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 (3): 470-473, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.470.473

Modeling and Formal Analysis of Communication Protocols Based on Game

Yun Jiang and Huaping Gong
Information Engineering Institute of Nanchang University,
Nanchang, Jiangxi, 330031, China

Abstract: A new Alternating-time Temporal Logic (ATL) analysis method based on game logic can model and analysis communication protocol, the paper use to analysis TMN protocol and the result indicates that this protocol can not satisfy fairness, finally the improved method was put forward.

Key words: Alternating-time temporal logic, formal analysis, TMN protocol, fairness

INTRODUCTION

With the extensive application of information transfer and data sharing in Internet, information security has become an important issue. Secure communication protocol is the basis to ensure the normal development of Internet activities. The basic properties of such protocol, including confidentiality, integrity, authentication, non-repudiation and fairness. Therefore, the communication protocol modeling and formal analysis is very important, we can use the formal results of the communication protocol to guide the design of the protocol or make up potential problems in the original protocol. Therefore, the formal analysis and verification study of communication protocol has great theoretical significance and practical value of applications, this is the technical support for the smooth development of the Internet.

Linear Temporal Logic (LTL) (Emerson, 1999) method and protocol analysis based on the Computation Tree Logic (CTL) (Clarke and Emerson, 1981) verification method has a strong description and it develops the automatic model checking tool SPIN (Holzmann, 2003) and SMV and NuSMV (Paolo and Riccardo, 2002), for automatic verification, it has been widely applied. These defects of the traditional temporal logic is to regard the protocol as a closed concurrent systems to research, it can not be described in protocol with the external environment (intrusion, network failure, etc.) contact and it also requires a protocol subject to strictly follow the established procedure, it not suitable for the description and analysis of the increasingly complexe-commerce protocols and large game protocol. A new logic analysis method proposed which is based on the Game ATL (Alur *et al*., 1997) (alternating-time temporal logic) to analysis transaction protocol, it can effectively solve the above problem. This method can descibe the main appropriate strategic behavior.

This article uses the ATL logic method and its application in the formal analysis of communication protocols to do the research and build the complex e-commerce protocol security, non-repudiation and fairness of the formal analysis of systematic approach, finally we use this method to formal analysis the TMN protocol (Young, 1989) strictly, the results demonstrate the effectiveness and convenient of the method.

ATS MODEL BASED ON GAME

Alternating Transition Systems (ATS) is formal tools for exchange agreement modeling. ATS is variables expansion of game in ordinary Kripke structure. Its corresponding model checking tools is MOCHA (Alur *et al*., 1985).

Definition 1: A exchange system is six group $S = \langle \Pi, \Sigma, Q, Q_0, \pi, \delta \rangle$. Among them, Π is proposition set, Σ is participants set, Q is state set, Q_0 is orinigal state set, π: $Q_0 \rightarrow 2^{\pi}$ is mapping from the state to proposition sets, δ: $Q_0 \times \Sigma \rightarrow 2^{2Q} \backslash \{\theta\}$ is a conversion function from {state×participants} to not empty choice set. Each choose is possible next state set. When the system is is stsat q, each participant choose a set $Q_a \epsilon \delta(q, a)$. So A participant insure next state of the system contained in its choice of Qa, Specific choice which one is to see the state in the system the choice of other participant. ATL (alternating-time tem-poral logic) is corresponding ATS system. The following are ATL formula definition.

Definition 2: A ATL formula in this form:

- p, among them, proposition $p \epsilon \Pi$
- $\neg\varphi$ or $\varphi_1 \vee \varphi_2$, among them φ_1 and φ_2 is ATL formula
- $\langle\langle A \rangle\rangle o\varphi$, $\langle\langle A \rangle\rangle o\varphi$, $\langle\langle A \rangle\rangle \varphi_1 \cup \varphi_2$ among them, $A \epsilon \Sigma$ is participants set, φ, φ_1 and φ_2 is ATL formula

Corresponding Author: Yun Jiang, Information Engineering Institute Nanchang University, Nanchang, Jiangxi, 330031, China

Definition 3 (strategy): One of the participants in the strategy is a mapping: f_a: $Q^+ \rightarrow 2^Q$, make all $q \in Q$ and $f_a(\lambda, q) \in \delta(q, a)$ are found.

If we want to use ATL logic fair communication protocol analysis, the first we must set a model for protocol system. The paper use Dijkstra (Kailar, 1996) guarded command language to set model. Each participant a corresponding to a form is guard-update command set. A calculation steps for definition: Each participant select a command of its own command set and Guard connects of the command is ture. All the choices of the participants in the command of the results obtained by the intersection of the update is system of the next state. Add a invaders I.

Definition 4: A system scenario is a multiset of instantiated protocol roles. Typically, a system scenario determines how many sessions are presented and which agents play which roles. For instance, the system scenario {responder (A, b, Na), responder (C, d, Nc)} (where responder is the role defined above) defines a system scenario with two responders (notice that there are no corresponding initiators), one played by b and the other by d. Uninstantiated variables represent unknown values:for example, variable A in the first responder role represents the (unknown) communicating party of b.

AGREEMENT MODELING

Basic assumptions: Considering the communication protocol of the general conditions, some of the more common to have the content of a basic assumptions. Communication protocol used general mark as follows:

A, B	:	The generation of information and the agreement receiver
TTP	:	Trusted third party
M, item	:	All kinds of news of in the agreement
K	:	Session key of between A and B
C	:	eK(M): Use K for M Encryption later got cipher text
Com	:	Communication channel
Channel	:	Assume that agreement between the parties involved in the channel is not reliable. The information transmitted could delay or lost and to the agreement with the passage between the trusted third party is the recovery, in other words the information transmitted could delay. But eventually it will in the limited time to reach its destination
Agreement subject	:	Participants of agreement may is not honest but Trusted third party is honest
Invaders	:	Assume invaders I can control channel, invaders can eavesdrop on, intercept, store, insert, delete, create, transmit and replay the messages

Privacy and security: Privacy of communications protocol: An attacker can't through the various attacks illegal ways to get the exchange information of agreement the participants, Use ATL formula can be described as follows:

$$\neg\langle\langle i\rangle\rangle\Diamond(m \vee item_A \vee item_B)$$

M is exchange message of agreement the participants $item_A$, $item_B$ are evidence of participation agreement, privacy and security of communications protocol is similar.

Nonrepudiation

Definition 5 (nonrepudiation): Agreement participate in both sides in the agreement can not deny that participate in the behavior of the agreement after the operation. This is mainly through the exchange of hair party the evidence and the NRO denied impersonation deny evidence to realize NRR_O.

If both of agreement are honest and channel agreement with normal operation, B have a strategy can get an itemA evidence of A in the agreement. As the same time A also have a strategy can get an item. Bevidence of Bin the agreement.

Use ATL formula can be described as follows:

$$\langle\langle A_h, B_h, Com\rangle\rangle\Diamond(\langle\langle B\rangle\rangle item_A \wedge item_B)$$

Fairness

Definition 6 (fairness): Communication protocol require fairness for agreement participate. If meet the following two conditions:

- At the end of the agreement, can provide effective NRR and NRO evidence for the sender and the receiver
- When agreement to suspend at any stage, Won't cause any party more advantage position than the other party. In other words, Both sides had either their expectations of things or both sides are not any positive information

A has not a strategy can control channel to make the system to such a state: A get item B evidence of B involved in agreement but has not strategy can get item A evidence of A involved in agreement. That agreement should be fair to B. Use ATL formula can be described as follows:

$$\neg\langle\langle A, Com\rangle\rangle\Diamond(item_B \wedge \neg\langle\langle B_h\rangle\rangle\Diamond item_A)$$

For A is fair agreement can be described as follows:

$$\neg\langle\langle B, Com\rangle\rangle\Diamond(item_A \wedge \neg\langle\langle A_h\rangle\rangle\Diamond item_B)$$

ANALYSIS OF TMN PROTOCOL

TMN analysis: TMN protocol contains three participants: initiator A, responder B and server S.

S distributes the key of conversation for the initiator A and responder B, Two different ways will be adopted to pose cipher codes:

- **Encryption standard:** For a given message M, intiator A and responder B, both can use encryption function E to generate encryption E (m), However, only third-party servers, only know how to decipher. RSA encryption is a typical example
- **Vernam encryption:** This encryption will be XOR operator with a pair of keys. That is V(k1, V(k1, k2)) = k2 and V(k2, V(k1, k2)) = k1. in other words, if an entity knows key k1, then it can get k2 through deciphering V (k1, k2). Here we suppose there is enough redundancy to guarantee the accurate deciphering units

TMN protocol want to establish a session key, need to exchange four informations:

- Message 1: A→S: A, S, B, {R1}pk(S)
- Message 2: S→B: S, B ,A
- Message 3: B→S: B, S, A, {R2}pk(S)
- Message 4: S→A: S, A, B, v(R1, R2)

When sender A wants to establish conversation with responder B, It will chose R1 key to encrypt and send it to third-party service provider S (message 1). S then sends message to B, A wish to launch a conversation (message 2). B confirmed the conversation and chooses encryption key R2 to encrypt and sends to server S (messages 3). S use the two encryption keys for Vernam encryption and returns to the A (message 4). When receiving the text of this Vernam encryption, A can use R1 to decipher, then it can get R2.

We use Promela to construct the model and testify the security of the cipher code protocol. The construction of this model includes two parts:

- Description of the protocol rules
- Description of the operation example

According to the above-mentioned trace semantics, we have successfully discovered two attack sequence which violates the security properties of TMN protocol by SPIN model:

Attack 1:

- Message m.1. a→μ(s): a, s, b{ta, r1}pk(s)
- Message m.1'. μ(a)→s: a, s, b, {te1, re}pk(s)
- Message m.2. s→b: s, b, a
- Message m.3. b→μ(s): b, s, a, {tb, r2}pk(s)
- Message m.3'. μ(b)→s: b, s, a, {ta, r1}pk(s)
- Message m.4. s→μ(a): s, a, b, v(r_e, r1)
- Message M.1. μ(a)→s: a, s, b, {te2, r1}pk(s)

Attack 2:

- m.1. a→μ(s) : a, s, b, {ta, sa, r1}pk(s)
- m.2. μ(s)→b: s, b, μ
- m.3. b→μ(s): b, s, μ, {tb, sb, r2}pk(s)
- M.1. μ(a)→s: a, s, b, {ta, sa, r1}pk(s)
- M.2. s→μ(b): s, b, a
- M.3. μ(b)→s: b, s, a, {tb, sb, r2}pk(s)
- M.4. s→μ(a): s, a, b, v(r1, r2)
- m.4. μ(s)→a: s, a, b, v(r1, r2)
- m.1. a μ(s): a, s, b, {ta, sa, r1}pk(s)
- M.1. μ→s: μ, s, a, {te, se, re1}pk(s)
- M.2. s→μ(a): s, a, μ
- M.3. μ(a)→s: a, s, μ, {ta, sa, r1}pk(s)
- M.4. s→μ: s, μ, a, v(re1, r1)
- m.4. μ(s)→a: s, a, b, v(r1, re1)

Agreement improvement: The improvement of the agreement in order to guarantee the fairness of the MK, sender A and TTP don't need Clock synchronization. This is different with the original agreement. It bring in two concepts: period of time and time point can describe the improved protocol The period of time only mean the length of the time, no matter what happens in this period of time. It can use integer.

When agreement is running, if SUB and NRR1 kept in the TTP's private directory at the same time, TTP would distinguish NRO of SUB and NRO of NRR1. If two NRO are inconformity, in other words one is false. TTP will not produce proof, otherwise TTP come into being

proof-Conk and Set and publish to their own public directory access for A and B. To avoid TTP indefinitely save evidence, TTP can define a time period in advance t0, it is said the evidence released the TTP t0 time after a unit will delete them. So we can assume that the maximum time for interference t a unit of time, so define t0 = td+x (x>0), A and B1 can always access to the evidence from the public directory of TTP in his own convenience.

For other participants B2 of undeniable evidence receive and management, we Can take the above a similar deal with. So, by increasing the time limit, can make the agreement is also denied that many MK has time limit and fairness.

CONCLUSIONS

Our technique supports a protocol designer to provide formal analysis of the security properties through specifying the security prosperities. We illustrate the utility and effectiveness of our technique by exposing two attacks on the well studied protocol TMN.

REFERENCES

Alur, R., T.A. Henzinger and O. Kupferman, 1997. Alternating-Time Temporal Logic. Proceeding of the 38th Annual Symposium on Foundations of Computer Science, October 19-22, 1997, Miami Beach, USA, pp: 194-203.

Alur, R., T.A. Henzinger, F.Y. C. Mang, S. Qadeer, S.K. Rajamani and S. Tasiran, 1985. MOCHA: Modularity inmodel checking. Proceedings of the 10th International Conference on Computer Aided Verification, (CAV'98), Springer-Verlag, pp: 521-525.

Clarke, E.M. and E.A. Emerson, 1981. Design and synthesis of synchronization skeletons using branching time temporal logic. Logics Programs, 131: 52-71.

Emerson, E.A., 1999. Handbook of Theoretical Computer Science. Vol. 2, The MIT Press, Cambridge, ISBN-13: 9780262720205, Pages: 2293.

Holzmann, G.J., 2003. The SPIN Model Checker: Primer and Reference Manual. 1st Edn., Addison Wesley, Boston, USA, ISBN-13: 9780321228628, Pages: 608.

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

Paolo, M. and S. Riccardo, 2002. Using SPIN to Verify Security Propertiesof Cryptographic Protocols. Proceedings of the 9th International SPIN Workshop on Model Checking of Software, April 11-13, 2002, Grenoble, France, pp: 187-204.

Young, M., 1989. Technical Writer's Handbook: Writing with Style and Clarity. University Science Books, Mill Valley, CA, ISBN: 0935702601, pp: 56-62.