A Formal Method of Secrecy and Authentication Analysis for Ad-hoc Secure Routing Protocol

Lei Yu, Yuyan Guo and Mingming Jiang*

***Abstract*—**Ideals and honesty theory is the branch of the strand space model theory. The concept of ideal can not only strictly define attacker's ability, but also give precise definition of protocol security attribute. The theory of honesty reduces the complexity of formal analysis for secure protocol, and makes the formal analysis more scientific and rigorous. Authentication and secrecy are the main security attributes of Ad-hoc secure routing protocol. Because the Ad-hoc network has the characteristics of no center, mobile and open, the formal description of the network environment and security attribute of Ad-hoc security routing protocol is more complex. Because of the lack of formalized theory in the structure and security attribute analysis of message components, the non-formal phenomenon exists in the analysis of security protocols using ideal and honesty theory. In this paper, the formal analysis theory of the structural features and security attributes of the message component is perfected, and the network environment and the security attribute of the secure routing protocol are formally defined by the ideal and honesty theory. Based on the formal analysis of the SGSR secure routing protocol, a more rigorous and effective formal analysis method for security and authentication of Ad-hoc security routing protocol is given.

***Keywords*—**strand space model theory, ideal and honesty theory, Ad-hoc secure routing protocol, formal analysis.

I. INTRODUCTION

MANET (Mobile Ad Hoc Network) has been widely applied to various fields such as industry, military, medical care and family by virtue of its self-organizing characteristic. In addition to the need to exchange network topology information, the single hop private key is required to exchange and the collected data information shall be transmitted through the network nodes in most MANET routing protocols, which is not only related to the normal execution of protocols but also involved in the privacy of the user data. It is just because of the characteristics such as free-center, mobile and open of the protocol in running network environment that makes the secrecy and completeness of data and the credibility among the network nodes become the key points in designing AD-hoc security routing protocol. The correctness of newly designed Ad-hoc security routing protocol shall be analyzed before the protocol is put into use so as to provide the correctness proof of Ad-hoc security routing protocol more rigorously and credibly. In recent years, various formal analysis methods and technologies for traditional cryptographic protocol have begun to be applied to analysis and research of Ad-hoc security routing protocol such as BAN logic[1], Athena method[2], strand space theory[3,4] and Meadows algebra model[5], etc. Different from the formal analysis of traditional cryptographic protocols, the security of Ad-hoc security routing protocol is not only related to the message organization structure but also restricted by its network topology structure.

In many formal analysis methods, strand space model theory[6,7] proposed by Fabrega et al. applies the theorem proving method to analyze the security of cryptographic protocols in the framework of Dolev-Yao model[8] through the formalization of the partial structure of protocol traces, which can not only avoid the explosion of state space universally in the model detection methods, but also has precise, rigorous and flexible advantages in the aspects of network environment modeling, protocol description, protocol analysis and theory expansion compared with other formal methods. In particular, the subsequent ideal and honesty theory[9] makes the description of the protocol message terms and protocol security attributive more accurate and the definition of the penetrator ability more stringent. Besides, the ideal and honesty theory simplifies the protocol analysis process and reduces the complexity of process analysis.

In consideration of the complexity of the Ad-hoc security routing protocol and the advantages of the strand space model theory on network environment model structure, protocol description as well as formal analysis methods, this paper focuses on studying the formal analysis methods of secrecy and authentication for the Ad-hoc security routing protocol with the ideal and honesty theory, based on the strand space model in combination with the specific Ad-hoc security routing protocol. Although the security of the protocol is closely related to the network topology, the realization mechanism and principle of authentication and secrecy for the protocol are consistent with that of the traditional cryptographic protocol, thus the Dolev-Yao model can describe the network environment of the protocol more accurately.

The formal analysis practice of the traditional cryptographic

This work was supported by Science Foundation for The Excellent Youth Scholars of Anhui University(gxyq2017154) , and in part by Natural Science Foundation of Anhui University (KJ2014A231,KJ2017A848,KJ2015A315).

Lei Yu is with the School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, Anhui, China.

Yuyan Guo is with the School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, Anhui, China.

Mingming Jiang is with the School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, Anhui, China (corresponding author; e-mail: jiangmm3806586@126.com).

protocol indicates that the lack of research on cryptographic properties of message structure in original strand space model theory causes non-formal phenomenon when the message components are analyzed with the ideal and honesty theory[7,9,10], thus resulting in non-rigorous process of protocol analysis and affecting the correctness of the protocol analysis result . So the research on the formalization and the cryptology property of the message component structure characteristic is a key to improve the formal analysis method of the Ad-hoc security routing protocol, which is also the innovation of this paper.

The experiment protocol to be adopted in this paper is SGSR protocol [11]that is the improved version of GSR protocol on the security mechanism in order to mainly prevent malignant node forge and tampering attack in the Ad-hoc network, in which the single hop private key delivery protocol (SHKE)is the core. In[11],the author provided the formal analysis of the protocol with the BAN logic in the initial design period of the SHKE protocol. Only authentication analysis of SHKE was offered, while the secrecy analysis of the single hop private key was not offered due to the defects of the BAN logic itself. Secondly, non-formal methods were overused in the initial assumption and the protocol analysis process of the SHKE protocol by the BAN logic, which could easily cause fault analysis conclusions. This paper will analyze the secrecy and authentication of SHKE protocol comprehensively and deeply with the improved ideal and honesty theory based on the strand space model so as to verify the correctness of the protocol design again.

II. Basic Theory of the Strand Space Model

A. Message Algebra Space

Definition 1. Suppose $\mathcal{A}$ as a message set that interacts among the protocol principal, $\mathcal{T}$ is the atomic message set, and $\mathcal{K}$ is the key set, then $\mathcal{T}$ is the subset of $\mathcal{A}$, denoted by $\mathcal{T} \subseteq \mathcal{A}$, and $\mathcal{K}$ is the subset of $\mathcal{A}$ meets $\mathcal{K} \subseteq \mathcal{A} \wedge \mathcal{K} \bigcap \mathcal{T} = \phi$, A unary operator on $\mathcal{A}$ is $inv: \mathcal{K} \to \mathcal{K}$, Two binary operators: $encr: \mathcal{K} \times \mathcal{A} \to \mathcal{A}$ and $join: \mathcal{A} \times \mathcal{A} \to \mathcal{A}$.

Suppose $m, n \in \mathcal{A}, k \in \mathcal{K}$, $inv(k)$ is commonly denoted by k^{-1} for simplicity and $encr(k, m)$ is denoted by $\{m\}_k$ and $join(m, n)$ is denoted by mn.

The sets generated by *encr* and *join* operations are respectively denoted by $\mathcal{E}$ and $\mathcal{J}$,and $\mathcal{K} \bigcap \mathcal{T} \bigcup \mathcal{E} \bigcap \mathcal{J} = \phi$.

Definition 2. $a, b, g, h \in \mathcal{A}, k \in \mathcal{K}$, and a is the sub-term of b, denoted by $a \subset b$. If $b \in \mathcal{T} \bigcap \mathcal{K}$, then $a = b$; if $b = \{h\}_k$, then $a \subset h \vee a = \{h\}_k$; if $b = gh$, then $a \subset g \vee a \subset h \vee a = gh$.

Definition 3. A pair $< \sigma, a >$ is a signed term, $\sigma \in \{+, -\}$, $a \in \mathcal{A}$, where $+a$ represents sending message and $-a$ represents receiving information and $(\pm\mathcal{A})^*$ represents the set of the signed term sequences and its element is $<< \sigma_1, a_1 >, \cdots, < \sigma_n, a_n >>$.

Definition 4. $h \in \mathcal{A}$, if $h \in \mathcal{T} \bigcup \mathcal{K} \bigcup \mathcal{E}$, then h is called the simple term, and if $h \in \mathcal{J}$, then h is called the connection term.

B. Freedom Assumptions on Term Algebra Space

Axiom 1. If $m_0, m_1, m_0^{'}, m_1^{'} \in \mathcal{A}$ and $k_0, k_1 \in \mathcal{K}$:

(1) $\{m_0\}_{k_0} = \{m_1\}_{k_1} \Rightarrow m_0 = m_1 \wedge k_0 = k_1$;

(2) $m_0 m_1 = m_0^{'} m_1^{'} \Rightarrow m_0 = m_0^{'} \wedge m_1 = m_1^{'}$;

(3) $m_0 m_1 \neq \{m_0^{'}\}_k$;

(4) $m_0 m_1 \notin \mathcal{K} \bigcup \mathcal{T}$;

(5) $\{m_0\}_k \notin \mathcal{K} \bigcup \mathcal{T}$.

C. Strand Space Model

Strands are message sending and receiving sequences of the protocol principal to denote the behavior of the legitimate participant and the action sequence of the penetrator.

Definition 5. A strand space represents a set Σ and a trace mapping $tr: \Sigma \to (\pm\mathcal{A})^*$.

Definition 6. Suppose Σ is a strand space and its construction method is as follows:

(1) $s \in \Sigma$, the node n on s is denoted by two-tuples $< s, i >$, $1 \le i \le length(tr(s))$,and the node set is denoted by $\mathcal{N}$.

(2) If $n \in \mathcal{N}$, then $strand(n)$ denotes that the strand of n is s, $index(n)$ denotes the position of n in s and $term(n)$ denotes the signed term of n, while $uns\_term(n)$ denotes the unsigned term of n, and $sign(n)$ denotes the sign of n.

(3) $n_1, n_2 \in \mathcal{N}$, $n_1 \to n_2$ denotes that there is $a \in \mathcal{A}$ to meet $term(n_1) = +a$ and $term(n_2) = -a$.

(4) $n_1, n_2 \in \mathcal{N}$, n_1 and n_2 belong to the same strand s, $index(n_2) > index(n_1)$, $i = index(n_2) - index(n_1)$. If $i \ge 1$, then $n_1 \Rightarrow^+ n_2$ denotes that n_1 is the predecessor of n_2, and if $i = 1$, $n_1 \Rightarrow n_2$ denotes that n_1 is the direct predecessor of n_2.

(5) $t \in \mathcal{A}, n, n^{'} \in \mathcal{N}, n^{'} \Rightarrow^+ n$. If t originates from n, if and only if $sign(n) = + \ \wedge t \subset term(n) \ \wedge t \not\subset term(n^{'})$; t only originates from n, if and only if only node n generates t.

(6) S is a set of unsigned term and the node $n \in \mathcal{N}$ is the entry point of S, if and only if there is $t \in S, term(n) = +t$, and if there is $n^{'} \Rightarrow^+ n$, then $t \not\subset term(n^{'})$.

Definition 7. Node set $\mathcal{N}$ and $\to$ edge set as well as $\Rightarrow$ edge set constitute the ordered graph of strand space Σ, denoted by $< \mathcal{N}, (\to \bigcup \Rightarrow) >$. Given set $\to_C \subset \to$, set $\Rightarrow_C \subset \Rightarrow$, and $C =< \mathcal{N}_C, (\to_C \bigcup \Rightarrow_C) >$ is a subgraph of $< \mathcal{N}, (\to \bigcup \Rightarrow) >$, then C is the protocol bundle on the strand space Σ if and only if:

(1) C is a finite set;

(2) If $n \in \mathcal{N}_C$ and $sign(n) = -$, then there is a only node $n^{'}$ such that $n^{'} \to_C n$;

(3) If $n \in \mathcal{N}_C$ and $n^{'} \Rightarrow n$, then $n^{'} \Rightarrow_C n$.

If $n \in \mathcal{N}_C$, then it is called that the node n is in the bundle $C =< \mathcal{N}_C, (\rightarrow_C \cup \Rightarrow_C) >$, denoted by $n \in C$. If there is $< s, i > \in \mathcal{N}_C$ for any integer $0 < i \leq length(s)$ and $s \in \Sigma$, then it is called that strand s is in the bundle C, where the maximum of i is called the height of strand s in the bundle C, denoted by $C - height(s)$.

D. Penetrator Capacity

Definition 8. Penetrator strand is used to describe the capacity of the penetrator in the network, of which the node is called as the penetrator node. I represents the penetrator and $\mathcal{K}_I$ means the key set of the penetrator, then the strand space model of the penetrator capacity is as follows:

(1) Sending plaintext: $M.< +t >$, where $t \in \mathcal{T}$;

(2) Issuing key: $K.< +k >$, and $k \in \mathcal{K}_I$, where $\mathcal{K}_I$ represents the key set mastered by the penetrator;

(3) Intercepting message: $F.< -g >$, where $g \in \mathcal{A}$;

(4) Retransmitting message: $T.< -g, +g, +g >$ where $g \in \mathcal{A}$;

(5) Connecting message: $C.< -g, -h, +gh >$, where $g, h \in \mathcal{A}$;

(6) Decomposing message: $S.< -gh, +g, +h >$, where $g, h \in \mathcal{A}$;

(7) Encrypting message: $E.< -k, -h, +\{h\}_k >$, where $g, h \in \mathcal{A}$ and $k \in \mathcal{K}_I$;

(8) Decrypting message: $D.< -k^{-1}, -\{h\}_k, +h >$, where $g, h \in \mathcal{A}$ and $k^{-1} \in \mathcal{K}_I$.

E. Ideal and Honesty

Definition 9. If $K \subseteq \mathcal{K}$, and I is the subset of $\mathcal{A}$, then the following conditions are met for any $h \in I$, $g \in \mathcal{A}$ and $k \in K$:

(1) $hg, gh \in I$;

(2) $\{g\}_k \in I$;

Then it is called that I is an $K - ideal$ of $\mathcal{A}$ and the minimum $K - ideal$ including g is denoted by $I_K[g]$. If $S \subseteq \mathcal{A}$, then $I_K[S]$ is the minimum $K - ideal$ including S.

Property 1. $g \subset h$, if and only if $h \in I_K[g]$.

Property 2. If $S \subseteq T$, then $I_K[S] \subseteq I_K[T]$.

Property 3. If $S \subseteq \mathcal{A}$, $K \subseteq \mathcal{K}$, then $\forall s \in S$ where s represents a simple term. If $gh \in I_K[S]$, then $g \in I_K[S]$ or $h \in I_K[S]$.

Property 4. If $S \subseteq \mathcal{A}$, $K \subseteq \mathcal{K}$, $\forall s \in S$ where s is a simple term and is not of the form $\{g\}_k$. If $\{h\}_k \in I_K[S]$, then $h \in I_K[S]$.

Property 5. If $S \subseteq \mathcal{A}$, $K \subseteq \mathcal{K}$, then $\forall s \in S$ where s is simple term and is not of the form $\{g\}_k$. If $\{h\}_k \in I_K[S]$, then $k \in K$.

Theorem 1. Suppose C is a bundle of $\mathcal{A}$, $I \subseteq \mathcal{A}$, $n \in \mathcal{N}$. If n is a minimal element of set $\{n \in C : term(n) \in I\}$, then n is an entry point of I.

Definition 10. Suppose C is a bundle of $\mathcal{A}$, $I \subseteq \mathcal{A}$, $n \in \mathcal{N}_I$ is the penetrator node. If n is the entry point of I, if and only if n is M node or K node, then it is called that I is honest.

Theorem 2. Suppose C is a bundle of $\mathcal{A}$, $S \subseteq \mathcal{T} \bigcup \mathcal{K}$, $K \subseteq \mathcal{K}$, and $\mathcal{K} \subseteq S \bigcup K^{-1}$, then $I_K[S]$ is honest.

Corollary 1. Suppose C is a bundle of $\mathcal{A}$, $\mathcal{K}_I$ is the key set of the penetrator, $\mathcal{K} = S \bigcup K^{-1}$, and $S \bigcap \mathcal{K}_I = \phi$. If there is a node $m \in C$ to make $term(m) \in I_K[S]$, then there is a regular node $n \in C$ to make that n is an entry point of $I_K[S]$.

Corollary 2. Suppose C is a bundle of $\mathcal{A}$, $\mathcal{K}_I$ is the key set of the penetrator, $\mathcal{K} = S \bigcup K^{-1}$, and $S \bigcap \mathcal{K}_I = \phi$. If there is no regular node $m \in C$ to be the entry point of $I_K[S]$, then no term in the form such as $\{g\}_k$ originates from a penetrator node.

III. 2 Message components

A. Formalization of Message Components

Definition 11. Suppose $t \subset term(n)$, if there is t' to meet $t \subset t' \subset term(n)$, then t' can only be a simple term, then it is called that t is the component of node n. Namely, the message component can only be atomic type or encryption type.

Definition 12. Suppose t is the message component of node n and its structure form is $\{h\}_k$. (1) If $k = null$ and $t \in \mathcal{T}$, then it is called that t is the atomic component of n, the type of t is denoted by T; (2) If $k = null$ and $t \in \mathcal{K}$, then it is called that t is the atomic component of n, the type of t is denoted by K; (3) If $k \neq null$ and $k \in \mathcal{K}$, then it is called that t is the encryption component of n, the type of t is denoted by E.

Definition 13. Suppose X is the protocol principal and n is the node on the strand of X, then t is the component of n to meet $a \subset t \subset term(n)$. If the X can obtain value a through component t, then it is called that the component t has knowability of principal X on value a. Otherwise, it is called that the component t has no knowability of principal X on value a.

B. Property of the Message Components

The cryptographic property of the message components can be obtained according to Definition 1 and Definition 7.

Property 6. Suppose t is the component of node n, $t \subset term(n)$, t is an atomic component, then t is knowable to all principals.

Property 7. Suppose t is the component of the node n, $t \subset term(n)$, t is the encrypted component with the form

$t=\{h\}_k$, where a is the component of h, X is the protocol principal and K_X is the private key set of X. (1) If $k^{-1}\in K_X$, then t has knowability to X on a. (2) If $k\in K_X$, $k^{-1}\notin K_X$, if t originates from principal X, then component t has unknowability to principal X on the value a.

IV. Correctness of the Protocol

A. Secrecy

Definition 14. Suppose $M,N\in\mathcal{A}$, where N represents simple term. $M\Rightarrow N$ denotes that N can be deducted from M through behaviors of F,T,C,S,E,D.

Definition 15. Suppose C is the protocol bundle, $h\in\mathcal{A}$ is the message term that needs to be secretive, $N=\{n:m\Rightarrow n,m\in M\}$. If $h\notin N$, then h has secrecy.

B. Authentication

Theorem 3. Suppose M is the set of all message terms in the protocol P, $M_{Auth}\subseteq M$ is the set of the authenticated terms, M_I is the message set to be constructed by the penetrator and $N=\{n:m\Rightarrow n,m\in M\}$ is the set of simple terms to be derived by the penetrator. Then the sufficient condition for P to meet the authentication is $I_{K_I}[M_I]\bigcap M_{Auth}=\phi$.

Theorem 3 can be proved according to Corollary 1, Corollary 2 and the minimal element theory.

Definition 16. Suppose C is the protocol bundle, A is the initiator of the protocol, B is the responder of the protocol, then A and B need to meet the following two conditions to authenticate each other:

(1) There is a unique initiator corresponding to it when B completes a round of protocol with the deemed initiator A by using all data on the B strand;

(2) There is a unique responder corresponding to it when A uses all data on the A strand so as to complete a round of protocol with the deemed responder B.

V. Analysis on Secrecy and Authentication of SHKE Protocol

The authentication and secrecy of SGSR are mainly realized through SHKE protocol that are abstracted out alone in the paper to facilitate the description and analysis of the protocol.

A. SHKE Protocol

$$M_1\quad A\rightarrow B:Cert_A\{N_a\}_{k_A^{-1}}N_a$$

$$M_2\quad B\rightarrow A:\{\{k_{TC-B},N_a\}_{k_B^{-1}}\}_{k_A}Cert_B$$

$$M_3\quad A\rightarrow B:\{\{k_{TC-A},N_a\}_{k_A^{-1}}\}_{k_B}$$

The above is the formal description of SHKE protocol, A and B are the abstract of the adjacent nodes in the Ad-hoc network, where A is the initiator and B is the responder. $A,B\in T_{name}$ ($T_{name}\subseteq T$) are the name set of the protocol principals. $Cert_A$ and $Cert_B$ are respectively the digital certificate of A and B. k_A and k_A^{-1} are respectively the private key and public key of A. k_B and k_B^{-1} are respectively the private key and public key of B. k_{TC-A} and k_{TC-B} are respectively the single hop authentication key for A and B. N_a is the random number generated by A. The bundle graph of SHKE protocol is illustrated as Figure 1.

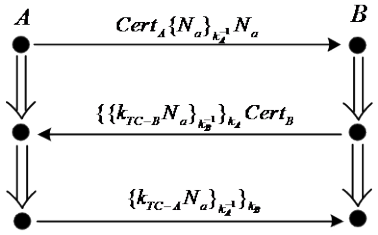

Fig.1. Bundle graph of SHKE protocol

In SHKE protocol, the random N_a is used to ensure the freshness, origin, and uniqueness of the message term, encryption with private keys is to prove the origin of k_{TC-A}, k_{TC-B} and N_a, and encryption using the public key to ensure the secrecy of k_{TC-A} and k_{TC-B}.The authentication and secrecy are the main security properties of this protocol.

B. Strand Space Model of SHKE Protocol

Definition 17. Suppose Σ is the strand space of SHKE protocol, $\mathcal{P}$ is the set of the penetrator strand, $init[*]$ is the set of the initiator strand, and $resp[*]$ is the set of the responder strand, $\Sigma=\mathcal{P}\bigcup init[*]\bigcup resp[*]$.

(1) Initiator strands $init[*]=init[A,B,Cert_A,Cert_B,N_a,k_{TC-A},k_{TC-B}]$, and the trace of $s\in init[*]$ is:

$$<+Cert_A\{N_a\}_{k_A^{-1}}N_a,$$
$$-\{\{k_{TC-B}N_a\}_{k_B^{-1}}\}_{k_A}Cert_B,$$
$$+\{\{k_{TC-A}N_a\}_{k_A^{-1}}\}_{k_B}>,$$

the principal corresponding to this strand is A.

(2) Responder strands $resp[*]=resp[A,B,Cert_A,Cert_B,N_a,k_{TC-A},k_{TC-B}]$, and the trace of $s\in resp[*]$ is:

$$<-Cert_A\{N_a\}_{k_A^{-1}}N_a,$$
$$+\{\{k_{TC-B}N_a\}_{k_B^{-1}}\}_{k_A}Cert_B,$$
$$-\{\{k_{TC-A},N_a\}_{k_A^{-1}}\}_{k_B}>,$$

the principal corresponding to this strand is B.

C. Secrecy Analysis

Proposition 1. Suppose Σ is the strand space of the SHKE protocol, C is a bundle in Σ, $A,B\in T_{name}$, $s_{Init}\in init[A,B,Cert_A,Cert_B,N_a,k_{TC-A},k_{TC-B}]$, $k_A^{-1},k_B^{-1},k_{TC-A}\notin K_I$, k_{TC-A},k_{TC-B},N_a are not equal to each other, and k_{TC-A} is uniquely generated in Σ, set

$S=\{k_A^{-1},k_B^{-1},k_{TC-A}\}$, $K=\mathcal{K}\setminus S$. Then $uns\_term(m)\notin I_K[S]$ for any $m\in C$.

Proof: It can be known that $S\bigcap\mathcal{K}_I=\phi$ and $\mathcal{K}=K\bigcup S$ from the assumption. It is only needed to prove that there is no regular node to be the entry point of $I_K[S]$ according to Corollary 1.

Prove by contradiction, suppose the regular node m is the entry point of $I_K[S]$, then $sign(m)=+$, $uns\_term(m)\in I_K[S]$, and then it can be obtained that $k_A^{-1}\subset term(m)$ $\vee k_B^{-1}\subset term(m)$ $\vee k_{TC-A}\subset term(m)$,according to the proposition assumption. It then can be known that there is no regular node to include k_A^{-1} and k_B^{-1} in the regular strand and $k_{TC-A}\neq k_{TC-B}$ from Definition 17, so $k_{TC-A}\subset term(m)$. Suppose s is the regular strand of the node m, then there are the following possibilities for $k_{TC-A}\subset term(m)$:

(1) $s\in init[*]$, $m=<s,1>$. Suppose k_{TC-A} is uniquely generated in Σ from the proposition, so $s=s_{init}$, $term(m)=+Cert_A\{N_a\}_{k_A^{-1}}N_a$. Because N_a is simple without the form of $\{h\}_{k_A^{-1}}$, then $k_A^{-1}\in K$ is obtained, which is contradictory to $K=\mathcal{K}\setminus S$ from Property 5.

(2) $s\in init[*]$, $m=<s,3>$. Suppose k_{TC-A} is uniquely generated in Σ from the proposition, so $s=s_{init}$, $term(m)=+\{\{k_{TC-A}N_a\}_{k_A^{-1}}\}_{k_B}$. Because $\{k_{TC-A}N_a\}_{k_A^{-1}}$ is simple and $k_B\neq k_A^{-1}$ as well as $\{k_{TC-A}N_a\}_{k_A^{-1}}$ does not have the form of $\{h\}_{k_B}$, then it can be known that $\{k_{TC-A}N_a\}_{k_A^{-1}}\in I_K[S]$ from $k_B\in K$ and Property 4; because $k_{TC-A}N_a$ is not simple, then it can be obtained that: $k_{TC-A}N_a\in S$ or $k_{TC-A}N_a\in I_K[S]\setminus S$; it can be known that $k_{TC-A}N_a\notin S$ from the proposition assumption, so $k_{TC-A}N_a\in I_K[S]\setminus S$; Since $\{k_{TC-A}N_a\}_{k_A^{-1}}\notin S$, then the result is $\{k_{TC-A}N_a\}_{k_A^{-1}}\in I_K[S]\setminus S$. According to definition of the idea, $k_A^{-1}\in K$ is obtained, which is contradictory to $K=\mathcal{K}\setminus S$.

To sum up, the regular node m is not the entry point of $I_K[S]$, so the assumption is not established while the conclusion of the Proposition 1 is true.

The SHKE protocol can meet the secrecy according to Definition 15.

Proposition 2. Suppose Σ is the bundle space of SHKE protocol, C is a bundle in Σ , $A,B\in\mathcal{T}_{name}$, $s_{resp}\in resp[A,B,Cert_A,Cert_B,N_a,k_{TC-A},k_{TC-B}]$, $k_A^{-1},k_B^{-1},k_{TC-A}\notin\mathcal{K}_I$, k_{TC-A},k_{TC-B},N_a are not equal to each other, and k_{TC-B} is uniquely generated in Σ , set $S=\{k_A^{-1},k_B^{-1},k_{TC-B}\}$, $K=\mathcal{K}\setminus S$. Then $uns\_term(m)\notin I_K[S]$ for any $m\in C$.

It can be proved that the conclusion of Proposition 2 is also true with ideal and honesty theory, the proof process is similar to that of Proposition 1, thus it is no longer to repeat.

The conclusions of Proposition 1 and Proposition 2 are true, indicating that SGSR protocol can meet the secrecy of the single hop private key.

D. Authentication Analysis

Lemma 1. Suppose C is a bundle in the strand space Σ of SGSR authentication and single hop private key delivery protocol, $X\in\mathcal{T}_{name}$ and $k_X^{-1}\notin\mathcal{K}_I$. Then no term in the form of $\{g\}_{k_X^{-1}}$ in C will originate from the penetrator node.

Proof: set $S=\{k_X^{-1}\}$, $K=\mathcal{K}$, suppose there is a regular node m to be the entry point of $I_K[S]$, then it can be known from Theorem 1 that: $m=<s_{init},1>\vee m=<s_{init},3>\vee m=<s_{resp},3>$, then $k_X^{-1}=N_a$ $\vee k_X^{-1}=k_{TC-A}$ $\vee k_X^{-1}=k_{TC-B}$, which is contradictory to $S\bigcap\{k_{TC-A},k_{TC-B},N_a\}=\phi$, so the assumption is not established. So there is no regular node to be the entry point of $I_K[S]$. No term in the form of $\{g\}_{k_X^{-1}}$ in C will originate from the penetrator node. Thus the lemma is proved.

Lemma 2. If $\{g\}_{k_X^{-1}}$ originates from the node m of a regular strand s , then there are the following conclusions:

(1) If $s\in init[*]$, then the structure form of g is $g=T$ or $g=KT$;

(2) If $s\in resp[*]$, then the structure form of g is $g=KT$.

Proof: if $\{g\}_{k_X^{-1}}$ originates from m , then $sign(m)=+$ according to Definition 6(5).

If $s\in init[*]$, then $m=<s,1>\vee m=<s,3>$. $<s,1>=+Cert_A\{N_a\}_{k_A^{-1}}N_a$, $<s,3>=+\{\{k_{TC-A}N_a\}_{k_A^{-1}}\}_{k_B}$, and the encrypted sub-terms in the form of $\{g\}_{k_X^{-1}}$ are respectively $\{N_a\}_{k_A^{-1}}$ and $\{k_{TC-A}N_a\}_{k_A^{-1}}$; so the structure form of g is similar to that in the conclusions (1) of the lemma.

If $s\in resp[*]$, then $m=<s,2>.<s,2>=+\{\{k_{TC-B}N_a\}_{k_B^{-1}}\}_{k_A}$ $Cert_B$ is in the form of the encrypted sub-term $\{k_{TC-B}N_a\}_{k_B^{-1}}$ similar to $\{g\}_{k_X^{-1}}$, so the structure form of g is in the form of conclusion (2) of the lemma.

Corollary 3. Suppose s is a regular strand in the strand space Σ of SHKE protocol:

(1) If $\{T\}_{k_X^{-1}}$ originates from s , then there are $B,K,K^{'}$ to achieve $s\in init[X,B,*,*,T,K,K^{'}]$ and $\{T\}_{k_X^{-1}}\subset<s,1>$, and T originates from s ;

(2) If $\{KT\}_{k_X^{-1}}$ originates from s , and $X\neq B$, then there are $B,K^{'}$ to achieve $s\in init[X,B,*,*,T,K,K^{'}]$ and $\{KT\}_{k_X^{-1}}\subset<s,3>$, and K originates from s ;

(3) If $\{KT\}_{k_X^{-1}}$ originates from s, and $X \neq A$, then there are $A, K^{'}$ to achieve $s \in resp[A, X, *, *, T, K^{'}, K]$ and $\{KT\}_{k_X^{-1}} \subset < s, 2 >$, and K originates from s.

Proof: Since s is a regular strand, $s \in init[*] \cup resp[*]$, $init[*]$ and $resp[*]$ are not intersected to each other, then the Corollary 3 can be proved by applying the conclusion of the Lemma 2.

1) Guarantee of Initiator

Since $Cert_A$ and $Cert_B$ are respectively the digital certificates of A and B in the message term of SHKE protocol, it only plays the role of publishing the public key without secrecy. It does not play a key role on authentication of the protocol. Then the analysis on $Cert_A$ and $Cert_B$ will be ignored in the authentication analysis of the protocol hereinafter.

Proposition 3. Suppose Σ is a strand space of the SGSR authentication and single hop private key delivery protocol and C is a bundle in Σ, $A \neq B$, the random value N_a uniquely originates from C, and $k_X^{-1} \notin \mathcal{K}_I$, $X \in \mathcal{T}_{name}$, then if $s_{init} \in init[A, B, *, *, N_a, k_{TC-A}, k_{TC-B}]$, and $C - height(s_{init}) = 3$, there will a unique regular strand $s_{resp} \in resp[A, B, *, *, N_a, k_{TC-A}, k_{TC-B}]$ in C and $C - height(s_{resp})$ is at least 2.

Proof: The trace of s_{init} has the following form $< +Cert_A\{N_a\}_{k_A^{-1}} N_a, \quad -\{\{k_{TC-B} N_a\}_{k_B^{-1}}\}_{k_A} Cert_B, \quad +\{\{k_{TC-A} N_a\}_{k_A^{-1}}\}_{k_B} >$ according to the proposition assumption. The message components $\{k_{TC-B} N_a\}_{k_B^{-1}}$ and $\{k_{TC-A} N_a\}_{k_A^{-1}}$ both have knowability to the principal A according to the Property 7.

(1) Because $k_A^{-1} \notin \mathcal{K}_I$ and $\{N_a\}_{k_A^{-1}} \subset term(< s_{init}, 1 >)$, it can be known that N_a originates from the regular node according to the Lemma 1; because $sign < s_{init}, 1 >= +$ and the set $\{m : m \Rightarrow^{+} < s_{init}, 1 >\}$ is null, the N_a uniquely originates from $< s_{init}, 1 >$.

(2) Because $k_B^{-1} \notin \mathcal{K}_I$, it can be known from the Lemma 1 that the sub-term $\{k_{TC-B} N_a\}_{k_B^{-1}} \subset term(< s_{init}, 2 >)$ originates from the regular node in C; because $k_A^{-1} \neq k_B^{-1}$, it can be known from the Corollary 3(3) that there is $A^{'} \in \mathcal{T}_{name}$, $k^{'} \in \mathcal{K}$ to make $s_{resp} \in resp[A^{'}, B, *, *, N_a, k_{TC-A^{'}}, k_{TC-B}]$, $\{k_{TC-B} N_a\}_{k_B^{-1}}$ originates from $< s_{resp}, 2 >$ and the sub-term $\{N_a\}_{k_{A^{'}}^{-1}} \subset term(< s_{resp}, 1 >)$.

(3) Because $k_{A^{'}}^{-1} \notin \mathcal{K}_I$, the sub-term $\{N_a\}_{k_{A^{'}}^{-1}}$ originates from a regular strand $s^{'}$ according to the Lemma 1; then $B^{'} \in \mathcal{T}_{name}$, $k_{TC-A^{'}}, k_{TC-B^{'}} \in \mathcal{K}$ can be concluded to make $s_{init}^{'} \in init[A^{'}, B^{'}, *, *, N_a, k_{TC-A^{'}}, k_{TC-B^{'}}]$ from the Corollary 3(1), where N_a originates from $s_{init}^{'}$; Because of the uniqueness of the N_a origin, $s_{init}^{'} = s_{init}$ is produced, then $A^{'} = A$, $B^{'} = B$, $k_{TC-A^{'}} = k_{TC-A}$, $k_{TC-B^{'}} = k_{TC-B}$ is obtained.

To sum up, based on the uniqueness of random value N_a originated from C, there is unique $s_{resp} \in resp[A, B, *, *, N_a, k_{TC-A}, k_{TC-B}]$, because $< s_{resp}, 2 > \in C$, then $C - height(s_{resp}) = 2$. The proposition is thus proved.

2) Guarantee of Responder

Proposition 4. Suppose Σ is the strand space of the SHKE protocol, C is a bundle in Σ, $A \neq B$, and the random value N_a uniquely originates in C, and $k_X^{-1} \notin \mathcal{K}_I$, $X \in \mathcal{T}_{name}$, k_{TC-B} is the responder strand of the unique origin, and there is injection relation between N_a and k_{TC-B}, then if $s_{resp} \in resp[A, B, *, *, N_a, k_{TC-A}, k_{TC-B}]$ and $C - height(s) = 3$, there will be unique regular strand $s_{init} \in init[A, B, *, *, N_a, k_{TC-A}, k_{TC-B}]$ in C and $C - height(s_{init}) = 3$.

Proof: The trace of s has the following form $< -Cert_A\{N_a\}_{k_A^{-1}} N_a, \quad +\{\{k_{TC-B} N_a\}_{k_B^{-1}}\}_{k_A} Cert_B, \quad -\{\{k_{TC-A} N_a\}_{k_A^{-1}}\}_{k_B} >$ from the proposition assumption. The message components $\{k_{TC-B} N_a\}_{k_B^{-1}}$ and $\{k_{TC-A} N_a\}_{k_A^{-1}}$ are both knowable to the principal B.

(1) Because $k_A^{-1} \notin \mathcal{K}_I$, it can be found from the Lemma 1 that the sub-term $\{k_{TC-A} N_a\}_{k_A^{-1}} \subset term(< s_{resp}, 3 >)$ originates from the regular node in C; because $k_A^{-1} \neq k_B^{-1}$, it can be found from the Corollary 3(2) that $B^{'} \in \mathcal{T}_{name}$, $k_{TC-B^{'}} \in \mathcal{K}$ makes $s_{init} \in init[A, B^{'}, *, *, N_a, k_{TC-A}, k_{TC-B^{'}}]$, $\{k_{TC-A} N_a\}_{k_A^{-1}}$ originates from $< s_{init}, 3 >$ and the sub-term $\{k_{TC-B^{'}} N_a\}_{k_B^{-1}} \subset term(< s_{init}, 2 >)$.

(2) Because $k_{B^{'}}^{-1} \notin \mathcal{K}_I$, it can be concluded from the Lemma 1 that the sub-term $\{k_{TC-B^{'}} N_a\}_{k_B^{-1}}$ originates from the regular node in C; it can be found from the Corollary 3(3) that $A^{'} \in \mathcal{T}_{name}$, $k_{TC-A^{'}} \in \mathcal{K}$ makes $s_{resp}^{'} \in resp[A^{'}, B^{'}, *, *, N_a, k_{TC-A^{'}}, k_{TC-B^{'}}]$, obtaining injection relation between N_a and k_{TC-B} for responder and because the random value N_a has the freshness, then $s_{resp}^{'} = s_{resp}$, then $A^{'} = A$, $B^{'} = B$, $k_{TC-A^{'}} = k_{TC-A}$, $k_{TC-B^{'}} = k_{TC-B}$.

To sum up, the uniqueness and freshness of random value N_a originated from C, so there is unique $s_{init} \in init[A, B, *, *, N_a, k_{TC-A}, k_{TC-B}]$. Since $< s_{init}, 3 > \in C$, then $C - height(s_{init}) = 3$. Thus the proposition conclusion is proved.

The SHKE protocol can meet the agreement among different nodes for mutual authentication according to the Definition 16 based on the conclusions of Proposition 3 and Proposition 4.

VI. Protocol Analysis Method

The analysis steps of the secrecy and authentication of the Ad-hoc security routing protocol can be provided by summarizing the formal analysis methods and thinking for SHKE protocol.

A. Secrecy Analysis

The secrecy analysis steps of the Ad-hoc security routing protocol are as follows by applying the ideal and honesty theory:

(1) Determine the message set S that needs to be secretive in the operation process of the protocol.

(2) Determine the key set K possibly known by penetrators. $K = \mathcal{K} \setminus S$ is the key set in $\mathcal{K}$ except the keys which cannot be obtained by the penetrator.

(3) Construct ideal $I_K[S]$. $I_K[S]$ is the message set possibly constructed by the penetrator in S.

(4) Prove that $I_K[S]$ is honest with the honesty theory. If $I_K[S]$ is honest, it shows that the message in S cannot be constructed by the penetrator, thus proving that the protocol meets the secrecy.

B. Authentication Analysis

The authentication analysis steps of the Ad-hoc security routing protocol are as follows by applying the ideal and honesty theory:

(1) Determine the set M_{Auth} of the authenticated terms, prove $I_{K_I}[M_I] \bigcap M_{Auth} = \phi$, namely the entry point of M_{Auth} is not the penetrator node;

(2) Analyze the structure form of $h \in M_{Auth}$ and determine the original strand of h;

(3) Determine the parameters of the strand where h is and the message term $t \subset h$ that originate from h according to the parameters of h;

(4) Provide the proposition assumptions of the regular strand s_B of the principal B in aspects of parameters, uniqueness and height according to the regular strand s_A of the protocol principal A;

(5) Make corollaries of the proposition conclusions according to the unique origin of g based on the message term $h \subset I_K[g]$; if the proposition conclusion is true, then the protocol satisfies the authentication of A to B;

(6) If the protocol meets the authentication of A to B and the authentication of B to A, then it satisfies the authentication agreement, namely the protocol satisfies the authentication.

VII. Conclusions

When analyzing the authentication of SHKE protocol, because the message components $\{\{k_{TC-B}N_a\}_{k_B^{-1}}\}_{k_A}$ and $\{\{k_{TC-A}N_a\}_{k_A^{-1}}\}_{k_B}$ are generated by double encryption of private key and public key, since only the private key $k_A^{-1}, k_B^{-1} \notin \mathcal{K}_I$ and the protocol principal have one-to-one mapping, so the encrypted component generated by the private key can be used for the authentication of its corresponding principal. The knowability of $\{k_{TC-B}N_a\}_{k_B^{-1}}$ and $\{k_{TC-A}N_a\}_{k_A^{-1}}$ to the principal is the basis of the consistency analysis of strand parameters for the protocol principal. Due to the lack of formal research on the structure of message components, the original strand space model theory can not give formal analysis of knowability of $\{\{k_{TC-B}N_a\}_{k_B^{-1}}\}_{k_A}$ and $\{\{k_{TC-A}N_a\}_{k_A^{-1}}\}_{k_B}$ to principals, which results in lack of rigor in protocol analysis process, which may affect the accuracy of protocol analysis results. The practice of SHKE protocol analysis shows that the formalization of message component structure and the theoretical nature of the visibility for message components lay the theoretical foundation for formal analysis of message components, and effectively solve the formalization phenomenon of knowability analysis for message term.

On the basis of SHKE analysis, the formal analysis method and steps of the mobile Ad-hoc routing protocol summarized in this paper shows that honest and ideal theory can not only give a precise definition of mobile Ad-hoc routing protocol security properties, but also strictly define the scope of the attack ability, simplify the analysis process of protocol, and reduce the complexity of protocol analysis. The formal analysis results of SHKE protocol with the ideal and honesty theory verify correctness of the design for SGSR protocol again.

References

[1] A. Alcaide, E. Palomar, J. M. Fuentes, and L.G.Manzano, "Privacy – aware average speed monitoring system for vehicular ad-hoc, networks", *Intelligent Transport Systems Iet*, vol.9, no.3, pp.293-305, 2014.

[2] M. N. Moghadam, H. Taheri, and M. Karrari, "Multi-class multipath routing protocol for low power wireless networks with heuristic optimal load distribution", *Wireless Personal Communications*, vol. 82, no.2, pp.861-881, 2015.

[3] R. Doss, S. Sundaresan, and W. Zhou. "A practical quadratic residues based scheme for authentication and privacy in mobile rfid systems", *Ad Hoc Networks*, vol.11, no.1, pp.383-396, 2013.

[4] Y. L. Wang and J. Z. Wang, "The Security Analysis for Ad Hoc Routing Protocols Based on Improved Strand Space", *International Symposium on Pervasive Computing and Applications* , vol.8, pp.585-588, Urumchi, China, August 2006.

[5] J. Liu, F. U. Fei, and J. M. Xiao, "Security analysis of secure routing protocols for ad hoc networks based on improved meadows model", *Journal of Applied Sciences*, vol.2008, no.3, pp.250-256, 2008.

[6] F. J. Thayer, J. C. Herzog, and J. D. Guttman, "Strand spaces: why is a security protocol correct? " ,*Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No.98CB36186)*, Oakland,CA, pp. 160-171, 1998.

[7] F. J. Thayer, J. C. Herzog, and J. D. Guttman, " Strand spaces: proving security protocols correct", *IOS Press*, vol.7, no.2-3, pp.191-230, 1999.

[8] D. Dolev and A. Yao, "On the security of public key protocols", I*nformation Theory IEEE Transactions on*, vol.29, no.2, pp.198-208,

1983.
[9] F. J. Thayer, J. C. Herzog, and J. D. Guttman, “Honest ideals on strand spaces”, *Proceedings. 11th IEEE Computer Security Foundations Workshop (Cat. No.98TB100238)*, Rockport, MA, pp. 66-77, 1998.
[10] V. Sureshkumar, A. Ramalingam, and S. Anandhi, “Analysis of Accountability Property in Payment Systems Using Strand Space Model”, *International Symposium on Security in Computing and Communication* , Springer, Cham, Vol.536, pp.424-437 .
[11] L.F. Xu, S. R. Xia, J. Chen, F. U. Cai, and J. Chen, “A secure routing protocol sgsr for mobile ad hoc networks”, *Computer Engineering & Science*, vol.29, no.4, 22-25, 2007.

Lei Yu was born on Jul. 20, 1978**.** He received the MS an BS degree in computer science and technology from Huaibei Normal University of China. Currently, he is an assistant professor and MS supervisor in the school of computer science and technology, Huaibei Normal University, China. His major research interests include cryptography and information security. He has published many papers in related journals.

Yuyan Guo was born on Apr. 24, 1984**.** She received the PhD degree in cryptography from Hohai University of China. Currently, She is a MS supervisor in the school of computer science and technology, Huaibei Normal University, China. Her research interests include cryptography and information security.

Mingming Jiang was born on May 7, 1984**.** He received the PhD degree in cryptography from Xidian University of China. Currently, he is a MS supervisor in the school of computer science and technology, Huaibei Normal University, China. His research focuses on the areas of security and cryptography.