiver pocesses the non-repudiation evidence of POO (proof of origin) or EOO (evidence of origin) of the sender, among which POO and POR are prescribed during protocol designing. Fairness means that if the e-commerce protocol is terminated unexpectedly in the process of running, the sender can receive the non-repudiation evidence (POR) if and only if the receiver receives the non-repudiation evidence (POO).

Timeliness is that the execution of the agreement should be finished in a certain time period. If there is a communication channel failure, or either the sender or the receiver involved in the agreement hinders the execution of the agreement no matter when and no matter what the purpose is, the protocol can continue to perform after a period of time so as not to damage the fairness of agreement. Since e-commerce protocols need to satisfy multiple special requirements, many factors should be taken into consideration in the design process of e-commerce protocols, even a well-designed e-commerce protocol also tend to have many security flaws. For instance, Needham-Schroeder protocol and Kerberos protocol were initially considered safe but proved to have a serious vulnerability 17 years later (Lowe, 1996).

The author firstly conducts an in-depth research into CMP1 protocol, finding some shortcomings like existence of redundancy, not meeting the requirements of fairness and timeliness and possibility of taking replay attack and so on. Then, aiming at these deficiencies, revision plans

Corresponding Author: Junmin Zhao, Henan University of Urban Construction, China

are put forward and changes of the agreement are made. Finally we make use of color Petri net protocol analysis method to model and simulate the new CMP1 protocol and analyze properties of the new protocol such as accountability, fairness, timeliness and replay attacks. The results show that the improved CMP1 protocol can meet the requirements of accountability, fairness, timeliness and not taking replay attack of the e-commerce.

INTRODUCTION TO CMP1 PROTOCOL AND ANALYSIS OF THE DEFECTS

CMP1 (Certified Electronic Mail) (Deng *et al*., 1996) protocol is one electronic trading agreement in electronic commerce protocol, which is put forward by Deng *et al*. (1996) and the purpose of which is to provide non-repudiation service for e-mail transmission. A specific description of the agreement is as follows:

$$EOO:\{m\}_{k_a^{-1}}$$

$$EOR:\{h(m)\}_{k_b^{-1}}$$

- $A \rightarrow B:h(m),\{k\}_{K_{TTP}},\{\{m\}_{k_a^{-1}}\}_K$
- $B \rightarrow TTP:\{h(m)\}_{k_b^{-1}},\{k\}_{K_{TTP}},\{\{m\}_{k_a^{-1}}\}_K$
- $TTP \rightarrow B:\{\{m\}_{k_a^{-1}}\}_{K_{TTP}^{-1}}$
- $TTP \rightarrow A:\{\{h(m)\}_{k_b^{-1}},(B,m)\}_{K_{TTP}^{-1}}$

Step 1: Entity A sends the summary h (m) of message m, the session key $\{k\}_{KTTP}$ which is encrypted by the public key of TTP and the signature of TTP as well as ??? encrypted by the session key K to entity B

Step 2: Entity B signs the summary h (m) and sends it to TTP together with $\{k\}_{KTTP}$ and $\{\{m\}_{k_a^{-1}}\}_K$

Step 3: After receiving the message sent by entity B, TTP decrypts the ciphertext with the session key K and signs it with its own private key and uses it as NOO to be sent back to entity B

Step 4: TTP signs the summary $\{h(m)\}_{k_b^{-1}}$ and (B, m) which have already been signed by entity B with its own private key and regards it as NOR to be sent to entity B

Properties of accountability, fairness and timeliness and so on are important indicators to measure the effectiveness of e-commerce protocols. After analyzing the process of implementation, we find many defects exist in CMP1 design. For example, protocol statements (1) is quite redundant. Entity A can skip the step of using session key K but uses the TTP public key $\{k\}_{KTTP}$ to sign $\{m\}_{k_a^{-1}}$ directly. Qing Sihan and others found redundancy in the design of EOO and EOR in CMP1 protocol too (Qing, 2003). Just making $EOO=\{m\}_{k_a^{-1}}$, $EOR=\{h(m)\}_{k_b^{-1}}$, $(B,m)_{K_{TTP}^{-1}}$ can meet the corresponding requirements; statement (3) and (4) in the protocol can also be simplified in the same way. Zhou Diancui and others found the protocol is not fair under the condition of unreliable communication channels (Zhou *et al*., 2001). When joining the FTP operation in step (3) and (4) of the protocol, the CMP1 protocol can satisfy fairness under the condition of unreliable communication channels. Xilin and others found that defects like clear exposure and taking replay attack exist in CMP1 protocol (Lin and Zhao, 2007). Problems can be solved if we encrypt some of the meaasges where clear message is easy to expose in the protocol and improve the statements which are easy to take replay attack. Loophole of the timeliness exists in protocol statement (2): If the participant entity B is dishonest and delays to send message to TTP and does not send it until entity A withdraws from the protocol because EOR is overtime. Then, entity B gets EOO sent by TTP, while entity A can not get EOR since it has already dropped out of the protocol. In this way, the protocol loses its fairness. This defect can be solved by increasing information of timeliness in the protocol.

E-commerce security is a very important matter and the protocol must meet the requirements of timeliness and fairness and also avoids the possibility of taking replay attack and so on to ensure its effectiveness. Therefore, the CMP1 protocol must be improved to fully meet the requirements of e-commerce protocols and to serve electronic commerce much better.

IMPROVEMENT OF CMP1 PROTOCOL

Aiming at the defects and flaws of CMP1 protocol, this study makes modification and improvement of it. The modified protocol statements are as follows:

$$EOO:\{\{m\}_{K_b}\}_{k_a^{-1}}$$

$$EOR:\{h(\{m\}_{K_b})\}_{k_b^{-1}},\{(B,\{m\}_{K_b})\}_{K_{TTP}^{-1}}$$

- $A \rightarrow B:h(\{m\}_{K_b}),\{\{\{m\}_{K_b}\}_{k_a^{-1}}\}_{K_{TTP}},\{T\}_{k_a^{-1}}$
- $B \rightarrow TTP:\{h(\{m\}_{K_b}),\{T\}_{k_a^{-1}}\}_{k_b^{-1}},\{\{\{m\}_{K_b}\}_{k_a^{-1}}\}_{K_{TTP}}$
- $B \leftrightarrow TTP:\{\{m\}_{K_b}\}_{K_a^{-1}}$
- $A \leftrightarrow TTP:\{\{h(\{m\}_{K_b})\}_{k_b^{-1}},\{(B,\{m\}_{K_b})\}_{K_{TTP}^{-1}}$

Operating conditions for new CMP1 protocol: New CMP1 protocol operation is based on the following assumptions:

- The assumption of the channels to run protocol: Set a longest time span for the network to be available, that is to say the network will not be permanently unavailable. This assumption is often used in the analysis of e-commerce protocols
- Since two time constraints are introduced in the the protocol, every entity needs to have a unified time system. It is assumed that TTP can provide time query service and both entity A and B can get time points from TTP. This assumption is easy to implement, just needing TTP to provide its own time in public access catalogue

Implementation process of new CMP1 protocol: Each step of the protocol execution will be analyzed in the following part:

- **A→B:** In this step, entity A sends entity B the summary h ($\{m\}_{Kb}$) of ciphertext $\{m\}_{Kb}$, the ciphertext $\{\{\{m\}_{K_b}\}_{K_a^{-1}}\}_{K_{TTP}}$ which is obtained through encrypting ciphertext $\{m\}_{Kb}$ by using the private key and the TTP key and the ciphertext $\{T\}_{k_a^{-1}}$/ which is obtained through encrypting T with the private key.
- Entity A gets the current time T_{nowA} through time query service provided by TTP and uses it as the time when entity A starts the protocol. Then we calculate the time constraint T = T T_{nowA}+t when entity B submits information to TTP. In the equation, t stands for the time that entity B needs to submit message to TTP from the moment T_{nowA}; $\{T\}_{k_a^{-1}}$ is the signature of entity A to T in order to prevent entity B from changing T optionally. The original CMP1 protocol was complex for it needs to encrypt $\{m\}_{k_a^{-1}}$ using the session key K and transmits K to entity B. The improved CMP1 protocol uses TTP public key instead of the session key K, which simplifies the protocol contents and improves the protocol efficiency.
- **B→TTP:** Entity B signs the summary h ($\{m\}_{Kb}$) and $\{T\}_{k_a^{-1}}$ with its own encryption key and sends $\{h(\{m\}_{K_b}),\{T\}_{K_a^{-1}}\}_{K_b^{-1}}$ and $\{\{\{m\}_{K_b}\}_{k_a^{-1}}\}_{K_{TTP}}$ to TTP

Entity B decrypts $\{T\}_{k_a^{-1}}$ after receiving it to gets T and gets T_{nowB}, the current time of TTP. If entity B agrees to the duration T that entity A sets to submit messages to TTP and T_{nowB} does not exceed T, then entity B needs to submit messages to TTP before the moment T. After receiving the message sent by entity B, TTP first verifies the signatures of entity A and B in $\{T\}_{K_a^{-1}}$ $\{T\}_{K_b^{-1}}$ and decrypts it to get T, then compares the current time point and T. If the current time is not over the period T, TTP will generate EOR and EOO and puts them in the public access catalogue, remaining until the moment $T+t_c+x$ (x>0) (It is assumed that longest time for the network to be unavailable is T_c. In this way, both entity A and B can get their deserved evidence from TTP through FTP operation. If the current time exceeds the period T, TTP considers the message sent by B is invalid and will not release EOR and EOO to terminate the protocol operation. In this step, only ciphertext $\{m\}_{Kb}$ can be got from TTP decryption, which ensures the confidentiality of the message m.

- **B↔TTP:** After entity B sends the message to TTP, it constantly check the public catelogue of TTP to determine whether there is the evidence of EOO. If entity B has not got the evidence of EOO by the time $T+t_c+x$ (x>0) on TTP, entity B considers the protocol has been terminated before TTP producing the evidence of EOO
- **A↔TTP:** Entity A keeps checking the public catelogue of TTP to determine whether there is the evidence of EOO. If entity A has not got the evidence of EOR by the time $T+t_c+x$ (x>0) on TTP, entity A considers the protocol has been terminated before TTP producing the evidence of EOR

The statements in the modified CMP1 protocol are much simpler. It can satisfy requirements of accountability, fairness, timeliness and not taking replay attacks as well as other attributes whether the channel is reliable or not.

ANALYSIS OF PETRI NETWORK IN THE NEW PROTOCOL

Electronic commerce protocol is the important guarantee of e-commerce activities can be performed safely. Attributes of e-commerce like accountability, fairness, timeliness and not taking replay attack are important indicators to measure whether an electronic commerce protocol is safe or not. The authors finds that there are loopholes in the classic CMP1 protocol and mends them to improve the efficiency of the protocol.

On the basis of color Petri net and CPN Tools (Panagiotis *et al*., 2005), we investigate the attributes of accountability, fairness, timeliness and not taking replay attack of the modified CMP1 protocol, to validate security properties of it. We adopt layered color Petri net (Xu *et al*., 2011; Lu, 2012.) to model the protocol, run the

model for simulation in CPN Tools and analyze as well as verify the security attributes of the new protocol by use of the state space analysis tools and query function method. In the process of analysis, we assume that the channel can be either reliable or unreliable, that neither entity A nor B is honest, that TTP is fair.

Modeling of the protocol: In order to model the protocol more clearly and accurately, we adopt hierarchical Petri net modeling method from top to bottom. In the first step, we establish entity models for each protocol participant and connect all the entities according to the process of the protocol and imitate the process of message transferring. Then, we establish a top-level model for the protocol to represent each subject with substitution transitions and display the process of message transmission clearly. Finally, we perfect the process of message circulation of each model and make necessary program decisions in the change or the output arcs according to the requirements of the protocol, in order to achieve the most perfect protocol modeling:

- **Color sets and variables:** Figure 1 below shows all sorts of color sets and variables that the improved model of CMP1 protocol established. We use a simple color set to represent public and private keys that each entity owns, as well as represent simple message types. We use composite message sets to represent complex message sets and customize some decision function used to verify signatures or produce corresponding time information. Each type of color set has a corresponding color variable
- **Top layer model:** By the implementation of the process, we can easily establish a top layer model. Library A2B, B2T, T2A, T2B respectively indicate that two entities send messages to each other. Among them, three substitution transitions A, B and TTP are the abstracts of each entity, which have their own corresponding submodels. The top layer model is shown in Fig. 2
- **Entity A:** According to the protocol of the statement, entity A encrypts m by using public key K_b of B to get encrypted message (m, K_b), then generates message hm after hash operation and gets ms after the signature operation through GHM change. The signed message will be encrypted by using TTP public-key K_t. The time point T when entity B submits message to TTP is randomly generated and signed, together with the former two parts hm and ms will be sent to entity B. The model of entity A is as shown in Fig. 3
- **Entity B:** After receiving the message that entity A sends, entity B decomposes the message and gets T by verifying the signature of A to T. Entity B signs T that entity A signed with its private key and sends it to TTP with the former two parts. Library b represents if entity B agree and true means agree, false disagree; library tf stores the results of whether entity B agree or not. Library tb, tf, b, vf and br partly simulates that if the time entity B sends messages to TTP meets the time requirement of entity A. The model of entity B is as shown in Fig. 4

```
colset PK=with Ka | Kb | Kt;
colset SK=with SKa | SKb | SKt;
colset M=with m | A | B | TTP;
colset H=with hs;
colset T=int with 0..100;
colset TB=int with 0..100;
colset ENC=product M*PK;
colset HASH=product H*ENC;
colset EOO=product ENC*SK;
colset E_S_E=product EOO*PK;
colset TS=product T*SK;
colset H_TS=product HASH*TS;
colset TS_S=product TS*SK;
colset H_S=product HASH*SK;
colset M_ENC=product M*ENC;
colset M_E_S=product M_ENC*SK;
colset MSG1=product HASH*E_S_E*TS;
colset MSG2=product H_S*TS_S*E_S_E*TB;
colset EOR=product H_S*M_E_S;
colset EB=union tfb:BOOL+eoo:EOO;
colset EA=union tfa:BOOL+eor:EOR;
var ta,tb,t:T;
var msg1:MSG1;
var msg2:MSG2;
var bb:BOOL;
fun VSig(pk:PK,sk:SK)= case (pk,sk) of
(pka,ska)=>true | (pkb,skb)=>true;
fun BagreeA(t:T,b:BOOL)=if b then discrete(0,t)
else discrete(t,100);
```

Fig. 1: Declaration of color Sets

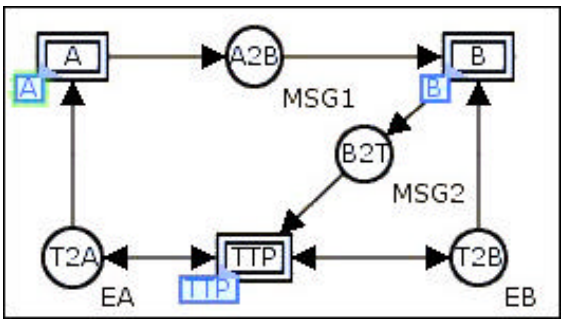

Fig. 2: Top layer model

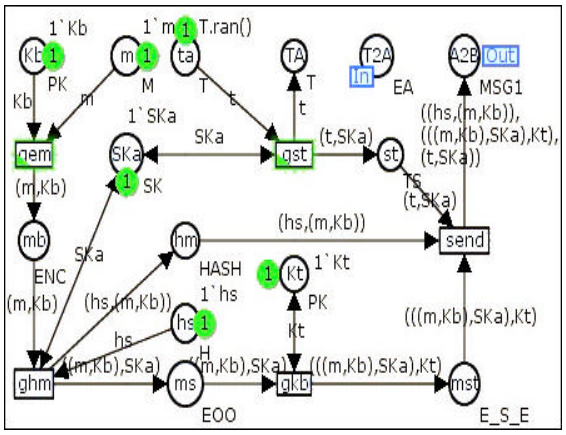

Fig. 3: Model of entity A

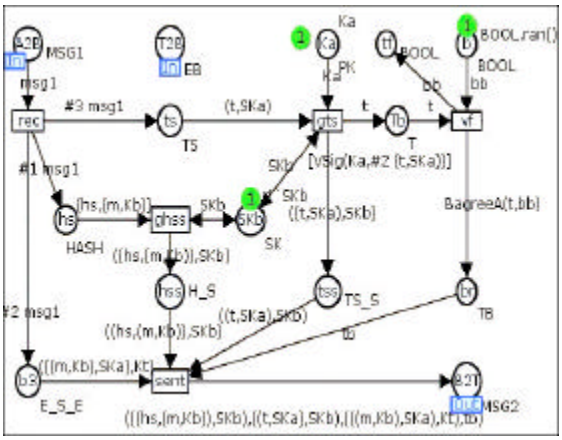

Fig. 4: Model of entity B

- **Entity TTP:** Entity TTP decomposes the message that entity B sent to generate EOO and EOR, then verifies if the time entity B submits message meets the time that entity A requires. If the time requirement of entity A is satisfied, then release EOO and EOR; if not, then EOO and EOR will not be released and a false token is used to show that EOO and EOR are not released. The model of the trusted third party TTP is shown in Fig. 5

Analysis of the protocol: We make use of the State Space Analysis tool in the CPN Tools to analyze the protocol. Firstly click Enter State Space tool to calculate all possible connected state of this model, then calculate the state space and the SCC state diagram, store the generated state space report in local disk. Part of the state space report is as follows:

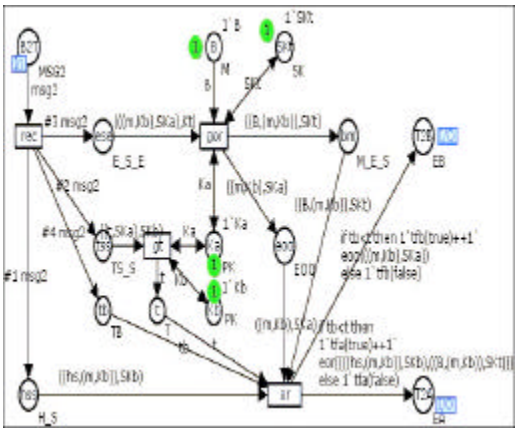

Fig. 5: Model of entity TTP

```
State Space
 Nodes: 27
 Arcs: 33
 Secs: 0
 Status: Full
 Scc Graph
 Nodes: 27
 Arcs: 33
 Secs: 0
Liveness Properties
Dead Markings: [27]
 Dead Transition Instances:
  None
 Live Transition Instances:
  None
```

As can be seen from the state space report, 27 nodes and 33 arcs are generated, among which the node [27] is a dead one. Below we will analyze each attribute of the protocol detailedly through adopting the state space report and query functions:

- **Accountability:** The accountability of e-commerce protocol means that all protocol participants shall be responsible for their actions (Kailar, 1996). In the events of dispute, all the protocol participants can provide effective evidence to ensure their own interests. The requirement of accountability is realized by non-repudiation evidences of the sender and non-repudiation evidence of the receiver. That is to say, after the completion of the protocol, we can guarantee that the sender can receive POR (proof of receipt) and the receiver can receive POO (proof of origin)

After the protocol is correctly executed, we run the query function SearchNodes () to inquire the result sets of each main entity. The purpose is to see if each entity has received corresponding non-repudiation evidences. If

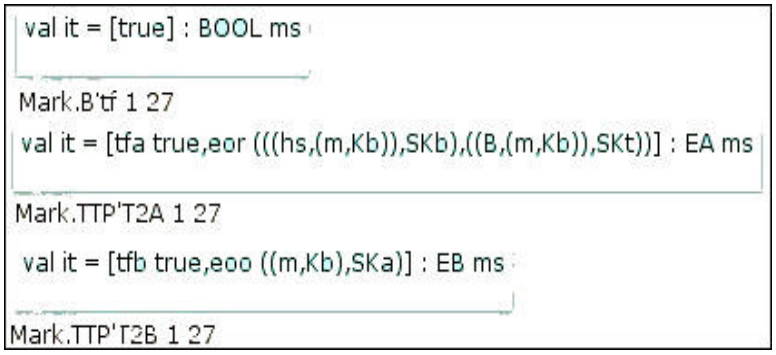

Fig. 6: Analysis of accountability

both entities receive corresponding non-repudiation evidences, then the protocol contents can meet the requirement of accountability. However, if neither entity receives corresponding non-repudiation evidences, then the protocol does not meet the requirement of accountability.

Under the condition of normal execution of the protocol: both entity A and entity B can obtain relevant evidence to satisfy the requirement of accountability, which can be seen from Fig. 6.

Fairness and timeliness: In the form analysis of e-commerce protocols, there are generally two steps. The first step is to verify if the protocol satisfies the requirement of accountability, while the second step is to verify the above definitions of fairness. In the process of execution of the protocol, if unexpected termination occurs, protocol participants should be in an equal status, neither side possesses the advantage (Gurgens *et al*., 2005). Namely, when the protocol runs over, the sender can receive evidence of POR and the receiver receives the evidence of POO. If dishonest participants in the protocol do not abide by time constraints, procrastinate or refuse to send messages, then protocol abnormalities could be lead to, which may affect the fairness of the protocol. Therefore, under the condition of different time, we get the nuanced model and calculate the state space of the model and run the query function. If one party receives non-repudiation evidences while the other party fails to obtain non-repudiation evidences, then the protocol does not meet the requirements of timeliness and fairness. Under the condition of various times, if both protocol participants have access to corresponding non-repudiation evidences or neither of them obtain corresponding non-repudiation evidences, and it is impossible for any party to obtain non-repudiation evidences while the other party does not obtain them, then the protocol meets the requirements of timeliness and fairness.

When messages that entity B submits meet the requirement of entity A, then the token of library b in the model of entity is 1, which means entity B generates messages and sent them out in the stipulated time that entity A requires. On the output arc of VF changes, we make use of a user-defined function B agree A (T, BB) to generate the time when B submits message. Finally, through the simulation run of CPN tools, we use the query function to inquire results.

As shown in Fig. 7, both A and B acquire the corresponding evidences, and at the same time there is no unsafe state, so it satisfies the requirement of fairness in this case.

When messages that entity B submits do not meet the requirement of entity A, then the token of library b in the model of entity is 0, which means entity B generates messages and sent them out in the stipulated time that entity A makes. On the output arc of VF changes, we make use of a user-defined function B agree A (T, BB) to generate the time when B submits message. Finally, through the simulation run of CPN tools, we use the query function to inquire results. As shown in Fig. 8, neither A nor B acquires the corresponding evidences and there is no unsafe state, so the requirement of fairness can also be satisfied in this case.

Replay attack analysis: assuming that entity A is the attacker or there is an external attacker entity C, and entity A or C intercepts message M that entity B sends to TTP. Since entity B has signed with the private key in message M, the approach in which entity A or C attempts to change T to delay to submit message M can not be achieved. If entity A or C sends M to TTP before time T, entity A and B can get EOR and EOO, respectively and

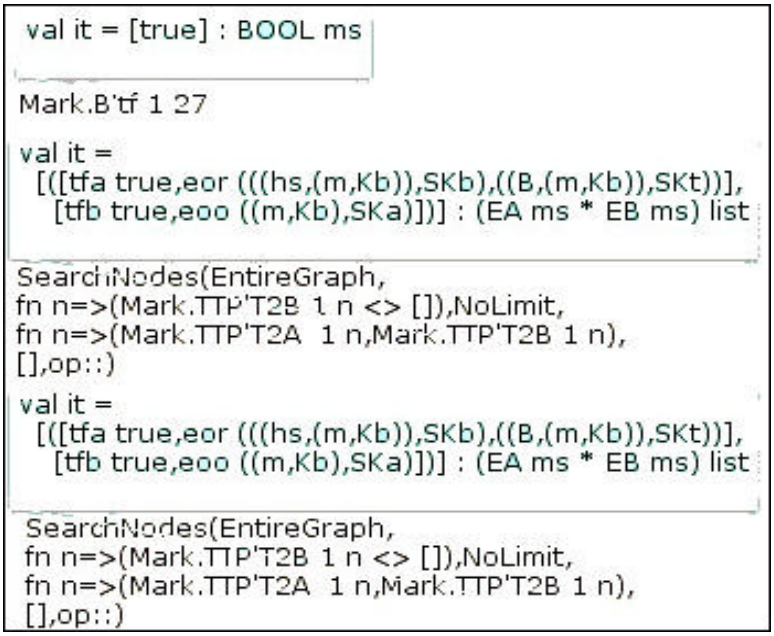

Fig. 7: Messages entity B submits meet the requirement of entity A

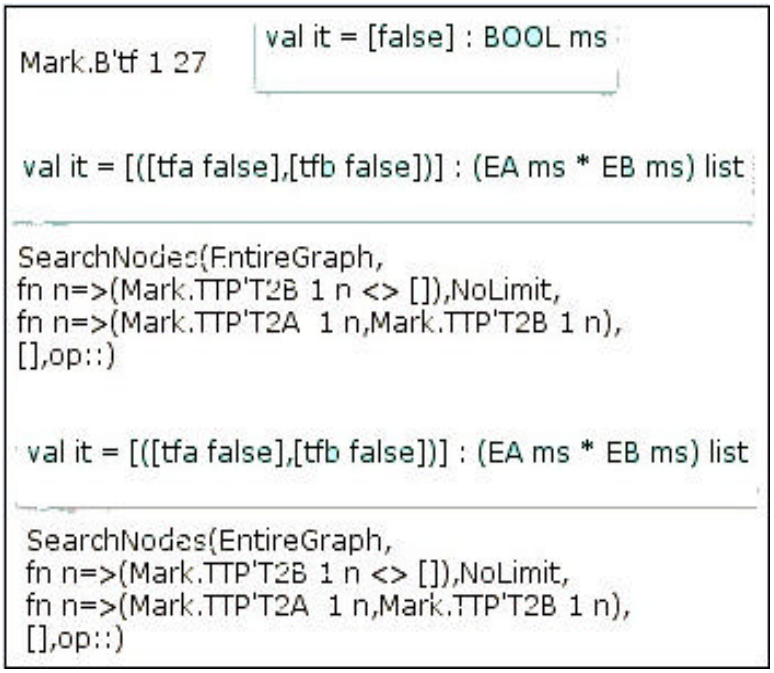

Fig. 8: Messages entity B submits do not meet the requirement of entity A

entity C can get EOR or EOO. However, since entity C does not have the private key of entity B and cannot decrypt or obtain plaintext of message M, so the fairness will not be affected. If entity A or C sends message M to TTP after time T and TTP will check whether the current point meet the condition. Obviously, this condition is

hard to be satisfied, then TTP will not release EOR and EOO and the protocol ends ahead of schedule. Finally, the attacker entity A or C does not get the any benefit and replay attack fails to work, not affecting the fairness of the protocol. Therefore, the modified CMP1 protocol does not take the replay attack.

In conclusion, the improved protocol satisfies the requirements of accountability, fairness, timeliness and replay attack.

CONCLUSION

E-commerce protocol is the basis the secure e-commerce activities to be carried out. In this paper, the authors carry on thorough analysis of the classic electronic commerce protocol CMP1, finding some shortcomings like existence of redundancy, not meeting the requirements of fairness and timeliness and possibility of taking replay attack and so on. Then, aiming at these deficiencies, revision plans are put forward and changes to the protocol are made. At the same time, the authors propose a new CMP1 protocol. Petri net method is a method with strict mathematical foundation and advantages of powerful analytical tools, and it has been successfully used in many fields. In order to validate the security of the improved protocol, this authors use color Petri net method to model the new protocol, and use the CPN Tools simulation Tools to simulate and analyze the improved CMP1 protocol. Also, the improved CMP1 protocol is investigated by using the state space analysis tools and query function. The results of the investigation show that the improved CMP1 protocol can meet the requirements of accountability, fairness and timeliness, and there is no risk of taking replay attack. Although color Petri net method can effectively analyze properties of accountability, fairness and timeliness in e-commerce protocols, there are limitations exist in the method. In the following study, the authors plan to study atomicity, anonymity and confidentiality of e-commerce protocols by using color Petri net method.

REFERENCES

Deng, R.H., L. Gong, A.A. Lazar and W. Wang, 1996. Practical protocols for certified electronic mail. J. Network Syst. Manage., 4: 279-297.

Bolignano, D., 1997. Towards the formal verification of electronic commerce protocols. Proceedings of the 10th Computer Security Foundations Workshop, June 10-12, 1997, Rockport, MA, USA., pp: 133-146.

Lowe, G., 1996. Breaking and fixing the needham-schroeder public-key protocol using FDR. Proceedings of the 2nd International Workshop on Tools and Algorithms for the Construction and Analysis of Systems, March 27-29, 1996, Passau, Germany, pp: 147-166.

Lu, B., 2012. A method of analyzing e-commerce protocols based on colored petri nets. YanShan University, pp: 15-26.

Panagiotis, K., V. Odontidis and M. Gousidou-Koutita, 2005. Colored Petri Net based model checking and failure analysis for E-commerce protocols. Proceedings of the 6th Workshop and Tutorial on Practical Use of Colored Petri Nets and the CPN Tools, October 24-26, 2005, Aarhus, Denmark, pp: 267-283.

Qing, S.H., 2003. Twenty years development of security protocols research. J. Software, 14: 1740-1752.

Kailar, R., 1996. Accountability in electronic commerce protocols. IEEE Trans. Software Eng., 22: 313-328.

Gurgens, S., C. Rudolph and H. Vogt, 2005. On the security of fair non-repudiation protocols. Int. J. Inform. Security, 4: 253-262.

Lin, X. and D.M. Zhao, 2007. Limitations and improvement of CMP. Microcomput. Inform., 23: 32-33.

Xu, Y., X.Y. Xie and H.G. Zhang, 2011. Modeling and analysis of electronic commerce protocols using colored petri nets. J. Software, 6: 1181-1187.

Zhou, D.C., S.H. Qing and Z.F. Zhou, 2001. A new approach for the analysis of electronic commerce J. Software, 12: 1318-1328.