Security Analysis of TBPKI-2 Protocol Based on Minimal Element Theory

Wen-Bei Zong[1] and Lei Yu[1,2,3]
(Corresponding author: Lei Yu)

School of Computer Science and Technology, Huaibei Normal Universtiy[1]
School of Information and Contral Engineering, China University of Mining and Technology[2]
Anhui Big-Data Research Center on University Management[3]
Huaibei, Anhui 235000, China
Email: yulei@chnu.edu.cn

(Received May 23, 2022; Revised and Accepted Oct. 11, 2022; First Online Oct. 15, 2022)

Abstract

The strand space model is a hybrid proof method combining theorem proof and protocol trace. It can not only analyze the correctness of security protocol but also be used to construct an attack model and reveal the internal defects of security protocol. Compared with other branches of the theory, the minimal element theory has more detailed and adequate advantages in the process of protocol analysis. For example, the TBPKI-2 protocol is a wireless network authentication protocol. It is optimized based on the PKI mechanism and has specific practical significance. Therefore, based on strand space theory, this paper analyzes the confidentiality and consistency of the protocol by using minimal element theory, accurately finds that the potential hidden danger in the protocol and its root cause is unable to block Man-in-the-Middle Attack, and proposes corresponding improvement suggestions according to the hidden danger and its root cause.

Keywords: Security Analysis; Security Protocol; Strand Space; TBPKI-2 Protocol

1 Introduction

Security protocol is a cryptography-based protocol that provides a variety of security services. With the rapid development of networking and information technology, some widely used protocols have gradually revealed their shortcomings. Therefore, it is necessary to analyze their security before improving or designing new security protocols. At present, there are mainly two analysis methods: non-formal and formal. Among the many formal analysis methods [8,11,17], in 1977, Fabrega, Herzog and Guttman established the strand space model theory [10], which is widely respected for its efficiency and rigor, simplicity and intuitiveness, and scalability, pushing the formal analysis technique of security protocol to a new level.

In recent years, it has been widely used in the analysis of security protocols [5, 7, 12, 16]. Strand space is a method combining theorem proof and protocol tracking. It can not only prove the correctness of security protocols, but also construct attacks and reveal the inherent defects of security protocols. With continuous research, strand space theory has been improving and expanding [9, 13]. Since the establishment of strand space model, there are three theoretical branches, namely, ideal and honesty, minimal element and authentication tests. Compared with other theoretical branches, the minimal element theory is more detailed and sufficient in the process of protocol analysis [15]. With the development of science and technology, the security of key agreement protocol in wireless communication [2, 4] has been attracting extensive attention. Therefore, in order to ensure the security of the protocol, we must analyze its security before using it. TBPKI-2 protocol [1] is a wireless network authentication protocol based on CVT. CVT is the validity credential of the entity's public key certificate. And the certificate ID of the entity, the validity term of the CVT and the public key of the entity can be decrypted from it. The content of the protocol is that A confirms its identity by showing CVT to B and completes the key negotiation between A and B.

Based on the minimal element theory in strand space, this paper will make a formal analysis of TBPKI-2 protocol from two aspects of confidentiality and consistency, point out the internal defects of the protocol and put forward some suggestions for improvement.

2 Strand Space Model Theory

2.1 Basic Concepts

Strand space is a two-tuple (Σ, tr), where Σ represents a set of strands. And strands among Σ can be used to represent any sequence, tr represents a mapping of the sequence composed of elements from Σ to A. Some basic concepts in strand space are given below (the basic concepts and theorems of minimal element theory can be found in [3, 10]):

1) Node n is a two-tuple $< s, i >$, where s is an element in Σ and i represents the sequence number of the node on this strand. Each node belongs to a unique strand. Node set is marked as N.

2) If $n =< s, i >$, the participant action represented by this node is represented as $(tr(s))_i = R_a$, where R_+ or $_-$, and a represents a message, then the node means that the participant sends or receives a.

3) If $n_1, n_2 \in N$, definition $n_1 \rightarrow n_2$ means $n_1 = +a, n_2 = -a$, which indicates that the message is sent from n_1 to n_2.

4) If $n_1, n_2 \in N$, definition $n_1 \Rightarrow n_2$ means that n_1 and n_2 are on the same strand and n_2 is the next node of n_1.

5) An unsigned term t appears in $n \in N$ if and only if $t \sqsubset term(n)$.

6) Let I as an unsigned term set. Node $n \in N$ is the entry point of I if and only if $term(n) = +t$, where $t \in I$, and for all nodes $n^{'} \Rightarrow^{+} n$, there is $term(n) \notin I$.

7) The unsigned term t originates from node $n \in N$ if and only if n is the entry point of the set $I = \{t^{'} : t \sqsubset t^{'}\}$.

8) The unsigned term t is uniquely originated if and only if t originates from the unique node $n \in N$.

Lemma 1. *Let C be a bundle, then $\preceq_c$ is a partial order relation with self-reflexivity, antisymmetry and transitivity. Any nonempty subset of bundle C has minimal elements under the partial order relation $\preceq_c$.*

Lemma 2. *Let C be a bundle and $S \subseteq C$ as a set of nodes satisfies the following property: $\forall m, m^{'}, unsterm(m) = unsterm(m^{'})$. Then $m \in S$ if and only if $m^{'} \in S$.*

If n is a $\preceq_{c-}$ minimal element of S, the sign of n is positive.

2.2 Penetrator Capability Description

In strand space theory, the penetrator's abilities are described by two parts: one is the key set initially mastered by the penetrator, and the other is the new information generated by the message that penetrator has intercepted. The atomic behavior of the penetrator is described by the penetrator trace, which is defined below:

1) M message: $< +t >$, where $t \in T$.

2) K key: $< +K >$, where $K \in K_p$.

3) C connect: $< -g, -h, +gh >$.

4) S separation: $< -gh, +g, +h >$.

5) E encryption: $< -K, -h, +\{h\}_K >$.

6) D decryption: $< -K^{-1}, -\{h\}_K, +h >$.

Definition 1. *Infiltrated strand space is a two-tuple (Σ, tr), where Σ is a strand space and $P \subseteq \Sigma$ satisfies the following condition: for all $p \subseteq P$, $tr(p)$ is a penetrator strand.*

Strands in P are called penetrator strands. Thus, if $s \in P$, strand $s \in \Sigma$ is a penetrator strand. And if strand is a penetrator strand, node n is called penetrator node. In addition, all strands and nodes are called regular strands and regular nodes.

Proposition 1. *Let C be a bundle and $K \in K \setminus K_p$.*

If K does not originate from a regular node, $K \not\sqsubset term(n)$ holds for any node $n \in C$. Specially, for any penetrator node $p \in C$, there is $K \not\sqsubset term(p)$.

3 Symbols and Assumptions

3.1 Symbols

The symbols used in this paper and their semantics are shown in Table 1.

3.2 Assumptions

The following assumptions are consistent with the actual situation.

1) Legitimate subjects in the network can also launch attacks;

2) The random number N_a is chosen irrelevantly to N_b. It can be proved that they are almost impossible to be equal in the probability model.

4 Strand Space Model and Analysis of TBPKI-2 Protocol

Further concretizing the term algebra:

1) Identifier set: $T_{name} \subseteq T$.Generally, A, B ... is used to represent identifier of the subject;

2) Mapping: $T_{name} \rightarrow K$. This mapping binds the subject to its public key.

The protocol is as follows:

1) $A \rightarrow B : CVT_A, N_a, K_i, Sign_a$.
$Sign_a = \{CVT_A, N_a, K_i\}_{K_a^{-1}}$, indicates the signature of subject A for this message;

2) $B \rightarrow A : CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r, Sign_b$.
$Sign_b = \{CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r\}_{K_b^{-1}}$, indicates the signature of subject B for this message;

3) $A \rightarrow B : \{N_b - 1\}_{K_{ab}}$.

Table 1: The semantics of symbols in the paper

Symbols	Semantics of symbols
A	Initiator of the protocol.
B	Responder of the protocol.
P	Penetrator of the protocol.
K_a, K_b, K_p	Public key of subject A, subject B and subject P.
K_a^{-1}, K_b^{-1}	Private key of subject A, subject B and subject P.
N_a, N_b	Random number generated by subject A and subject B.
CVT_a, CVT_b	Validity certificate of public key certificates of subject A and subject B.
$TCVP$	Trusted and valid third party.
(g, n)	The public number of D-H algorithm [6], and g is the primitive element of module n.
K_i, K_r	The partial key generated by subject A and subject B (g^x, g^y).
K_{ab}	Session keys for subjects A and B (g^{xy}).
C	Bundle.
Σ	Strand space.
$a \sqsubset b$	Term a is a subterm of term b.
s	Strand.
$Sign_a, Sign_b$	Signatures made with private keys K_a^{-1} and K_b^{-1} of subject A and subject B.

4.1 Strand Space of TBPKI-2

Definition 2. *Let (Σ, P) be an infiltrated strand space. If Σ is composed of the following three strands, it is called a TBPKI-2 strand space.*

1) Penetrator strand $s \in P$;

2) Initiator strand $s \in Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$. Its trace is $< +CVT_A N_a K_i Sign_a, -CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b, +\{N_b - 1\}_{K_{ab}} >$. Here A, $B \in T_{name}$, N_a, $N_b \in T$ and $N_a \notin T_{name}$. $Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$ represents the set of all strands having above trace, and the subject corresponding to this strand is A;

3) Responder strand $s \in Resp[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$ is corresponding to the initiator strand. Its trace is $< -CVT_A N_a K_i Sign_a, +CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b, -\{N_b - 1\}_{K_{ab}} >$. Here $A, B \in T_{name}$, $N_a, N_b \in T$ and $N_b \notin T_{name}$. $Resp[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$ represents the set of all strands having above trace, and the subject corresponding to this strand is B.

If $s \in Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$ is a regular strand, A is called the initiator of s. And if $s \in Resp[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$ is a regular strand, B is called the responder of s. N_a, N_b are called the corresponding initiator and responder values.

4.2 Responder Analysis for TBPKI-2 Protocol

4.2.1 Consistency Analysis of Responder

Proposition 2. *Assuming the following conditions are valid:*

1) *Σ is a TBPKI-2 space, C is a bundle of Σ, s is a responder strand. And $s \in Resp[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$, with $C - hight(s) = 3$;*

2) *$K_b \notin K_p$;*

3) *$N_a \neq N_b$, and N_b is the only origin in Σ.*

Therefore, C contains an initiator strand $t \in Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$, with $C - hight(t) = 3$.

Arbitrarily Select $\Sigma, C, s, A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r$ that satisfies the assumptions in Proposition 2. Node $< s, 2 >$ outputs the value $CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b$. It is marked as n_0, and its term is marked as v_0. Node $< s, 3 >$ receives the value $\{N_{b-1}\}_{K_{ab}}$. It is marked as n_3 and its term is marked as v_3. In the proof process, other two nodes n_1 and n_2 are used, which satisfy $n_0 \prec n_1 \prec n_2 \prec n_3$.

Lemma 3. *N_b originates from n_0.*

Proof. By Proposition 1, $N_b \sqsubset v_0$, and the sign of n_0 is positive. Therefore, it only need to prove $N_b \not\sqsubset n'$, where n' is the precursor node $< s, 1 >$ on the same strand as n_0. By Proposition 2, $N_a \neq N_b$ can be proved, so $term(n') = \{CVT_A, N_a, K_i, Sign_a\}$. Finally, it need to verify $N_b \neq A$. By Definition 1, $N_b \notin T_{name}$, so $N_b \neq A$. Thus, $N_b \not\sqsubset n'$. □

Lemma 4. *Set $S = \{n \in C : N_b \sqsubset term(n) \bigwedge v_0 \not\sqsubset term(n)\}$ has a minimal element $\preceq_{n2}$, n_2 is a regular node and its sign is positive.The initiator strand contains nodes n_1 and n_2, and the responder strand contains nodes n_0 and n_3. Node n_2 contains N_b.*

Proof. Because $n_3 \in C$ and n_3 contains N_b but not v_0, $n_3 \in S$. Therefore, it is a nonempty set. By Lemma 1, there is at least one minimal element $\preceq_{-n2}$. By Lemma 2, the sign of n_2 is positive.

According to the trace of penetrator strand P, it is proved that n_2 cannot be on penetrator strand P.

- M**:** Trace $tr(p)$ has form $< +t >$, where $t \in T$. Thus, $t = N_b$. At this time, N_b originates from this strand, but this is obviously impossible. By lemma 3, N_b originates from a regular node n_0, and according to Assumption 3 of Proposition 2, N_b is the only origin in Σ. Therefore, N_b is not generated on the strand M;

- C**:** Trace $tr(p)$ has form $< -g, -h, +gh >$. It is obvious that the regular node is not the minimal element of set S. Therefore, N_b is not generated on strand C;

- K**:** Trace $tr(p)$ has form $< +K_0 >$, where $K_0 \in K_p$. But $N_b \not\sqsubset K_0$. Therefore, N_b is not generated on strand K;

- E**:** Trace $tr(p)$ has form $< -K_0, -h, +\{h\}_{K_0} >$, assuming $N_b \sqsubset \{h\}_{K_0} \bigwedge v_0 \not\sqsubset \{h\}_{K_0}$. Because $N_b \neq \{h\}_{K_0}$, there is $N_b \sqsubset h$. However, $v_0 \not\sqsubset h$, so this positive node cannot be the minimal element of set S. Therefore, N_b is not generated on strand E;

- D**:** Trace $tr(p)$ has form $< -K_0^{-1}, -\{h\}_{K_0}, +h >$. If this positive node is the minimal element of set S, then there must exist $v_0 \not\sqsubset h$ and $v_0 \sqsubset \{h\}_{K_0}$. Therefore, according to the free encryption assumption, there must be $h = \{CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b\}$ and $K_0 = K_b^{-1}$. So there exists a node m (the first node on this strand) with $term(m) = K_b$. Because Proposition 1 assumes $K_b \notin K_p$, it is deduced that K_b originates from a regular node. But there is no initiator strand or responder strand originated from K_b. Therefore, N_b is not generated on strand D;

- S**:** Trace $tr(p)$ has form $< -gh, +g, +h >$, assuming $term(n_2) = g$, which can be proved similarly when $term(n_2) = h$. $N_b \sqsubset g$ and $v_0 \not\sqsubset g$ due to $n_2 \in S$. From the minimality of n_2, there is $v_0 \sqsubset gh$. But $v_0 \neq gh$, so $v_0 \sqsubset h$.

Let $T = \{m \in C : m \prec n_2 \bigwedge gh \sqsubset term(m)\}$, each element in T is a penetrator node. Because regular node does not contain the subterm gh, and $< p, 1 > \in T$, T is a nonempty set. By Lemma 1,2, T contains a minimal element m, and its sign is positive. The following proof that m is impossible on penetrator strand S.

Firstly, the minimal element in T cannot appear on the strand of type M and K.

- S**:** If $gh \sqsubset term(m)$, m is a regular node that lies on a S-type penetrator strand p'. There is $gh \sqsubset term(< p', 1 >)$. And $< p', 1 > \prec m$ contradicts the minimality of m in T.

- E**:** If $gh \sqsubset term(m)$, m is a regular node that lies on a E-type penetrator strand p'. There is $gh \sqsubset term(< p', 2 >)$. And $< p', 2 > \prec m$ contradicts the minimality of m in T.

- D**:** If $gh \sqsubset term(m)$, m is a regular node that lies on a D-type penetrator strand p'. There is $gh \sqsubset term(< p', 2 >)$. And $< p', 1 > \prec m$ contradicts the minimality of m in T.

- C**:** If $gh \sqsubset term(m)$, m is a regular node that lies on a C-type penetrator strand p', and m is the minimal element of T. Therefore, $gh = term(m)$, and the trace of p' has form $< -g, -h, +gh >$. So $term(< p', 1 >) = term(n_2)$. And $< p', 1 > \prec n_2$ contradicts the minimality of n_2 in S.

As mentioned above, n_2 cannot be on a penetrator strand, it must be on a regular strand. □

Definition 3. *Minimal element $\preceq n_2$ in the fixed set $S = \{n \in C : N_b \sqsubset term(n) \bigwedge v_o \not\sqsubset term(n)\}$. At this time, node n_2 is a regular node and its sign is positive.*

Lemma 5. *There exist a precursor node n_1 of node n_2 on strand t, and $term(n_1) = \{CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r, Sign_b\}$. The lemma content is shown in Figure 1.*

Proof. By Lemma 3, N_b originates from n_0. According to Condition 3 of Proposition 2, N_b is the only origin in Σ. Because $v_0 \sqsubset term(n_0) \bigwedge v_0 \not\sqsubset term(n_2)$, $n_2 \neq n_0$. Thus, N_b does not originate from n_2. Because there is a precursor node n_1 of n_2 on strand t, $N_b \sqsubset term(n_1)$. From the minimality of n_2, it follows that $v_0 = \{CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r, Sign_b\} \sqsubset term(n_1)$. From Assumptions 2 of Proposition 2, $K_b \notin K_p$, so $term(n_1) = \{CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r, Sign_b\}$. □

Lemma 6. *The regular strand t containing n_1 and n_2 is an initiator strand of bundle C.*

Proof. Node n_2 is a regular node with positive sign and its precursor node n_1 has form $\{CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b\}$. If t is a responder strand, it only be a node with negative symbol after n_1, so t is an initiator strand. Therefore, n_1

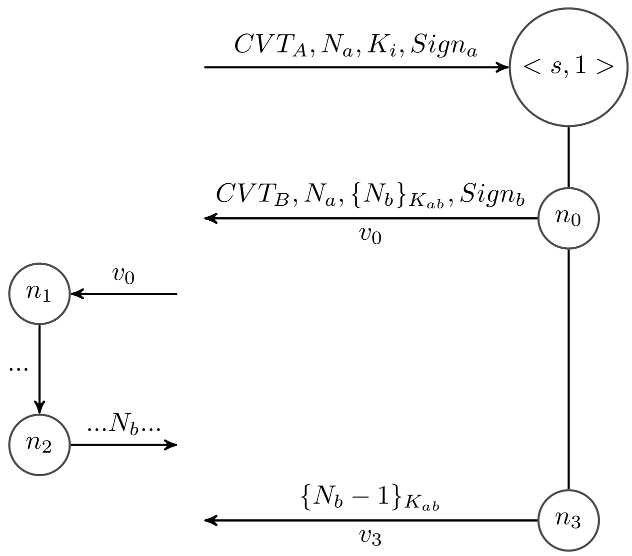

Figure 1: Node n_1 contains v_0

and n_2 are the 2nd and 3rd nodes on the strand respectively. The last node in t is contained in the bundle, so $C - hight(t) = 3$. □

Proposition 3. *Set Σ is a TBPKI-2 space, and N_a is the only origin in Σ. Therefore, for any A, B and N_b, there exist one such strand $t \in Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$ at most.*

Proof. For any A, B, N_a, if $t \in Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$, the sign of $< t, 1 >$ is positive, $N_a \sqsubset term(< t, 1 >)$ and N_a cannot appear earlier on t. Therefore, N_a originates from node $< t, 1 >$. Thus, if N_a is the only origin in Σ, there exist one such t at most. □

4.2.2 Confidentiality Analysis of Responder

Proposition 4. *Assuming the following conditions are valid:*

1) *Σ is a TBPKI-2 space, C is a bundle of Σ, s is a responder strand. And $s \in Resp[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$, with $C - hight(s) = 3$;*

2) *$K_a \notin K_p$, and $K_b \notin K_p$;*

3) *$N_a \neq N_b$, and N_b is the only origin in Σ.*

Therefore, for any node $m \in C$ satisfying $N_b \sqsubset term(n)$, $\{CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b\} \sqsubset term(m)$ is established or $\{N_b - 1\}_{K_{ab}} \sqsubset term(m)$ is established. Specially, $N_b \neq term(m)$.

Arbitrarily select Σ, C, s, A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r that satisfies the assumptions in Proposition 2. Node $< s, 2 >$ outputs the value $CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b$. It is marked as n_0, and its term is marked as v_0. Node $< s, 3 >$ receives the value $\{N_b - 1\}_{K_{ab}}$. It is marked as n_3, and its term is marked as v_3. Consider the following set: $S = \{n \in C : N_b \sqsubset term(n) \bigwedge v_0 \not\sqsubset term(n) \bigwedge v_3 \not\sqsubset term(n)$.

Lemma 7. *The minimal element of S is not a regular node.*

Proof. Inversely assumed that there exist a minimal element that is a regular node $m \in S$. According to Lemma 2, the sign of m is positive.

1) Only the sign of n_0 is positive and $v_0 \sqsubset term(n_0)$, so m cannot be on the strand s;

2) Assume that is located on the responder strand $s^{'} \neq s$. Then, $m =< s^{'}, 2 >$, $term(n) = \{CVT, N, \{N^{'}\}_{K_d}, K, Sign_e\}$. Because $N_b \sqsubset term(m)$, $N_b = N$ or $N_b = N^{'}$.

   a. If $N_b = N$, because the term of $< s^{'}, 1 >$ is $\{CVT, N, K, Sign_c\} = \{CVT, N_b, K, Sign_c\}$, $N_b \sqsubset term(< s^{'}, 1 >)$. And $v_0 \not\sqsubset \{CVT, N_b, K, Sign_c\}$, $v_3 \not\sqsubset \{CVT, N_b, K, Sign_c\}$, so $< s^{'}, 1 > \in S$. However, $< s^{'}, 1 > \prec m$ contradicts the minimality of m;

   b. If $N_b \neq N$ and $N_b = N^{'}$, so N_b originates from m. It contradicts that n_0 is the only origin of N_b.

So m cannot be on responder strand $s^{'} \neq s$.

1) Assuming it is located on the initiator strand $s^{'} \neq s$. Then m may be located at the 1st node or the 3rd node of $s^{'}$.

   a. If $m =< s^{'}, 1 >$, because $N_b \sqsubset term(m)$, N_b originates from m. It contradicts that n_0 is the only origin of N_b;

   b. If $m =< s^{'}, 3 >$, $term(m) = \{N_b - 1\}_{K_{ab}}$, the second node $< s^{'}, 2 >$ has the form $\{CVT, N, \{N_b\}_{K_d}, K, Sign_e\}$. It contradicts the minimality of m.

So m cannot be on initiator strand $s^{'} \neq s$. □

Lemma 8. *The minimal element of S is not a penetrator node.*

Proof. The proof process is similar to Lemma 4. □

4.3 Initiator Analysis for TBPKI-2 Protocol

4.3.1 Confidentiality Analysis of Initiator

Proposition 5. *Assuming the following conditions are valid:*

1) *Σ is a TBPKI-2 space, C is a bundle of Σ, s is a Initiator strand. And $s \in Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$, with $C - hight(s) = 3$;*

2) *$K_a \notin K_p$, and $K_b \notin K_p$;*

3) *$N_a \neq N_b$, and N_a is the only origin in Σ; $K_i \neq K_r$, and K_i is the only origin in Σ.*

Therefore, for any node $m \in C$ satisfying $N_b \sqsubset term(n)$, $\{CVT_A N_a K_i Sign_a\} \sqsubset term(m)$ is established or $\{CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b\} \sqsubset term(m)$ is established. Specially, $N_a \neq term(m)$.

The proof process is same as 4.2.2. It can obtain the confidentiality of N_a.

4.3.2 Consistency Analysis of Initiator

Proposition 6. *Assuming the following conditions are valid:*

1) *Σ is a TBPKI-2 space, C is a bundle of Σ, s is a responder strand. And $s \in Init[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$, with $C - hight(s) = 3$;*

2) *$K_a \notin K_p$, and $K_{ab} \notin K_p$;*

3) *$N_a \neq N_b$, and N_a is the only origin in Σ.*

Therefore, C contains a responder strand $t \in Resp[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$, with $C - hight(t) = 2$.

Proof. Here is a brief proof. Considering the set $\{m \in C : \{CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r, Sign_b\} \sqsubset term(m)\}$ contains node $< s, 2 >$, so it is nonempty. And it has a minimal element m_0. If m_0 is on a regular strand t, then $t \in Resp[A, B, N_a, N_b, CVT_A, CVT_B, K_i, K_r]$. And t at least has two nodes in C.

If m_0 lies on a penetrator strand t, it can be proved that t is a penetrator strand of type E and its trace is $\{-K_b^{-1}, -CVT_B N_a \{N_b\}_{K_{ab}} K_r, +CVT_B N_a \{N_b\}_{K_{ab}} K_r Sign_b\}$. However, this contradicts Proposition 5, so N_a cannot appear on a node like $< t, 2 >$.

The conclusion on uniqueness corresponding to Proposition 3 can be proved similarly. □

4.4 Other Confidentiality Analysis of TBPKI-2 Protocol

The information that TBPKI-2 protocol needs to keep confidential also includes K_i and K_r. Because the first step $A \to B : CVT_A, N_a, K_i, Sign_a$ and the second step $B \to A : CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r, Sign_b$ in the protocol sending process, K_i and K_r are not encrypted. Therefore, penetrator P can obtain $K_i(g^x)$ and $K_r(g^y)$. The x, y contained in them are secret data. So penetrator P can deduce the secret data x, y and send the secret data through the strand S. Therefore, K_i and K_r cannot guarantee the confidentiality.

5 Improvement

For the improvement of TBPKI-2 protocol, the information sent between A and B is encrypted after private key signature. As follows:

1) $A \to B : \{CVT_A, N_a, K_i, Sign_a\}_{K_b}$.
   $Sign_a = \{CVT_A, N_a, K_i\}_{K_a^{-1}}$, indicates the signature of subject A for this message;

2) $B \to A : \{CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r, Sign_b\}_{K_a}$.
   $Sign_b = \{CVT_B, N_a, \{N_b\}_{K_{ab}}, K_r\}_{K_b^{-1}}$, indicates the signature of subject B for this message;

3) $A \to B : \{N_b - 1\}_{K_{ab}}$.

Because the private key of subject is unbreakable, the improved protocol can prevent Man-in-the-Middle Attack [14]. Therefore it can solve the hidden danger of possibly obtaining confidential information in 4.4 confidentiality analysis. After the improvement, the security of the protocol is guaranteed and the purpose of the protocol can be achieved. That is, secret key negotiation is performed while the identity of the communication subject is verified.

6 Comparison with Other Method

BAN logic pioneered the formal analysis of security protocols and has been widely appreciated for its simplicity and practicality. However, BAN logic can only analyze the authentication nature of the protocol to find its flaws, but cannot analyze the confidentiality nature of the protocol to ensure the security of the protocol. Compared with this method, strand space theory has the following advantages:

1) In the strand space model, the meaning of security protocol correctness includes both consistency and confidentiality. So the analysis scope of BAN logic is expanded;

2) The strand space model accurately describes the possible behaviors of penetrators in the system;

3) The strand space model is simpler to prove the correctness of security protocols and can more accurately confirm the assumptions made.

7 Conclusion

TBPKI-2 protocol can effectively prevent replay attacks, malicious tampering of information and other common attacks by ensuring the freshness of the temporary value and the unsolvability of the subject's private key. And it also can realize the purpose of confirming the source of information. However, it has the drawback of being intercepted by the penetrator and cracking the session key, so it cannot effectively achieve the purpose of key negotiation. Therefore, the TBPKI-2 protocol needs to be further improved. Because the private key of the subject is not cracked, it can be encrypted by public key before sent. It can prevent Man-in-the-Middle Attack during message transmission, and securing the security of the protocol.

Acknowledgments

This study was supported by the Natural Science Foundation of Anhui University (KJ2020A0034), the crosswise project entrusted by Anhui Yunxinfu Information Technology Co., Ltd. to Huaibei Normal University in 2021 (Construction of Information security technology guarantee system of information management platform). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] Z. Chen, W. Liao, S. Shen, and H. Wang, "Wireless network authentication protocol based on PKI mechanism optimization," *Computer Engineering and Design*, vol. 33, no. 9, pp. 3297–3300, 2012.

[2] S. Chiou, H. Pan, E. F. Cahyadi, and M. Hwang, "Cryptanalysis of the mutual authentication and key agreement protocol with smart cards for wireless communications," *International Journal of Network Security*, vol. 21, no. 1, pp. 100–104, 2019.

[3] R. Focardi and F. L. Luccio, "Secure key management policies in strand spaces," in *Protocols, Strands, and Logic - Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday*, Lecture Notes in Computer Science, D. Dougherty, J. Meseguer, S. A. Mödersheim, and P. D. Rowe, Eds., vol. 13066. Springer, pp. 175–197, 2021.

[4] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless body area networks," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 1–8, 2019.

[5] S. Hagihara, M. Shimakawa, and N. Yonezaki, "Verification of verifiability of voting protocols by strand space analysis," in *Proceedings of the 8th International Conference on Software and Computer Applications, ICSCA'19*, pp. 363–368, 2019.

[6] L. Huang, T. Chang, and M. Hwang, "A conference key scheme based on the diffie-hellman key exchange," *International Journal of Network Security*, vol. 20, no. 6, pp. 1221–1226, 2018.

[7] J. Liu, Y. Lai, S. Yang, and L. Xu, "Bilateral authentication protocol for WSN and certification by strand space model," vol. 46, no. 9, pp. 169–175, 2019.

[8] Y. Liu, Q. Meng, X. Liu, J. Wang, L. Zhang, and C. Tang, "Formal method for security analysis of electronic payment protocols," *IEICE Transactions on Information Systems*, vol. 101-D, no. 9, pp. 2291–2297, 2018.

[9] S. Pinsky, "Joshua guttman: Pioneering strand spaces," in *Protocols, Strands, and Logic - Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday*, Lecture Notes in Computer Science, D. Dougherty, J. Meseguer, S. A. Mödersheim, and P. D. Rowe, Eds., vol. 13066. Springer, pp. 348–354, 2021.

[10] F. Journal of Thayer, J. C. Herzog, and J. D. Guttman, "Strand spaces: Why is a security protocol correct?" in *IEEE Symposium on Security and Privacy*, pp. 160–171, 1998.

[11] J. Yan, S. Ishibashi, Y. Goto, and J. Cheng, "A study on fine-grained security properties of cryptographic protocols for formal analysis method with reasoning," in *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI 2018, Guangzhou, China, October 8-12, 2018*, G. Wang, Q. Han, M. Z. A. Bhuiyan, X. Ma, F. Loulergue, P. Li, M. Roveri, and L. Chen, Eds. IEEE, pp. 210–215, 2018.

[12] F. Yang, S. Escobar, C. A. Meadows, and J. Meseguer, "Strand spaces with choice via a process algebra semantics," *CoRR*, vol. abs/1904.09946, 2019. (http://arxiv.org/abs/1904.09946)

[13] M. Yao, J. Zhang, and X. Weng, "Research of formal analysis based on extended strand space theories," in *15th International Conference on Intelligent Computing Theories and Application (ICIC'19)*, Lecture Notes in Computer Science, vol. 11644, 2019.

[14] E. Ylli and J. Fejzaj, "Man in the middle: Attack and protection," in *Proceedings of the 4th International Conference on Recent Trends and Applications in Computer Science and Information Technology*, pp. 198–204. 2021.

[15] L. Yu, Y. Guo, and M. Jiang, "Improvement of strand space theory for application of minimal element method," *Quarterly Journal of Indian Pulp and Paper Technical Association*, vol. 30, no. 1, pp. 94–105, 2018.

[16] L. Yu, Y. Y. Guo, Z. P. Zhuo, and S. M. Wei, "Analysis and improvement of otway-rees based on enhanced authentication tests," *International Journal of Network Security*, vol. 23, no. 3, pp. 426–435, 2021.

[17] L. Yu, Z. Y. Yang, and Z. P. Zhuo, "Extension of pcl theory and its application in improved ccitt x.509 analysis," *International Journal of Network Security*, vol. 23, no. 2, pp. 305–313, 2021.

Biography

Wen-bei Zong was born in 2000. She received the MS degree in software engineering from Huainan Normal University of China. Currently, She is a graduate student in the school of computer science and technology, Huaibei Normal University, China. Her research interests include cryptography and information security. (12111080780@chnu.edu.cn)

Lei Yu was born in 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.(yulei@chnu.edu.cn)