New Defense System of Military Network based on Minimization of Counterexamples Algorithm on Model Checking

JIANG Jian-ping[1,a], XING Qing-long[2,b], Deng Wei[3,c]

93 unit of 91388 Army, Zhan Jiang of Guang Dong 524022

[a]14759362@qq.com, [b]xql@163.com, [c]chenlizhidengwei@163.com

Keywords: network security; model checking; counterexample; protocol

Abstract. Network is the basis of the army informationization construction, and security is the guarantee for the army informationization construction. The article firstly analyzes the hidden trouble of the military network and the lack of defense methods, and then introduces a new defense system of military network based on minimization of counterexamples algorithm on model checking, to analyze the validity of the network security protocols. The algorithm, based on the algorithm Gastin P proposes, and then given an informal analysis on the well-known Needham-Schroeder public-key authentication protocol, can provide quite efficient and omnidirectional security for military networks.

Introduction

At present, our army is in the key period of new military changes-the new stage of compound develop of mechanization with information, an important contents of information construction is a quick development of network construction. Along with the extension of the network scale, the exaltation of the applied level for OA, the degree of data share and commutation is also more and more high, rely on a calculator network more and more while changing an old work method. The creation, replication, deliver, report, destroy of secret content file mostly all to carry on on the calculator network, the electronics text file is more difficult to control and more easily to divulge than secret document of former paper quality [1].

The troops calculator network differs from other networks, it carries out a special task, and its safety directly relates to the victory or defeat of the war and the peace or chaos of the nation.How to ensure the safety of troops calculator network, putting a rigorous topic in front of us. Currently, most parts of our army calculator networks have already used various kind of safe product, such as fire wall, the detection system to inbreak, the virus protection system, the audit system of information, loophole scanning system etc., they all take safe communication protocol as the foundation and precondition, guaranteed the safety of troops network environment to some extent, however, each safe product still keeps basically staying around the situation of "single soldier's battle", formed an independent and passive protection to the network, didn't solve a network safe problem from the whole angle, the brief integration and fold to add already can not answer for the more and more complicated network environment and safety, various safe product based on correspondence safety protocol, can not provide enough overlay rate to satisfy the full and complete request of system verification.

Aiming at the special request of troops network safety, the writer tries to set out from the technical angle and combine the famous Needham-Schroeder public key identity attestation protocol, putting forward a new algorithmic frame, making various safe technique, equipments to farthest exert respectively, setting up the impregnable fortress to protect troops network safety.

The main correspondence protocol

Invade detection|break protocol（IDBP）

The protocol mainly used to correspondence between the fire wall and the invade detection system.Because these two kinds of techniques of fire wall and invade detection have stronger repairability with each other, therefore the protocol is the most important wreath in the whole safe

network protection system.When invade detection system detects a hacker to invade behavior on the network or the host, corresponding with interface of fire wall through IDBP protocol, noticing fire wall to make dynamic rule to achieve the control and break of invading behavior.

Information check filter protocol（ICFP）

The protocol is used to achieve the organic interaction between the fire wall and the check system for information contents.After the fire wall receives the information from the source host, the ICFP customer in the fire wall protocol requests the ICFP server of outer security equipment to carry on a check processing to the information through ICFP after info cache; according to needing, ICFP server carrys on operations such as character list to match, modification or secret level reviewing etc. to the information, and the result data after processed and response information were sent back to the ICFP customer in the fire wall;The ICFP customer according to the designation of response information, info cache combined with result data will be snet to the target host or break the information.In addition to synchronously checking mode, ICFP protocol still supports asynchronously checking mode, its main characteristics is an ICFP customer doesn’t need info cache, this kind of mode is adapted to a particular information check system, and the efficiency is higher.

Attestation service interface protocol（ASIP）

ASIP protocol is mainly used for organic interaction between fire wall and attestation system.After the customer passes the identity discrimination of attestation system firstly, the attestation system notify the fire wall to make dynamic customer|set rule through ASIP protocol, achieving the percolation strategy according to customer's identity.

Remote management protocol（RMP）

The RMP protocol opened the remote management interface of fire wall system, it can safely access the safe strategy and safe rule(dynamic rule|static rule) of fire wall system remotely through the RMP protocol, and carry on corresponding operation such as reading and modifying. More securities equipment can expediently interact with fire wall system deeply through RMP protocol.

The algorithm actualization

The safe protection system of troops' network based on minimization of counterexamples algorithm on model checking, which takes correspondence safety protocol as its foundation and premise, complicated day by day along with soft hardware system of calculator and network ,the onefold dynamic imitate method already can not provide enough overlay rate.Therefore, the formal verification method such as model detection is becoming the important means to verify the complicated system.Compared with other formal verification methods such as prove axioms, the main advantage of model detection lies in:When affirmer being breached, the model examination method can give counterexamples to explain the reason that affirm was breached.However, usually because of the very long counterexamples of complicated system, causing to comprehend very hard, and needing to cost a great deal of time to check great variable and events, to find out the source of error, these objective factors all directly influenced the efficiency of model detection verification.

Firstly, this stanza analyzes the algorithm idea that Gastin .P puts forward to find out the minimization of counterexamples;Then carrying on informal analysis to the algorithm combined with famous Needham Schroeder public key identity attestation protocol, and giving the analytical conclusion;Finally, putting forward to a new algorithm frame combined with the strategy of reset syntax to solve the weakness that the algorithm needs to carry on the iterated through state again to find out the minimization of counterexamples.

Gastin.P algorithm idea of minimization of counterexamples

According to the second definition of counterexamples, its form is path $\rho = \rho = \rho 1 \rho 2 \rho 3$.Where, $\rho 1 \rho 2$ is a path which initialization state can reach accepting status, $\rho 3 \rho 2$ is a simple loop which can reach itself from accepting status, showing as figure 1.Therefore, the minimization of counterexamples is defined to this form which can make the length of ρ shortest.

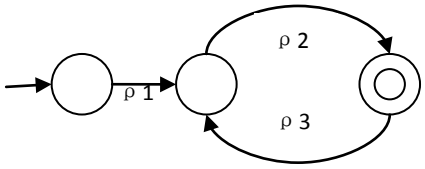

Fig. 1 the second definition of counterexamples

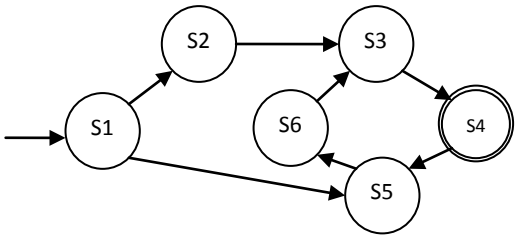

Fig. 2 blunder away the minimization of counterexamples（one）

The SPN existing algorithm of minimization of counterexamples is an improved depth nested preferential searching algorithm.To the iterated through status, The status is a new status, or its depth is smaller in the new path.But the algorithm can not promise to find out a minimization of counterexamples, because of finding out the first counterexamples, when iterating through a status, if its depth is bigger than the depth in the counterexamples, then SPN will remount and can not find out its minimum anti- example thus.Exist two kinds of instances, will make the algorithm blunder away its minimization of counterexamples.There are two instances which will cause the algorithm to blunder away its minimization of counterexamples. Two examples below will explain those two kinds of instances respectively, the moving label among them means the iterated through order.

automatic machines of figure 2, the first counterexamples that is found out is S1S2S3S4S5S6S3.After iterated through, the depth of status is set as follows:(S1,1), (S2,2) , (S3,3) , (S4,4) , (S5,5) , (S6, 6).The SPN algorithm starts to remount, reaching the status S5 from the status S1, its depth is 2.Due to the depth is smaller than its originally, then it can reach the status S6 from the status S5, its depth is 3.also it can reach the status S3 from the status S6, its depth is 4. Due to the depth is bigger than its originally, the SPN algorithm starts to remount,thus blundered away the minimization of counterexamples S1S5S6S3S4S5.

The second circumstance is aiming at accepted status, show as figure 3.After finding out the first counterexamples, though the depth of status no longer minish,we should also reach the status that has been already reached.The first counterexamples that is found out is S1S2S3S4S1, status depth is(S1,1),(S2,2), (S3,3), (S4, 2) . When reach the status S4 from the status S2 of the path S1S2S4, duo to any depth of status in the path no longer minish, then SPN algorithm starts to remount and blundered away the minimization of counterexamples S1S2S4S1.In this case, the existed related length minish, such as the length from accept that the status S2 to the status S4 minished.(from 2 to 1)

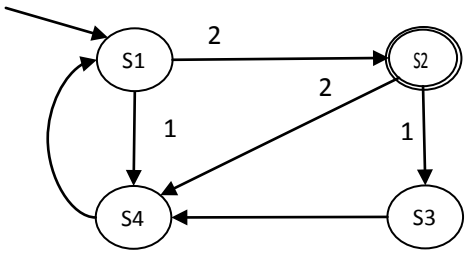

Fig. 3 blunder away the minimization of counterexamples（two）

To solve these two kinds of instances above, Gastin. P putted forward to a new algorithm of minimization of counterexamples. Inducting two operating models in the algorithm, one was a normal mode(a normal mode), several standards of the model can make algorithm remount;The other is a more safe mode(a more safe model), in the model, as long as satisfying one of the two conditions below , then will stop iterateing through.One was a current path which produce

circulation itself, the other was that the length of current path is longer than the length of minimization of counterexamples which have been already found out.If the algorithm got into safe mode and a status S will be pushed into the stack, then the algorithm will be in safe mode until the status S was pushed off. Examples of figure 2, when overreach the status S5 the second-time, because of S 5 → depths minishing, then the algorithm goes into the 11-12th row safe mode. Examples of figure 3, when overreach the status S2, the algorithm goes into the 7-8th row safe mode.

To carry on informal analysis to the algorithm combined with NS protocol

In the article announced in 2002, the PaoloMaggi's used the model detection tool SPN[8] to verify the famous NS public key identity attestation protocol at first time,he found out an counterexamples, and give the process of counterexamples creation through MSC(Message Sequence Circuit).The first edition 1.0 of the rapid conversion system from LTL formula to Büchi automaton is developed by Denis Oddoux, currently the latest edition 1.1 is the edition improved by Paul Gastin on this foundation.This text carries on informal analysis to Gastin.P algorithm based on the analysis of Büchi automaton from edition 1.1 combined with NS public key identity attestation protocol is 1.1.The analytical process is as follows:

The 1st step:Starting from the initialization status of Büchi automation(brief as BA), there are 8 migrations side, migrations thst satisfy condition are only to be migration 3 and 6, if we choose migration 6, it can not get the counterexamples with searching hereafter.So we can only choose migration 3.

The 2nd step:Starting From migration 3, we get into the init progress of BA, the migration that can be choosed are only two, if we choose migration 2, truth is to be the same as the analysis above, it can not get the counterexamples with searching hereafter.So we also can only choose to migration 1.

The 3rd step and the 4th step:There is only one migration at these two steps, so putting them together to analyse.

The 5th step:The status has 4 migrations, because of 3 among of them all dissatisfied, so it can choose the migration that it can reach oneself.

The 6th step and the 7th step:Getting into Pini progress from this step, carried out the first sentence of the atomic operation, the s value didn't change at this time, still is 0.

The 8th step:Carrying out the next migration, then the sponsor A sends out news 1 to the invader I:ca!A, Na, A, I.

The 9th step:The invader receives news 1.There are two migrations that can be provided to choose at this time.According to the parameter of news, it can but choose one migration among of them.The invader decodes the news at this time, so kNa=1.

The 10th step: The status has 4 migrations, because of 3 among of them all dissatisfied, so it can choose the migration that it can reach oneself.

The 11th step:At this time the invader according to the knowledge for studying, sends out news 1 to responser.The migration that can be provided to choose has 18, 3 migrations among of them dissatisfied, so it will only choose from 15 other migrations.For finding out the minimization of counterexamples among them,then choose migration ca!B, Na, A, B.

The 12th step:The responser receives news 1.Carrying on the receive sentence of atomic operation of the first responser’s progress at this time.

The 13th step:Carrying out the next migration, namely the 2nd sentence of atomic operation, at this time q=1.

The 14th step:Continuing to carry out the next migration, namely the 3rd sentence of atomic operation. The responser sends out news 2 to the invader 2, namely ca!B, Na, Nb, A.

The 15th step:The invader receives news 2.At this time 2 migrations can be chosed.According to the parameter of news, it can but choose one migration among of them.At this time, the invader can not decrypt the news, only can save the news, then k_Na_Nb__A=1.

The 16th step:The status has 4 migrations, because of 3 migrations among of them all dissatisfied, so it can choose the migration that it can reach oneself.

The 17th step:At this time the invader according to the knowledge for studying, sends out news 2 to responser. The migration that can be provided to choose has 6, for finding out the minimization of counterexamples among them,then choose migration ca!A, Na, Nb, A.

The 18th step:The sponsor receives news 2. Carrying on the first receive sentence of the 2nd atomic operation of the sponsor’s progress at this time.

The 19th step and the 20th step:Carrying out the next migration, namely the 2nd sentence of the atomic operation.The p value didn't change at this time, still is 0.

The 21th step:Continuing to carry out the next migration, namely the 3rd sentence of the atomic operation.The sponsor sends out news 3 to the invader, namely cb!A, Nb, B.

The 22th step:The invader receives news 3.There are two migrations that can be provided to choose at this time.According to the parameter of news, it can but choose one migration among of them.At this time, the invader decodes the news, thus k_Nb=1.

The 23th step:The status has 4 migrations, because of 3 migrations among of them all dissatisfied, so it can choose the migration that it can reach oneself.

The 24th step:The invader according to the knowledge for studying, sends out news to responser.At this time, because of only one migration, so it must choose to carry out it, namely:cb!B, Nb, A.

The 25th step:The responser receives news 3. Carrying on the first receive sentence of the 2nd atomic operation at this time.

The 26th step:Carrying out the next migration, namely the 2nd sentence of the atomic operation, at this time r=1.

The 27th step:Because r=1, so the migration carries on the accessed status at this time.

The 28th step:Because s value is still 0, it can reach oneself from accessing status at this time.At this time, the minimization of counterexamples havs already been found out, the algorithm ends.

Carrying on informal analysis to Gastin.P algorithm combined with NS public key identity attestation protocol, we found out the minimization of counterexamples just through 28 migrations among of them, it si the same as and the result got from SPN4.2.9 t, it indicates validity that the algorithm seek the the minimization of counterexamples of protocol.

Optimization

Although the Gastin.P algorithm is used to analyze the usefulness of network safety protocol, the algorithm needs to carry on the iterated through state again to find out the minimization of counterexamples. To solve this problem, a new algorithm frame is put forward based on the algorithm and combined with the strategy of reset syntax, show as figure 4.

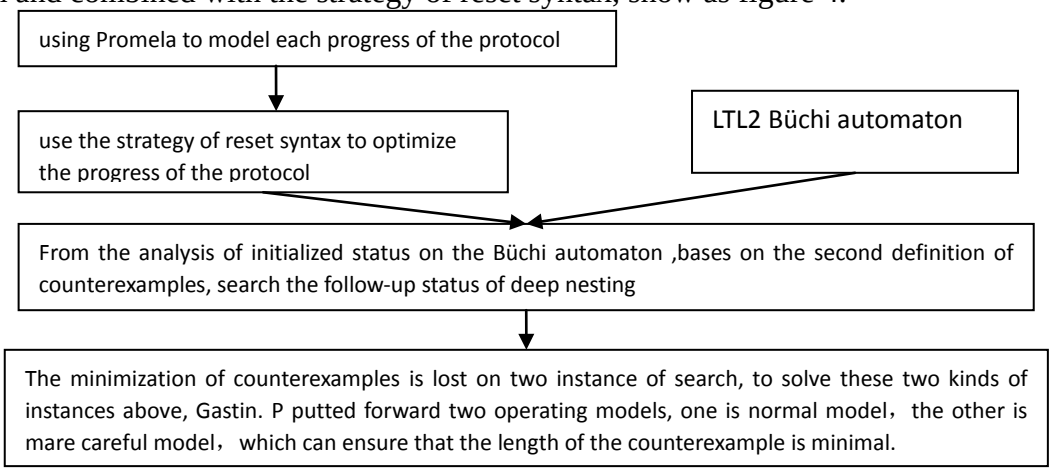

Fig. 4 the algorithm frame based on the strategy of reset syntax

That is, above as we analyzed the status migration between the progress of the protocol on the Büchi automation that created by the linearity tense logic formula LTL, we carry on the optimization with the strategy of reset syntax , the mainly work is optimizing and adjusting the promela codes of send sentence and receive sentence on the inbreak progress. Then we analyze the NS public key identity attestation protocol again on the new algorithm frame. To parallel the contrast of the front and back analysis result, under the same movement environment, that is SPN

4.2.9 and Cygwin 2.340.2.5, the hardware is Intel(R) Celeron(R), the 2.68 Ghzs CPU and the memory 512 MBs, we get table 1. We can obviously find that the strategy of reset syntax can effectively solve the problem of iterated through state on the search of the minimization of counterexamples.

Table 1 the contrast of the front and back analysis result

The number of status	The instance of parallel	
	Before optimization	After optimization
The number of memory	306	34
the number of iterated through	315	22
The number of migration	621	56
The number of migration= The number of memory + The number of iterated through		

Summary

The troops' information network carries out special tasks and has the highest request to the network safety. The safe protection system of troops' network based on minimization of counterexamples algorithm on model checking, which takes correspondence safety protocol as its foundation and premise and takes fire wall as its core, interacting with each other through various safe correspondence protocol, forming a dynamic, integrity safe system.This text puts forward a kind of new algorithm frame, based on carrying on informal analysis to the algorithm combined with famous NS public key identity attestation protocol and combined with the strategy of reset syntax, which can consumedly reduce the time that algorithm needs to carry on the iterated through state again to find out the minimization of counterexamples.Therefore, the new algorithm frame is of has high efficiency when used to analyse the network correspondence safety protocol, the safety of whole system gets a very great exaltation, then can satisfy the request of troops network safety.

Reference

[1] Wang Tao .The suggestion and thinking that keeps secret to the network information safety of our army [J]. communication engineering, 2003,(3) :9-12.

[2] Gao Jin Lian, Gao Hui Sheng. Preliminary study on Invade and protection system IPS [J].Network safe technique and application, 2005,(8) :35-37.

[3] Li Zeng Jun, Wang Xue Qin. Network safe primary analysis [J].Cabled T.V. technique, 2005, 12(10):67-69.

[4] Chen Yun Ming. The systemic studies on dynamic network safe model [J].Network safe technique and application, 2005,(5) :47-49.

[5] Lan Shi Long, Luo Ting. The overview of invades detection system [J]. Transaction of Logistic engineering college, 2003, 19(2):68-71

[6] Gastin P,Moro P, Zeitoun M. Minimization of Counter- examples in SPN[C]//ETAPS 2004 and ACM SIGSOFT Proceedings of the 11th Internation SPN Workshop on Model Checking Software, Ap ril 1 - 3, Barcelona, Spain Lecture Notes in Computer Science,Volume 2989, Springer Verlag, 2004: 92 – 108

[7] Lin Hui Ming, Zhang Wen Hui. the theory, method and application of model detection [J].Electronics transaction, 2002, 12(A):1 907 - 1 912

[8] Holzmann G J. The SPN Model Checker, Primer and Reference Manual [M]. Boston, USA: Addison – Wesley 2003.