A Novel Identity Authentication Scheme of Wireless Mesh Network Based on Improved Kerberos Protocol

Min Li [1], *Xin Lv* [*1], *Wei Song* [2], *Wenhuan Zhou* [1]
[1] College of Computer and Information, Hohai University, HHU
[2] Office of Jiangsu Province Flood Control and Drought Relief Headquarters
Nanjing, China
[*] Corresponding Author: lvxin.gs@163.com

Rongzhi Qi [1], *Huaizhi Su* [3]
[1] College of Computer and Information, Hohai University, HHU
[3] College of Water Conservancy and Hydropower Engineering, HHU
Nanjing, China

Abstract—*The traditional Kerberos protocol exists some limitations in achieving clock synchronization and storing key, meanwhile, it is vulnerable from password guessing attack and attacks caused by malicious software. In this paper, a new authentication scheme is proposed for wireless mesh network. By utilizing public key encryption techniques, the security of the proposed scheme is enhanced. Besides, timestamp in the traditional protocol is replaced by random numbers to implementation cost. The analysis shows that the improved authentication protocol is fit for wireless Mesh network, which can make identity authentication more secure and efficient.*

Keywords-Kerberos protocol; public key encryption; Wireless Mesh network; identity Authentication

I. INTRODUCTION

A. Background

With the increasing social requirements of flexible mobile communications services, and traditional network technologies are based on infrastructures which is unable to provide flexible mobile communication services, wireless network technology is developing rapidly nowadays. Different from the traditional wireless network, Wireless Mesh network (WMN)[1] is a new kind of technology, which allows each node to receive and transmit signals in the network. Compared to traditional wireless network, Wireless Mesh network has many advantages:1) non line of sight transmission expands the application field of wireless broadband[2]; 2)high transmission rate makes transmission distance relatively short; 3)high reliability; 4)faster network configuration and maintenance; 5)low cost. These advantages indicate that, WMN is a leap of wireless network technology which has a very broad application prospect. In wireless Mesh networks (Wireless Mesh Networks), nodes can be divided into three types according to their functions[3]: ①MP (Mesh Point), MP only supports the Mesh interconnection; ② MAP (Mesh Access Point), MAP supports Mesh interconnection and access;③MPP (Mesh Point with a Portal), MPP supports Mesh interconnection and network communication[4]. The WMN architecture is shown as figure 1.

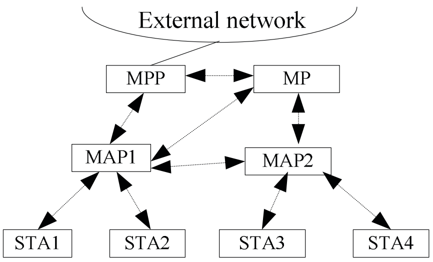

Figure 1. A Typical WMN Architecture

B. Kerberos Authentication Protocol

Kerberos is a key network authentication protocol developed by Massachusetts Institute of Technology (MIT). Based on KDC (key distribution center), a symmetric key encryption algorithm was utilized by this authentication protocol. Then, through the trusted third party KDC, both sides of network communication can be identified mutually. This authentication mechanism does not depend on the operating system and the address of the host. Kerberos identity authentication system includes a range of services, in addition to the user C, the following three parts are also included: ①Authentication server (AS)[5]. AS is used to verify the identity of the user C when login, and pass the identity authorization bill TGT to authenticated user, which is used to prove the identity to service authorization server TGS[6].②Service authorization server (TGS).Service authorization server (TGS) provides service access ticket to user C who has already been authenticated. With this service access ticket user C can apply for access to other services. ③Application Server. The application server is the final executor of service[7].The Kerberos authentication protocol process is shown as Fig. 2.

978-1-4799-4169-8/14 $31.00 © 2014 IEEE
DOI 10.1109/DCABES.2014.41

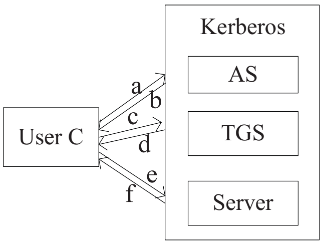

Figure 2. Flow Chart of Kerberos Authentication Protocol

The principle of Kerberos protocol is generally divided into three phases, and each phase has two steps. User C sends a message to the AS server to request an identity authorization bill TGT, which will be sent back to the user C after the secret key encryption by user. User asks the service authorization server for service access bills which will be used as proof to request permission to access specific server. The server can be accessed by the user if the identity of the user is secure[8].The specific process of Kerberos protocol is shown as follows:

(1) User C asks the authentication server AS for certification services; user C gets the identity authorization bill:

$$C \to AS : \mathrm{ID}_C \parallel Times \parallel Nonce_1 \parallel ID_{tgs}$$

$$AS \to C:$$

$$ID_C \parallel Ticket_{tgs} \parallel E_{Kc}\left[K_{C,tgs} \parallel Nonce_1 \parallel ID_{tgs} \parallel Times\right]$$

$$Ticket_{tgs} = E_{Ktgs}\left[K_{C,tgs} \parallel AD_C \parallel ID_C \parallel Times\right]$$

(2) User C apply for Service authorization from TGS; user C receive Service authorization paper:

$$C \to TGS :$$

$$ID_V \parallel Nonce_2 \parallel Times \parallel Authenticator_C \parallel Ticket_{tgs}$$

$$TGS \to C : \mathrm{Ticket}_V \parallel ID_C \parallel E_{Kc,tgs}\begin{bmatrix} K_{C,V} \parallel Nonce2 \parallel \\ Times \parallel ID_V \end{bmatrix}$$

$$Ticket_{tgs} = E_{Ktgs}\left[ID_C \parallel AD_C \parallel Times \parallel K_{C,tgs}\right]$$

$$Ticket_V = E_{Kv}\left[ID_C \parallel AD_C \parallel Times \parallel K_{C,V}\right]$$

$$Authenticator_C = E_{K\,\mathrm{c,tgs}}\left[TS_1 \parallel ID_C\right]$$

(3) User C asks the application server for access services; user C obtains access permissions:

$$C \to V : Authenticator_C \parallel Ticket_V$$

$$V \to C : E_{Kc,v}\left[Subkey \parallel Seq *\right]$$

$$Ticket_V = E_{Kv}\left[ID_C \parallel AD_C \parallel Times \parallel K_{C,V}\right]$$

$$Authenticator_C = E_{Kc,v}\left[TS_2 \parallel Subkey \parallel ID_C \parallel Seq *\right]$$

C. Kerberos-based WMN Identity Authentication Mechanism

In wireless Mesh network (WMN), firstly, the server will authenticate the identity of each new node MP. When the authentication is passed, the new node MP will be allowed to access the network. At the same time, MP will be authorized to access. A mutual trust relationship will be established between MP and KNAS, and the secret key will be shared. In the initial authentication phase, single sign-on (sso), unified authorization, centralized authentication methods are used to divide identity authentication and access authorization into two parts. The authentication and authorization entity complete the identity authentication and access authentication of MP. KNAS on the MPP Node is a network access server. KNAS, service authorization server and the authentication server make up the authenticator system together. AS is used to verify the identity of user C, and pass the identity authorization bill TGT to authenticated user, which is used to prove the identity to service authorization server TGS. As long as the new node MP does not leave the network, TGT will be used for a long time, thus greatly shorten the interactive authentication process in subsequent periodic access. After the authentication, TGS will inspect the authorization bill of MP. If MP passes the inspection, it will be allowed to access the network and receive an access service bill, including a key shared by each MPP node. Thus, the new node MP can also continue to interconnect with the neighbor nodes. Wireless Mesh network security mechanism structure is shown as figure 3.

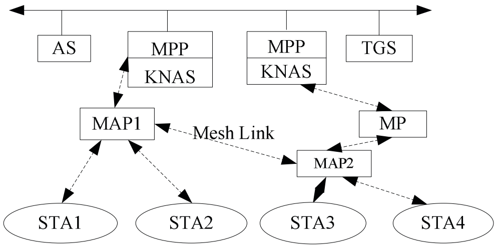

Figure 3. WMN Security Mechanism Architecture

D. The Limitations of Kerberos Protocol

Although Kerberos protocol is the major identity authentication protocol at present, and to a certain extent, Kerberos protocol can guarantee the security of the network. Though it has incomparable advantages and strong practicability, Kerberos protocol still has drawbacks and defects of its own.

- **Clock synchronization.** Timestamp was added to the bills and certifications in the Kerberos protocol, which is used to solve the problem of replay attack. Only when the timestamp differs little, data can be considered as valid. This requires the machine time of user C, authentication server (AS) and service authorization server be roughly the same. However, in the distributed network environment, such precise time requirement is difficult to achieve. At the same time, attackers could take advantage of this feature, too. Once the bill is got and then sent immediately, it will be difficult to be searched within prescribed period of time, thus increases the potential hazards of replay attack.
- **Password guessing attack.** In Kerberos protocol, the message authentication server (AS) sent to user C is encrypted by the secret key EKc of user C, while EKc derives from user's password which is encrypted by Hash function. So the attacker may collect a large number of TGS bills, calculate and analyze the user password to steal users' information.
- **Key storage.** Symmetric key algorithm is used in Kerberos, which requires establishing a high standard maintenance mechanism to share the secret key. With the expansion of Internet network and the growing number of the shared secret keys, the problems of

storage, management, maintenance of the secret key are difficult to solve[9].

- **Malicious software attacks.** The security requirements for Kerberos software are high in Kerberos authentication protocol, if security is not high enough, the attacker may execute Kerberos protocol and record the user's password to replace the Kerberos software that user uses, leading to attack.

II. WMN IDENTITY AUTHENTICATION MECHANISM BASED ON THE IMPROVED KERBEROS

A. The Improved Kerberos protocol

The Kerberos protocol model discussed in this paper is shown as Figure 4. It is similar to the traditional Kerberos protocol mode, specific process is shown as below:

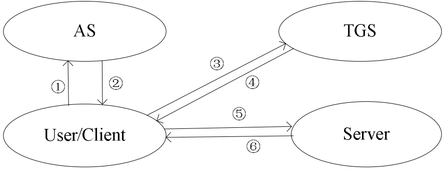

Figure 4. The Schematic Diagram of The Improved Kerberos Protocol

$\Pr vK_X$ denotes private key for X; $PubK_X$ denotes public key for X; $K_{X,Y}$ denotes shared key for X and Y; $\{m\}_k$ denotes encrypt q $\{m\}$ by k.

(1) $MP \rightarrow AS:\{\{MP, AS, TGS, K_{MP,AS}\}\mathrm{PrvK}_{MP}\}PubK_{AS}$

(2) $AS \rightarrow MP:\{\{MP, K_{MP,tgs}\}K_{MP,tgs}, \{T_{MP,tgs}\}PubK_{MP}\}$

$T_{MP,tgs}:\{AS, MP, TGS, Addr, Lifetime, K_{,\mathrm{MP,tgs}}\}\Pr vK_{AS}$

(3) $MP \rightarrow TGS:\{A_{MP,\,tgs}, \{T_{MP,tgs}\}PubK_{tgs}\}$

$A_{MP,tgs} = \{MP, MPP, Addr, Lifetime, N_{MP}\}K_{MP,tgs}$

(4) $TGS \rightarrow MP:\{\{T_{MP,\,MPP}, N_{MP}\}K_{MP,\,tgs}\}$

$T_{MP,MPP}:\{TGS, MP, MPP, K_{MP,MPP}, Lifetime\}\Pr vK_{tgs}$

(5) $MP \rightarrow MPP:\{\{MPP, MP, N_{MPP}\}K_{MP,MPP}, T_{MP,\,MPP}\}PubK_{MPP}$

(6) $MPP \rightarrow MP:\{MP, MPP, N_{MPP}\}K_{MP,MPP}$

In the improved Kerberos protocol, each new access node MP has a pair of asymmetric secret key. The open key of the new node MP can be open to all people, but the private key of the new node MP is kept by itself; A random number was introduced to replace the timestamp in the traditional Kerberos protocol in (3)(4)(5)(6) steps.

B. The Improved WMN Identity Authentication Mechanism Based on Kerberos

In order to solve the problems in the traditional Kerberos protocol, such as clock synchronization, password guessing, key storage, malicious software attacks, Smart Cards was introduced into Kerberos protocol, which can effectively solve the problem of password guessing. However, in order to support the technology of Smart Cards, new hardware device should be added to the system at the same time[10]. The problem of clock synchronization can be solved by serial number cycle mechanisms in Kerberos protocol, and the original timestamp will be replaced by the random number which is generated from user C. In a certain degree, it can solve the problem of replay attack, however, this may change the structure of the Kerberos protocol. In addition, Kerberos protocol also can be improved by public key cryptography, which is another research hotspot at present. This method can efficiently solve the problems of excessive consumption of key storage management. However, drawbacks are also obvious that it takes more encryption and decryption time of public key cryptosystem than symmetric key cryptosystem.

Based on the state of art above, a new solution based on traditional Kerberos protocol was proposed in this paper, the specific process is as below:

1. New node MP sends a message to the authentication server AS to request certification service and apply for certification authorization bill TGT, which is used to prove the identity of MP to TGS. The request message includes MP's name, AS's name, service authorization server's name, shared cryptographic key $K_{MP,AS}$ between AS and MP. The shared encryption key $K_{MP,AS}$ is generated from MP randomly, which replaces the function of timestamp in traditional Kerberos protocol.

After the certification of MP by AS, the response message will be sent back to MP. The response message will be encrypted by $K_{MP,AS}$ which ensures that the response message is generated from the AS. The message that MP sends to AS is digitally signed with the private key $\Pr vK_{MP}$ of MP, which can prove that the message is generated from MP. Then the message will be encrypted with the public key of AS, which guarantees that the message only can be decrypted by authentication server AS.

2. When authentication server AS receives the message that MP sent, the message will be decrypted by AS first, the decryption process will be accomplished by utilizing the encryption and decryption key of AS. After decryption, the authentication message will be inspected and signed by the public key in the certificate comes from MP by AS. If the signature and authentication passed, AS will response to the MP by sending a message. The response message contains the shared key $K_{MP,tgs}$ between MP and TGS. The shared key $K_{MP,tgs}$ is generated by the authentication server AS randomly, and is encrypted with the shared key $K_{MP,as}$ between MP and AS, which ensures the security of the shared key $K_{MP,tgs}$. At the same time, the message also contains an identity authorization bill $T_{MP,tgs}$, which will be sent to the service authorization server TGS to prove the access permissions. The identity authorization bill $T_{MP,tgs}$ contains the AS's name, the shared key $K_{MP,tgs}$ between MP and TGS, MP's name, TGS's name, MP's address Addr, and the effective time Lifetime of the identity authorization bill $T_{MP,tgs}$ of MP. The authorization bills $T_{MP,tgs}$ of MP is signed by the private key of AS, then the bill will be encrypted by the public

key $PubK_{MP}$ of MP, which ensures $T_{MP,tgs}$ be more secure.

When the new node MP receives messages from the authentication server AS, $\{MP, K_{MP,tgs}\}K_{MP,as}$ will be decrypted with the shared encryption key $K_{MP,as}$ between the MP and AS. After decryption, MP's name and the shared encryption key between MP and TGS will be obtained. $\{T_{MP,tgs}\}PubK_{MP}$ will be decrypted with its public key $PubK_{MP}$ by MP, and the digital signature of AS will also be removed , thus $K_{MP,tgs}$ will be acquired. This two $K_{MP,tgs}$ will be compared to confirm whether they are same. If so, the shared encryption key $K_{MP,tgs}$ between MP and TGS will be saved by MP. Then the shared encryption key will be utilized as the key to communicate between TGS and MP, and to visit TGS together with $T_{MP,tgs}$.

The identity authorization bill $T_{MP,tgs}$ sent by AS will be encrypted with public key of TGS, that is $AS \rightarrow MP : \{\{K_{MP,tgs}\}K_{MP,as}, \{T_{MP,tgs}\}PubK_{tgs}\}$. Therefore, attackers may disguise as AS to send others' $T_{MP,tgs}$ or replay previous $T_{MP,tgs}$ to MP, which MP can't identify. In this paper, public key of MP is utilized to encrypt first, once MP receives response messages from AS, private key of its own will be utilized to decrypt the message upon. Then, comparing the decrypted information with that in the $T_{MP,tgs}$, it will be confirmed whether the messages is fake or replayed.

3. When accessing wireless Mesh network, new node MP will send a message to TGS first, apply for authorization bill for visiting TGS. The request message contains the authentication information $A_{MP,tgs}$ and identity authorization bill $T_{MP,tgs}$. Then public key of TGS will be utilized to encrypt the $T_{MP,tgs}$, which can ensure that MP's identity authorization bill $T_{MP,tgs}$ can only be decrypted by TGS, thus guarantee the security of $K_{MP,tgs}$ further. The authentication information $A_{MP,tgs}$ in request message contains the MP's name, node MPP's name, MP's address, the validity date of passport, and random number, etc. The authentication information is encrypted by the session key $K_{MP,tgs}$ between the new node MP and the TGS. When TGS receives the request message, $\{T_{MP,tgs}\}PubK_{tgs}$ be will decrypted with private key $\Pr vK_{tgs}$. At the same TGS will verify the digital signature of the AS inside $T_{MP,tgs}$. If the verification passes, it means that the new node MP can access the Internet. Then the TGS will receive the session key $K_{MP,tgs}$ between MP and TGS. Then, the authentication information $A_{MP,tgs}$ will be decrypted by the TGS with the session key. After comparing and analyzing the new node MP's name, address Addr, and with the corresponding information in $T_{MP,tgs}$, TGS will confirm whether the message sender is the new node MP marked by $T_{MP,tgs}$ or not.

4. When the new node MP receives a response message from the TGS, the response message will be decrypted with $K_{MP,tgs}$ by MP, then the random number information N_{MP} will be acquired. The random number N_{MP} will be compared with the random number N_{MP} that MP itself sent to the TGS. If the two numbers are equal, then it can be confirmed that this message is a new message. Then, the signatures in the passport will be verified by the new node MP, if the verification passes, then it can be proved that the passport is sent by TGS itself[11]. The bill $T_{MP,MPP}$ will be reserved by MP to obtain the right to access MPP for MP. In addition, the new node MP will reserve the session key between MP and MPP. When receiving a response message from TGS, MP will utilize his private key to decrypt the response information to gain the $T_{MPP,MP}$ and the random number N_{MP} . Then the new node MP will verify the signature of TGS. After the verification, the $K_{MP,MPP}$ will be saved and used as the shared key between MP and MPP.

5. When a new node MP apply for access to wireless Mesh network (WMN), the new node MP will send messages to the KNAS server on the MPP to request access service. The message contains the name of MPP, the name of MP, random number and the passport $T_{MP,MPP}$ requested from TGS, in which, MPP's name, MP's name and the random number are encrypted with the shared key between MP and MPP. After encryption, $K_{MP,MPP}$ will be encrypted with the public key once again. This double encryption can improve the security of the message.

When the KNAS server on the MPP receives a request message from the new node MP, the KNAS server will use its private key to decrypt the message to obtain permission $T_{MP,MPP}$. MPP will first verify the signature of $T_{MP,MPP}$. The pass of verification proves that the passport come from TGS, then MPP utilize $K_{MP,MPP}$ of $T_{MP,MPP}$ to decrypt $\{MPP, MP, N_{MPP}\}K_{MP,MPP}$. After that, MP's name and MPP's name will be compared with those that MP sent to the KNAS server. If they are the same, it shows that the sender of this message is the new node MP marked in the passport, by which MP will be identified [12]. At last, $K_{MP,MPP}$ in the $T_{MP,MPP}$ will be saved by MPP as the shared key between MP and MPP.

6. After the verification on MP by KNAS on the MPP, KNAS will send confirmation message to the new node MP. The confirmation message includes the name of the MPP, the name of MP and the random number. The message is encrypted with the shared key $K_{MP,MPP}$ between MP and MPP. The new node MP will decrypt the response information MPP sent with $K_{MP,MPP}$ .After decryption, MP will verify whether the MPP's name, MP's name and N_{MPP} are the same or not. If they are the same, it proves that MPP has permit MP to access Mesh wireless network, and MP has got the shared session key between MP and MPP. That means MP has passed the authentication, and

can interconnect with at least one MPP. Then both sides can communicate with each other with the shared key.

III. SECURITY ANALYSIS

In this paper, traditional Kerberos protocol was improved by adding public key cryptosystem, which in a certain extent overcome the shortcomings of traditional Kerberos, and improve the security of Wireless Mesh network identity authentication scheme. Compared with the traditional Kerberos protocol, the new Kerberos protocol can meet the security standards better. The new Kerberos protocol has the following characteristics:

a) Random number was introduced into the Kerberos protocol to replace the timestamp in the traditional Kerberos protocol, which avoids the clock synchronization problem in the network. When the new node MP receives the response information sent by TGS, MP will decrypt the response message with session key between MP and TGS to get Nc. Compare Nc with the random number that MP sent to TGS. If they are the same, it means that the message is new, not a retransmitted one, which can prevent the replay attacks.

b) In the Kerberos protocol discussed in this scheme, message is first encrypted with the private key of the sender and then the public key of receiver. Only after being decrypted with private key of the sender, can we know which public key should be used to get the final information; PIK technique was brought to guarantee the integrity of messages between MP and the server, which could alleviate the password guessing problem in the traditional Kerberos protocol.

c) In the improved Kerberos protocol, only public key of the new node MP is reserved in the authentication server AS. The private key of the new node MP is kept by MP itself. Therefore, even if the database is accessed illegally, not too much damage will be caused.

d) According to the improved Kerberos protocol, operations are taken only in the new node MP and authentication server AS. While in the sessions between MP and TGS, or MP and MPP, there isn't any operation. Thus, public key will not be involved into high-cost calculation. Therefore, execution efficiency will be improved. The requirements for the PKI (Public Key Infrastructure) are relatively low due to the limited quantities of the AS, TGS and MPP.

IV. CONCLUSIONS

In order to make up the shortage of the traditional Kerberos protocol, an improved authentication scheme was proposed in this paper. PKI techniques are introduced in the scheme to secure the process of authenticating, and random number is added in the interaction between entities in the scheme. The analysis indicates that the proposed scheme is practical in wireless mesh network.

In future work, we are focusing on the authentication in mobile cloud computing environment, more precisely, how to design the federal authentication protocol in cross-domain situation.

ACKNOWLEDGMENT

This paper is supported by National Natural Science Foundation of China: "Research on Trusted Technologies for The Terminals in The Distributed Network Environment" (Grant No. 60903018), "Research on the Security Technologies for Cloud Computing Platform" (Grant No. 61272543), and "The National Twelfth Five-Year Key Technology Research and Development Program of the Ministry of Science and Technology of China" (Grant No. 2013BAB06B04), "Key Technology Project of China Huaneng Group" (Grant No.HNKJ13-H17-04).

REFERENCES

[1] I. Akyildiz, and X. Wang, Wireless mesh networks, John Wiley & Sons, 2009.

[2] I.F. Akyildiz, X. Wang, and W. Wang, Wireless mesh networks: a survey, Computer networks, vol. 47, no. 4, 2005, pp. 445-487.

[3] W. Ze, W. Qi, L. Wenju, and K. Yongzhen, Scalable authentication protocol for wireless mesh network access, IEEE Press, Year Published, pp. 3051-3054.

[4] L. Wenju, S. Yuzhen, and W. Ze, A wireless mesh network authentication method based on identity based signature, IEEE, Year Published, pp. 1-4.

[5] B.C. Neuman, and T. Ts'O, Kerberos: An authentication service for computer networks, Communications Magazine, IEEE, vol. 32, no. 9, 1994, pp. 33-38.

[6] Wei He, The research of remote access VPN password authentication protocol based on improved Kerberos system, Zhejiang: Zhejiang University, 2003, pp.

[7] P.L. Hellewell, T.W. Van Der Horst, and K.E. Seamons, Extensible Pre-authentication Kerberos, IEEE, Year Published, pp. 201-210.

[8] S.T.F. Al-Janabi, and M. Rasheed, Public-Key Cryptography Enabled Kerberos Authentication, IEEE, Year Published, pp. 209-214.

[9] N.T. Abdelmajid, M.A. Hossain, S. Shepherd, and K. Mahmoud, Location-Based Kerberos Authentication Protocol, IEEE, Year Published, pp. 1099-1104.

[10] B. Wang, Y. Wang, and H. Zhang, A new secure password authentication scheme using smart cards, Wuhan University Journal of Natural Sciences, vol. 13, no. 6, 2008, pp. 739-743.

[11] Xilan Wu, Yuanzhong Shu, Zetao Jiang , and Zhihong Wu, An improved Kerberos protocol combined with PKI Technology, Computer Application and Software, vol. 26, no. 2, 2009, pp. 85-86.

[12] Peishun Liu, and Hongyu Liu, The research on the identity authentication technology of the ocean environment information of cloud computing, The Technology Journal of Huazhong University of Science (Natural Science Edition), vol. 1, 2012.