Application and Research of Problem-driven Approach in Identifying Protocol Teaching

Zhengqin Xu[1],* Wendong Zhao[2], Laixian Peng[3], Hai Wang[4]
[1234]College of Communication Engineering, Army Engineering University, Nanjing, China
155267201@qq.com
*Wendong Zhao

Key word: Problem Driven, Problem Chain, Identification

Abstract: Problem-driven teaching method is a kind of teaching method, which takes the problem as the traction, combs the knowledge points in the course and establishes the problem chain by the teachers, so that the students always focus on the problems in the learning process and constantly seek solutions. In this paper, the problem-driven teaching method is applied to the computer network course, and the classroom organization process of the problem-driven teaching is explained in detail with the example of the course of "Identification Protocol". Practice has proved that problem-driven teaching method can stimulate students & apos; interest in learning, and cultivate students & apos; ability of independent learning and innovation.

1. Introduction

Voltaire, a French scholar, said well that "the obnoxious art is to say everything". Problem-driven teaching method is to guide students to study and cooperate with each other by designing a series of "question chains" in classroom teaching. In the process of solving problems, students can make progress, thus improving their comprehensive quality[1].

The origin of problem-driven teaching method can be traced back to the teaching mode of "situation, problem, hypothesis, reasoning and verification" put forward by Dewey, an American pragmatist educator in the late 19th century. His emphasis on "learning by doing" has a great impact on the whole educational circle. In 1960, Barrows and Tamblyn put forward the Problem-Based Learning (PBL) teaching method in the field of medical education to overcome the shortcomings of the newly graduated medical doctors who have a lot of professional knowledge but lack the ability of clinical application. In 1969, McMaster University of Canada first established PBL-based education strategy in the medical field, and then gradually extended to teaching activities in business, pedagogy, architecture, law, engineering and other disciplines. It has obvious effects on training students & apos; ability to innovate independently and solve problems. Harneyman University in the United States has implemented this teaching method in dental hygiene disciplines in the School of Public Health and Purdue University. At the present stage, problem-driven teaching method has developed more deeply in various fields of education in Western countries. Their classroom teaching pays more attention to inspiration and induction, independent inquiry, and the cultivation of students & apos; innovative thinking. Under this kind of education, the trainees also showed a strong sense of innovation and research and development ability [2][3][4].

Tao Xingzhi, a famous educator in China, said, "Creation begins with problems. Only when there are problems, can we think. Only when there are problems, can we find ways to solve problems and find independent ideas. "Problem-driven teaching is to guide and maintain students & apos; learning interest and motivation by exploring problems, so that students & apos; learning is not only the transfer and transmission of knowledge from outside to inside, but also the process of students & apos; initiative to construct their own knowledge and experience. Through the interaction of new experience and original knowledge and experience, students can enrich and enrich their knowledge and ability [5] [6-8].

2. Design Principles of Problems

Question-driven teaching should follow the following two principles in the design of problems in the teaching process [9]:

(1) Problem design should be based on students & apos; experience and knowledge. The difficulty of the problem should be appropriate. Under the guidance of teachers, students can think and solve problems independently and independently.

The design of classroom problems is based on the principle of stimulating students & apos; interest in inquiry, which can stimulate students & apos; interest in learning and make them have strong desire for exploration and knowledge. Taking the computer network course I teach as an example, in the process of teaching, I often contact the knowledge of network application in life, put forward the problems related to knowledge points at the appropriate time, and guide them according to the students & apos; existing knowledge, which can stimulate students & apos; interest, study and solve problems, and then produce a strong sense of achievement and pride. This kind of feeling will further stimulate students to rediscover, explore and create.

(2) The design and solution of classroom problems should be gradual. As far as possible, the questions raised in class should not be in place at one step. They should be progressive and hierarchical. Teachers should conform to students & apos; thinking habits when designing problems, design a series of logical problems from shallow to deep according to students & apos; specific conditions, and pay attention to the rational arrangement of the order of the problems, especially the key and difficult points of the content. Through careful design, they should lay down the problems in turn, lead the students to "pick up the steps" and actively acquire knowledge. For example, in the section "Reliable Transport Protocol", the instructor can ask, "How can data be transmitted over a completely reliable channel?" Then, it puts forward "If there is a bit error channel, how should the data be transmitted reliably?" Finally, the paper proposes "how can data be transmitted reliably in a packet loss channel with bit errors?" As the problem progresses from layer to layer, a reliable and error-free data transmission protocol is finally obtained.

3. Implementation steps of problem-driven Teaching

In the process of implementing the problem-driven teaching method, it can be divided into the following steps: creating situations and putting forward problems; analyzing, exploring and solving problems; and summing up results, summarizing and reflecting.

In practical teaching, we can organize problem-driven teaching according to the above steps. The first step is to create a situation, to create a real application environment for specific teaching content, and to stimulate students & apos; interest. The second link is to guide the students to solve problems. This link can adopt the way of students & apos; independent thinking or discussion with each other. In this link, we should highlight the main position of the students, help them realize self-motivation and self-monitoring, make the classroom teaching process based on multilateral interaction, and then make the classroom teaching form a climax, but also help teachers understand the students & apos; learning situation and personal characteristics. The third step is to sum up the problems that have been solved by teachers or trainees and put forward new problems.

4. Examples of problem-driven teaching method

"Computer network" is a computer course with strong theoretical and practical nature. The object of study is the basic principle and technology of computer network, which has many knowledge points, wide range of knowledge, very abstract network protocol, and no necessary connection between knowledge points. Therefore, it is difficult for students to master network knowledge. For example, there is a parallel relationship among the protocols in the network course. Before beginners establish the concept of network system, the network protocols are like a mess and disorder. One protocol has not yet been understood thoroughly, and they have to start learning the new protocol in the next chapter. Students often feel that the chapters have nothing to do with each other and are confused

naturally. The implementation of traditional curriculum is based on the teachers & apos; pre-designed teaching plan, which mainly adopts the traditional teaching mode of passive and mechanical acceptance of knowledge. If there are few opportunities for communication between teachers and students according to this model, students will feel that the course is dull, naturally their interest in learning will be low, and the learning effect is not ideal. If we can use appropriate questions to guide the content of each course, through careful design of questions and problem-oriented, so that students can be placed in the dynamic learning process of thinking and solving problems, students will have strong interest and strong desire to answer, firmly attract their attention, give full play to their subjective initiative in learning, and thus optimize. Classroom teaching can improve teaching quality and achieve teaching effect.

We have successfully applied problem-driven teaching in the section of "authentication protocol" in the course of "Computer Network". The following elaborates the specific implementation ideas and process.

The first step: setting up the situation

This lesson is based on an exercise called "Joint Warrior" of the US Army. The Navy Command System was successfully invaded by an Air Force Captain and gained control of the fleet. The topic is that the identification of the Air Force Captain by the system server has some problems: how to design the authentication protocol?

Context Design: "In today & apos; s ubiquitous computer network, QQ, Wechat system, campus network will be logged in every day. How can the server identify the client & apos; s login? Please design a one-way authentication protocol for campus network login. Design three roles: client Alice confirms his identity to server Bob through the network. Sam is an intruder.

This situation is introduced by the familiar military cases and the situations encountered in real life. Setting up problems can effectively arouse the students & apos; inquiry psychology and ignite the spark of their thinking, thus forming the problem consciousness and stimulating the students & apos; potential and interest in solving problems.

The second step is to solve the problem.

In the process of protocol design, a series of "problem chains" are used as the links of the whole course. The design of the problem is progressive and gradual, until the final solution is reached.

Question 1:

Ask students to design an identity authentication protocol 1.0 based on their usual experience.

Protocol 1.0 Alice explicitly sends "I am Alice" and password to Bob.

Teacher & apos;s question: Can 1.0 protocol be eavesdropped by Sam? If it can be eavesdropped, how should it be improved?

After discussion, it is concluded that because there is no authentication mechanism and security measures, it is easy to be eavesdropped by Sam, thus posing as Alice.

Question 2:

Teachers asked: Solve the loophole in Protocol 1 - > How not to be eavesdropped?

After discussion, the trainees proposed that the protocol 2.0 could be designed by using the encrypted password.

Protocol 2.0 Alice sends me "I am Alice" and encrypted password to Bob.

Teacher & apos; s question: How to encrypt?

Participants concluded: (after discussion) Encrypt passwords using symmetric keys learned in the last lesson.

Teacher & apos; s question: Sam can & apos; t know the exact content of the password, can' t he pretend to be Alice?

Use questions to stimulate students & apos; interest and desire to explore, and then draw out that even if you don & apos; t know the exact content of the password, you just need to record the encrypted version of the password and play it back to Bob, then you can impersonate Alice.

Question 3:

Teacher & apos; s Question: Enlighten the students, what is the reason why Sam can impersonate Alice in Protocol 2.0?

It & apos;s because Bob doesn & apos ;t know if Alice is still on the other end of the connection or "alive".

Teachers ask questions: Has this problem ever been encountered in computer networks?

After discussing with the trainees, it is concluded that this problem has similarities and differences with TCP three-handshake protocol and can be solved by the same strategy.

Finally, we conclude that this protocol can be successfully designed by using shared symmetric key Ka-b and non-multiplicity R.

Protocol 3.0, as shown in Figure 1:

1) Alice sends a message to bob, "I & apos; m Alice."

2) Bob chooses a non-multiplicity R and sends it to Alice

3) Alice uses the symmetric key Ka-b she shares with Bob to encrypt the non-multiplicity and sends the encrypted non-multiplicity Ka-b (R) to Bob.

4) Bob decrypts the received message, and if R & apos; = R is decrypted, the identity of Alice can be determined.

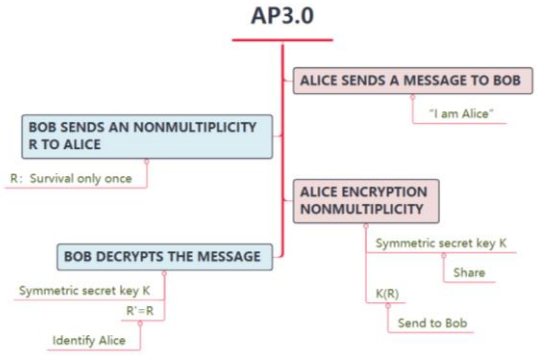

Fig.1. Agreement 3

How to design an authentication protocol for campus network login?

Teacher asked: What is the key to designing this agreement?

Discussions and Answers: Choose the appropriate symmetric key and use protocol 3.0

Tip: After the client registers, the server will save the username and password in the database.

After discussion, the participants came to the conclusion that the password could be chosen as the shared symmetric key. The protocol design is shown in Figure 2.

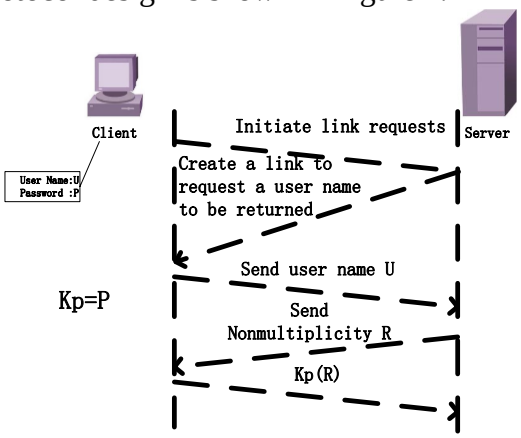

Fig. 2. Campus Network Logon Authentication Protocol

In this link, the problem set up is like a ladder from low to high, from easy to difficult, progressively, guiding the students to deepen their thinking step by step, gradually designing protocol 1.0 to protocol 3.0, guiding the students to find problems, explore problems and solve problems in the design process, so as to build a knowledge framework independently, and finally solve the problems raised at the beginning of the classroom.

The third part: summarizing and evaluating, and putting forward new problems

Summary and evaluation: Lead students to think about "Why can one-way authentication protocols be designed with shared symmetric keys and multiplicities?" "One-way authentication protocol can make use of the shared symmetric key only if the client proves its identity to the server side, while the server side does not need to prove its identity to the client side, that is, based on the absolute trust of the client to the server side, so the client can send its shared key to the server side."

Question asked: "For two-way authentication protocols, such as two military radio communications, can the design of authentication protocols continue to use shared symmetric keys and multiplicities? What problems would it bring? If you can & apos; t share a symmetric key, which way can you use it?

Through the guidance of a series of problems of teachers and the discussion and exploration of the trainees, we can finally master the design method of the protocol and how to find and deal with the loopholes in the protocol design. Finally, we can design a reliable authentication protocol by ourselves.

5. Concluding remarks

Problem-driven teaching method, through the rational setting of heuristic, exploratory and warm-up questions, stimulates students & apos; enthusiasm for learning, and strengthens teacher-student interaction through classroom discussion, questioning, group building and other forms. Before using the problem-driven teaching method, students often feel abstract and difficult to understand the content of complex network protocols when learning computer network knowledge, which leads to students & apos; unwillingness to do in-depth study and thinking. After using the problem-driven teaching method in the teaching problems of various protocols and services in the network, the learners can quickly grasp the contents of learning, and can integrate them, so that they can really know what they are and why they are. And the students unconsciously develop the habit of thinking, and cultivate innovative thinking.

Reference

[1] Mohammad Imran, Problem-based learning versus lecture-based learning in pharmacology in a junior doctor teaching program: a cross over study from northern India [J], International Journal of Research in Medical Sciences, 2015, Nov; 3 (11): 3296-3299.

[2] Agus Salim, The Problem Based Learning Model To Improve The Students & apos; Critical Thinking Ability [3], Journal of Research and Method in Education, 2018, Mar (2): 36-40

[3] Ilhan KARATAS, The Effect of Learning Environments Based on Problem Solving on Students & apos; Achievements of Problem Solving [J], International Electronic Journal of Elementary Education, 2013, 5 (3): 249-268.

[4] Melanie LaForce, Problem-Based Learning (PBL) and Student Interest in STEM Careers: The Roles of Motivation and Ability Beliefs, Education Science, 2017, 7:4-6.

[5] Fan Fusheng, Application of Problem-driven Teaching Method in Physics Teaching [J]. Teaching and Management, 2012, 6(18): 141-143.

[6] Feng Di, Yang Mingwei, Zhou Zhen. Problem-driven Teaching Approach for Information Optics and Optical Information Processing [J]. Education and Teaching Forum, 2012, 10(30):40-14.

[7] Zhang Xia, An Empirical Study of Scaffolding Teaching under the Constructivist Teaching Concept [J]. Teaching Research, 2011, (11):150-153.

[8] Zhang Mingfang, on the application of constructivist Scaffolding Teaching Model in interpreting teaching [J]. Journal of Jiangxi Institute of Education, 2013, (6):121-124.

[9] Qutao. Application of Scaffolding Teaching in Kindergarten Collective Teaching [J]. School, 2013, (32): 162-164.