Analysis and Optimization of Delegation-based Sequenced Packet Exchange (SPX) Protocol: A Kailar Logic Approach

Ebrima Jaw[1]*, Wang Xue Ming[3]
College of Computer Science and Technology, Guizhou University (GZU), Guizhou, Guiyang, China[1, 3]
School of Information Technology and Communication University of The Gambia (UTG)[1]

Mbemba Hydara[2]
School of Information Technology and Communication University of The Gambia (UTG)
Greater Banjul, Serekunda, The Gambia

***Abstract*—Accountability within electronic commerce protocols has tremendous significance, especially those that require answerability for the actions taken by participants. In this study, the authors evaluate the delegation of accountability based on the Sequenced Packet Exchange (SPX) protocol. The study emphasizes the concept of provability as a benchmark to formalize accountability. Moreover, this paper proposed a new framework that enables principals to delegate individual rights to other principals and how the delegator's accountability is handed over or retained, which provides the crucial functionality of tracing how accountability is distributed among principals within a system. The study provides a novel solution to accountability challenges and analysis of protocols, such as introducing novel conditions for distributing essential credentials among the grantor and the grantee and analyzing delegation-based protocols. The approach adopted will help prevent potential compromises of the integrity of online transactions. By extension, it will also serve as a best practice solution for settling legal disputes among principals.**

***Keywords*—Delegator; accountability; grantor; Kailar logic; principal; client; delegate; grantee**

I. Introduction

The advent of cutting-edge technologies such as Big Data, Cloud Computing, the Internet of Things (IoT), and Web-Based Distributed applications has increased the need for electronic commerce transactions and other web-based services. Apart from revolutionizing the way business is conducted. Research has shown that companies that leverage these technologies gain massive profit margins compared to legacy systems [1].

Also, electronic commerce has progressively developed because of the rapid increase in businesses migrating to the web, which has opened up a new paradigm for computer scientists willing to dedicate their time and resources to the research, design, development, and optimization of protocols that provide security, authentication, authorization, verification, and confidentiality including accountability of internet-based commercial transactions [2], [3].

Lack of accountability among principals in any electronic transaction can introduce deception because of the prevalence of fraud and malicious activities on the internet. Consequently, this can make the electronic transaction process very unreliable. Therefore, proving accountability among principal actors deserves an equal degree of importance as offline transactions. For instance, in a data breach or privacy violation, a network administrator may delegate backup service of sensitive data to junior staff. Therefore, it will be essential for the parties to prove to a third party about their conduct for accountability purposes.

The design of efficient and error-free electronic transaction protocol has been a challenging task in computer science. Computer scientists often rely on formal analysis to detect, optimize flaws and redundancies in the design and production stages. However, most analysis methods before Kailar logic deal with various entities' beliefs and protocols. Therefore, this paper presents a formal analysis method using Kailar Logic [4]. The ability of principals to prove accountability in any electronic transactions is analyzed and evaluated, including how accountability is assured using existing protocols [5], [6].

There has been significant work on other protocols, but research on the analysis of delegation-based protocols is yet to be adequately explored. In this work, the author uses the Kailar Logic analysis method and techniques based on the Delegation-Based SPX protocol to prove accountability among participating principals. In this context, the primary objective of proving accountability and provability among participants within the protocol form the basis of the study [7].

A. Accountability

Accountability in scientific journals is "the state whereby a principal is associated with an action that can be proven to a third party," wherein the third party is different from the prover and the initiator [4]. Similarly, Accountability also means a particular subject can prove to a third party that it is responsible for initiating a specific action or object. However, in this paper, the focus of Accountability is on internet transactions. How relevant principals involved in the transaction keep track of the evidence of each party. For instance, the whole transaction process should be evident or transparent to all participants [7].

Since the goal of the Kailar framework (Kailar Logic) is to provide Accountability among participants of a given Internet transaction, thus ensuring non-repudiation of the parties, which is made possible with the help of transaction records or digital

*Corresponding Author

fingerprints. The whole concept hinges on tracking every transaction end-to-end during the process and, most importantly, the source or origin. The result can be used as evidence to resolve legal disputes among participants of any online Internet transaction. This paper uses Accountability based on the above definition [8].

B. Summary of Provability and Belief

A statement y is believed by an individual if he or she is convinced of it. However, suppose a participant can convince another participant about statement y. In that case, it means the participant can prove statement y, which is achieved through the collective conveyance of the validity of statement y to an audience through a set of statements referred to as proof of statement y. Similarly, the capability to produce the required set of statements that can convince an audience about statement y is the capability to prove statement y [9].

C. Asymmetric and Symmetric Encryption

The past decades have witnessed the use of Symmetric Encryption algorithms in many systems and protocols. The encryption scheme is where a single secret key is used to encrypt and decrypt a message possessed by all the participants involved in the communication. Co-relating this definition to the new concept of Believe and Provability, assuming we have two participants in an Internet transaction, namely A and B. If B receives a message encrypted with a key he possesses, which he did not send, he has believed that A sent it. However, he cannot prove this to a third party, making this approach unsuitable for this paper.

Nonetheless, with the growing vulnerabilities on the Internet, the need for a new approach in the form of Asymmetric Encryption is required. This encryption scheme involves two related keys, one public, and the other secret or private keys. The former (public) is used to encrypt the message while the latter decrypts the same message. Moreover, while the private key is kept secure by the participating entities, the public key is made available to everyone to encrypt the message they wish to send. This approach addresses the gap in the symmetric scheme because it does not rely on trust but instead keys belonging to participants themselves, therefore providing accountability. However, they are also susceptible to tampering. Consequently, this work considers using asymmetric encryption techniques for the entire analysis process of the proposed approach.

Based on existing literature, security researchers have made significant progress in protocol analysis. However, the degree of exploration into protocol analysis detailing characteristics of accountability is sparse. In this study, accountability analysis of delegation-based protocols is explored. This inspired the notion that delegation is about the standard technique of conveying accountabilities among principals. The main contributions of the paper are the following:

- Developed a new framework that enables principals to delegate individual rights to other principals and went further to show how the delegator's accountability is either handed over or retained.
- Provides a novel solution to accountability challenges and analysis of protocols.
- The result of the approach will help prevent potential compromise of the integrity of online transactions. It will also serve as solution for legal disputes settlement among principals.

The rest of the paper is organized as follows: Section 2 discusses the related work. Section 3 deals with Kailar Logic and its properties, and Section 4 summarizes the symbols and theories utilized in this work. Similarly, Section 5 discusses the proposed Delegation-Based SPX protocol, and finally, Section 6 concludes with a summary.

II. Related Work

Determining which protocol fulfills or lacks the necessary accountability for electronic commerce and other domains, the past decades have seen several researchers proposed quite a few accountability logics for electronic transactions. Therefore, this section discussed a few of the works accomplished by researchers in analyzing accountability.

In [8], the authors stressed the importance of accountability and how it can resolve disputes among participants in any internet transaction. They stated that accountability enables each party to be aware of what has been done and who is responsible for every action performed during the transaction, consequently holding participants involved in a transaction accountable for their actions with undeniable justification. Furthermore, the authors stress that the primary goal of accountability is to use sufficient recorded evidence to resolve disputes among participants, which could be used in a court of law if disputes arise at the end of a transaction, however, despite many researchers' claim that they proposed a protocol that meets the accountability need of internet transactions. The authors of this paper have argued that such claimants are yet to meet the standards needed to eliminate disputes effectively.

The need to address this gap inspired them to propose a new accountability security property for Internet transactions. In their approach to enhancing security, the following two accountability properties were proposed. The first property is centered on responsibility by harvesting evidence for all activities made during Internet transactions, which participants will use to resolve disputes if it arises. Finally, the second property involves responsiveness, availability of evidence, and the speed at which trusted third participants send evidence to external participants to resolve disputes.

A detailed and reliable accountability analysis approach using a mobile payment protocol is proposed in [10]. The proposed protocol comprises five engaging parties: client or payer, who purchases services and goods from merchants, a merchant or payee denoted as a store, or a person who has services and goods to sell to the client. Similarly, a financial company denoted Mobile Network Operator (MNO) serves as a financial company for both the payer and the payee.

Finally, the Time stamp center (TSC) for authorization among the parties. The protocol underscores seven phases with specific functions. They are as follows: payment initialization, payment subtraction request, payment authorization request,

payment confirmation request, payment confirmation response, payment authorization response, and payment subtraction response. The major drawback of the protocol is the use of symmetric encryption, which is the main focus of this paper. Also, the protocol provides weak authentication, such as providing only on payer side. This paper therefore deduces that the approach in this protocol can lead to potential fraud by the attacker. As a result, it lacks all the attributes of accountability.

Similarly, the vulnerability of KN's logic, such as lack of reasoning for accountability in symmetric key and revealing secret information to a verifier, was identified by the authors of [11]. Therefore, to mitigate these challenges, a novel logic (KP's logic) is proposed that will only send the required information to the verifier, and the authors claimed that their approach could eliminate disputes among participants. Nonetheless, research has shown that KP's logic lacks the critical reasoning for accountability in symmetric encryption, inspiring the authors in [12] to extend the KP's logic and proposed the KSL's logic, which has the robustness of analyzing protocols for both asymmetric and symmetric encryption processes. However, their proposed protocol details were never described in detail, but information for more reading was provided in their reference section [13].

Kailar is probably the first to propose a modal logic with the primary objective of reasoning about accountability. It continues to highlight Kaila's definition for accountability as concerned with the ability to prove the association of an originator with some action to a third party without revealing any private information to the third party." The prover is the party who can prove such statements, while the verifier is the party being convinced of the proof. Kailar has adopted the "CanProve" modal operator to validate the notion of accountability, for instance, "A CanProve x to B," where A and B signify the prover and verifier, respectively, and x stands for a general statement about some action [14].

Nevertheless, research has shown that Kailar's approach can only provide reasoning for the accountability of signed messages but is insufficient for analyzing complex cryptographic messages such as hashed messages and signed encrypted messages. Also, quite a few researchers have stated that Kailar's prover CanProve x to verifier cannot justify the predicates and rules because of its lack of semantics and finally does not reason about verifiers [4], [15]. Therefore, they are casting doubts about the correctness of Kailar's calculus, which inspired Kessler and Neumann to adopt a new modal logic to mitigate this challenge. They claimed to have handled this concern found in Kailar's novel framework.

To mitigate the identified concerns in Kessler and Neumann's (K&N) and Kailar's framework, the authors in [16] presented a novel modal logic that extends the idea of Kessler and Neumann, which applies the idea of provable authorization on private information. The prover efficiently sends only the required information to the judge during dispute resolution, enabling proving some statements without revealing secret information. This approach has claimed to be very efficient and safe because the prover can prove statements without revealing any private information to the verifier. The authors extend K&N's logic in two phases used to analyze both iKP and SET protocol, respectively. However, they claimed the message format of SET has led to the lack of accountability after all the two analyses were conducted. Nevertheless, a successful proof of money accountability was achieved for the iKP due to its message format.

Finally, the first automated model of accountability in electronic payment protocol centered on Blanchet probabilistic polynomial calculus was proposed by the authors in [17]. Injective or Non-injective correspondence is used to express the accountability of money and goods, respectively, using CryptoVerif automated tool. The authors were able to automatically analyze the accountability of the money and goods of electronic payment protocols. This approach is found to be very efficient and valuable as it is regarded to be the first of its kind in the analysis of accountability with the electronic transaction [18].

III. KAILAR LOGIC

In 1996, Rajashekar Kailar introduced a new Kailar Logic framework to analyze accountability among participants within electronic-commerce transactions or other related protocols requiring accountability analysis. The rationale behind Kailar Logic is to ascertain the accurate establishment of the origin of a message among the participants involved in a protocol exchange. For instance, participants involved in a protocol exchange or electronic transaction treat signed messages as undeniable statements. Therefore, to convince another party through the use of proof of statements in a sequence of operations will consequently make that statement true.

Before the advent of the Kailar Logic, most of the logic was based on a belief approach that has yet to address the needs of modern protocols adequately. The introduction of Kailar Logic provides accountability analysis of protocols and enables the detection and deletion of redundant information within analyzed protocols [4].

Kailar Logic uses the following six (6) logic components as signs and four (4) postulates as explained in the next section.

A: Sender of message

B: Receiver of message

SK_p: Secret Key of party **P**, used for signing digital signatures

PK_p: Public Key of party **P**, used for encryption and for verifying signature signed under **SK_p**

h(x): Output of one-way hash function **h()** with message ***x*** as its input

{x}PK_p: Encryption of message **x** under **P**'s public key, **PK_p**

{x}SK_p: Message **x** signed with **P**'s Secret key **SK_p**

{x}k: Symmetric-key encryption of message ***x*** under a session key **k**.

A. Components of Kailar Logic

This paper considers only a few of Kailar Logic statements and postulates that would be needed to analyze the protocol's accountability. Also, due to restriction of content, these statements and postulates are briefly explained.

1) Strong Proof: "A CanProve x" and Weak Proof: "A CanProve x to B": Firstly, the Strong Proof: "A CanProve x" is the proofing of x to a third party B by principal A, which denotes that A can persuade the principal B of statement x by executing a series of sequence of operations and not disclosing any secret of y(y≠x) to B. Finally, Weak Proof: "A CanProve x to B", is the process of weakly proving statement x to principal B, which means principal A can persuade the principal B of statement x after performing a sequence of operations that do not disclose any secret about y(y≠x) to B. However, to attain accountability in this work, this paper only use the Strong Proof: "A CanProve x" [4].

2) Signature Verification Component: "K_a Authenticates A": This statement denotes that the signature of principal **A** can be authenticated using the key $\mathbf{K_a}$. Therefore, to fulfill the needs of accountability analysis in this paper, any encrypted statement with $\mathbf{K_a}$ can be associated with principal **A**. Also, since it was mentioned earlier that this paper would be using asymmetric encryption in this work, $\mathbf{K_a}$ can safely be denoted as the public key and $\mathbf{K_a^{-1}}$ to be the private key to enhance the easy understanding of this statement.

3) Message Interpretation: ***"x in m":*** The statement ***"x in m"*** implies that ***x*** is one or several plaintexts or ciphertext fields or groups found in the message m, which is commonly just referred to as the interpretable fields or groups in many works of literature. However, this interpretation needs to be clearly defined by the protocol designers because it is protocol specific.

4) Declaration Component: ***"A Says x":*** The declaration ***A Says x*** implies that the principal ***A*** is answerable for the statement ***x*** and any other statement implied by the ***x***, making ***A*** to be accountable for ***x***. Furthermore, if ***A*** says any statement composed of more than one part, ***A*** is accountable for all of those statements. For instance, if A declares the cascade of two formulas ***x*** and ***y***, then ***A*** declares each of them, ***A Says (x, y) ⇒ A Says x*** and ***A Says y***.

5) Message Receiving Component: "A Receives m SignedWith K^{-1}": The message receipt denotes that the Principal ***A*** receives a message ***m*** signed with a private key $\boldsymbol{K^{-1}}$. Also, in this definition, the signatures and contents associated with the messages are denoted by ***m***. The following postulate is used for analysis in most of the existing literature. It indicates that ***x*** is a combination of fields or an interpretation of a field within the message.

$$\frac{\text{A Receives m SignedWith K} - 1;\ \text{x in m}}{\text{A Receives x SignedWith K} - 1}$$

6) Trust Component: "A IsTrustedOn x" and "A IsTrustedOn x by B" : Finally, the global and no-global trust denotes that if principal ***A*** is trusted on statement ***x***, then ***A*** has the power to endorse ***x*** and equally liable for making statement ***x***. However, to be specific, when ***A*** is globally trusted on ***x*** (***"A IsTrustedOn x"***), then it means ***A IsTrustedOn x*** by all principal, in contrary, when ***A*** is Non-globally trust on ***x*** (***"A IsTrustedOn x by B"***), then it means that the principal ***A*** is accountable to prove to principal ***B*** that ***A*** is responsible for statement ***x***, which means that ***A*** is trusted on statement ***x*** [4].

B. Postulates of Kailar Logic

This segment introduces the properties of accountability by using some of the notations explained below. Although Kailar Logic has lots of postulates, some of which are general properties and others are specific to electronic messages that are digitally signed. However, this paper will only introduce the necessary postulates to analyze accountability among participants with an electronic transaction. Therefore, below are some of the utilized postulates, and the following form will be used to express the postulates presented in this paper.

$$\frac{P;\ Q}{R}$$

The above postulate signifies that if the statement P and Q hold concurrently, then it means the resulting statement R equally holds, and P and Q signify the basis of the rule.

1) Conjunction: This postulate denotes that if the principal ***A*** can prove that both statement ***x*** and ***y*** hold, consequently ***A*** can prove that the conjunction ***x∧y*** is true. It is instrumental in analyzing the accountability among principals because to examine the proving scope of each principal, this postulate can compose their statements to conclude. Similarly, the individual statements signed and sent across the network can be used to hold principals accountable for the composite statements they have made.

$$\frac{A\ CanProve\ x;\ A\ CanProve\ y}{A\ CanProve\ (x \wedge y)}$$

2) Inference: In [4], principal ***A*** can prove ***y*** holds if ***A*** can prove ***x*** and at the same time ***x*** denotes ***y***, which also means since ***x*** implies ***y*** and ***A*** can prove ***x***, then ***A*** can prove that ***y*** is real. Statements such as (***x⇒y***), which is used to express the interpretation of signed messages, should always be explicitly defined by the protocol designers, and usually used in the analysis to derive inferred results from statements that are ascertained.

$$\frac{A\ CanProve\ x;\ x \Rightarrow y}{A\ CanProve\ x}$$

3) Signature Rules: When ***A*** receives a message ***m*** signed with key $\boldsymbol{K^{-1}}$, and at the same time the message ***m*** contains statement ***x***, and principal ***A*** can prove that during the message signature, the key ***K*** authenticates the principal ***B***. Therefore, ***B Says x*** can indeed be proved by the principal ***A***. This postulate plays a significant role in helping to prove that principals are accountable for the messages signed by them.

$$\frac{\text{A Receives (m SignedWith } K^{-1});\ \text{x in m};\quad A\ CanProve\ (K\ Authenticates\ B)}{A\ CanProve\ (B\ Says\ x)}$$

4) Trust Rules: As mentioned earlier, the paper will focus on the postulates that have importance toward the

accountability analysis. Therefore, other trust postulates will not be primarily included in this paper but will be used as a prerequisite to get to the results of the trust postulate used in this paper. Consequently, newbies to this framework will need to go and read the missing trust postulates. This trust postulate denotes that if the principal ***B***, who is an authority on ***x***, and at the same time ***Says x***, can be proved by principal ***A***, then ***A*** can prove that the statement ***x*** holds. The outcome below can be attained by applying ***Conjunction***, ***Inference*** on $\mathbf{T_1}$, which is not presented in this work, and finally applying $\mathbf{T_2}$ on the resulting statement. Note that the author decided to exclude both $\mathbf{T_1}$ and $\mathbf{T_2}$ in this work.

A CanProve (B Says x);

$$\frac{A\ CanProve\ (B\ IsTrustedOn\ x)}{A\ CanProve\ x}$$

IV. Summary of the Symbols and Theories

This paper, as mentioned earlier, will follow the general communication protocol, which has a group of principals exchanging messages among each other, commonly denoted by uppercase letters, for instance (X, Y…). Similarly, the message interpretations are the statements by each message and are commonly denoted by lowercase letters (x, y …), and these terms will enhance the primary objectives of proving the origin of the message based on the capacity of the involved principals. For instance, a proof of *statement x* can be regarded as a set of operations that convinces another principal of *statement x*. However, the steps of the proof are mainly dependent on the specifications of the designed protocol. Therefore, this paper will not stress on the steps of proof but instead the analysis of accountability within the Delegation-Based Sequenced Packet Exchange (SPX) [19]. Furthermore, this paper uses the Greek Capital Letter Psi (Ψ) to represents the set of rights that a principal can execute. Equally, the paper introduces a new term called CanExecute, which symbolizes the ability a principal has to execute certain delegated or given rights. For instance,

"X CanExecute Ψ.": It means principal X has all the rights to execute the assigned rights to Ψ. Similarly,

"X CanExecute Ψ with K.": This means that principal X can only execute the rights assigned to Ψ with the key K, and in both examples, principal X will be held responsible for those executed rights. As mentioned earlier, rights could mean objects or actions to be executed.

A. Synopsis of the Newly Introduced "X CanExecute Ψ" Postulates

As discussed above regarding the "*X CanExecute Ψ*" postulate, this section will not only help the readers to understand the full capabilities of this postulate, but it will also highlight its significances in the analysis stage. A principal providing can execute a right or set of rights he or she has permission to execute from another principal, who could be a Trusted Authority in this analysis, such as administrator of computer systems and networks, as mentioned in the introduction. Expressly, a principal can only delegate the rights he or she can execute to another principal. For instance, *principal X* can only delegate a set of rights *Ψ* to *principal Y* only if it has the right to execute the rights listed in *Ψ*. To conclude, the above-delegated rights Ψ executed by to Y should hold *principal X* answerable for delegating these rights to *principal Y*, and there must be authentication in place when *principal Y* executes the delegated rights Ψ. Therefore, this paper introduces two new postulates to support our analysis, and they are denoted as [Ẍ], and [Ỹ], respectively.

1) [Ẍ]: The postulate above, "[$\mathbf{\ddot{X}}$]", denotes that the listed set of rights in **Ψ** can be executed by *principal X*, while in the second statement, he or she also delegates to *principal Y* to execute the same rights. Finally, the postulate's last statement denotes that in executing the delegated rights listed in **Ψ**, *principal Y* will be authenticated with the key $\mathbf{K_{Del}}$. However, to illustrate the magnitude of power a principal has when delegated to execute given sets of rights, we can omit the authentication key **K**, which means once a principal "*X CanExecute Ψ with K*", then principal "*X CanExecute Ψ* " without the key **K**, which the author defined in [$\mathbf{\tilde{Y}}$].

X CanExecute Ψ;

X Says (delegation of Ψ to Y);

$$\frac{(KDel\ Authenticates\ Y);}{Y\ CanExecute\ \Psi\ with\ KDel}$$

2) [Ỹ]: Likewise, the above postulate "[$\mathbf{\tilde{Y}}$]" will be employed during the accountability analysis. This postulate will enable the efficient proof of principals' answerability for the given or delegated sets of rights to execute. For instance, if "*Y CanExecute Ψ with* K_{Del}" where **Y** is the delegate, then our analysis should be able to justify "delegate CanProve (*delegate CanExecute Ψ with* K_{Del}), in which $\mathbf{K_{Del}}$ represents the delegation key of the protocol. Likewise, the delegator's proof of not being responsible for the delegate's actions is equally significant. For example, if "**X** Says (*delegations of Ψ to Y*)" where **X** is the delegator, and **Y** is the delegate, then principal **X** should be able to prove that **Y** is answerable for the actions executed on the delegated set of rights listed in **Ψ**, which can be denoted as delegator (**X**) CanProve (K_{Del} *Authenticates delegate(Y)*)

$$\frac{X\ CanExecute\ \Psi\ with\ K;}{X\ CanExecute\ \Psi}$$

B. The Deletion-based Sequenced Packet Exchange (SPX)

In this section, a Delegation-Based Sequenced Packet Exchange (SPX) is used to study how delegates can hold or prove that the delegators are answerable for their actions during an electronic transaction and vice visa. The authors of [19] highlighted that in SPX, the principals exchange authentication tokens to authenticate each other, which authorizes the secure exchange of session keys. Furthermore, this paper focuses on the analysis of accountability and the delegation capability SPX provides but not the detailed explanation of the SPX protocol. Therefore, readers can refer to [19] for more information. Regardless, this paper provides a brief synopsis of the content of the SPX authentication exchange:

Client CanProve (K_s Authenticates *Server*) [G1]

Server CanProve (K_c, Authenticates *Client*) [G2]

Delegate CanProve (K_{Del}, Authenticates *Delegator*) [G3]

The description of the protocol is as follows:

1. C → CDC: S
2. CDC → C: {{S, K_s, T_{A1},} K_{TA1}^{-1},}K_{CDC}^{-1}
3. CDC → C: {K_{Del}, T,} K_c^{-1}{K_{des}} Ks; {K_{Del}^{-1}} K_{des}
4. S → CDC: C
5. CDC → S: {{C, K_c, T_{A2},} K_{TA2}^{1},}K_{CDC}^{-1}
6. S → C: Response (Accept / Reject)

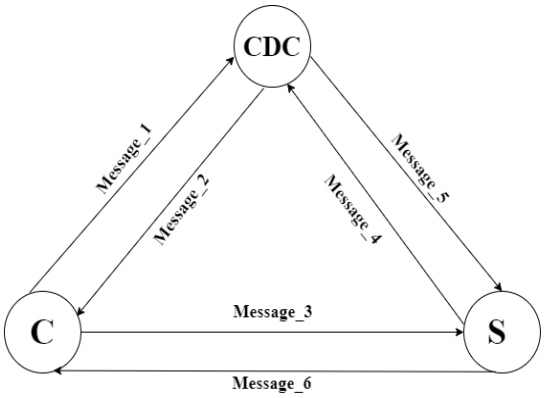

Fig. 1. The Tardo-Alagappan Delegation-Based SPX Protocol.

This section explains a classical Delegation-Based SPX protocol presented in Fig. 1, using the above notation (1-6). Firstly, **C** denotes the Claimant, **S** denotes the verifier, while **CDC** is the Certificate Distribution Center. The first message (*message_1*) signifies **C** is sending the identity of the verifier to **CDC**, then **CDC** responds with a certificate belonging to **S** issued by the Trusted Authority1 (**TA_1**) in the second message (*message_2*), which is encrypted with the private key of **CDC**. Next, **C** sends its delegation public key in the following message (*message_3*), a secret **DES** key **Kdes**, encrypted with **S**'s public key, and the private delegation key encrypted with this secret key. To verify the signature on the delegation key **C**, **S** gathers the above information, sends the certificate of **C** to **CDC**, and gets a key certificate issued by Trusted Authority2 (**TA_2**) from **CDC** (*message_4* and *message_5*). Finally, the public key of **C** in the received certificate was employed by **S** to authenticate the signature of **C** on the delegation key. **S** will respond in the last message ((*message_6*) with an "Accept" only if he or she is convinced with **C**'s delegation key; else, respond "Reject." Note that **TA_1**, **TA_2**, and **CDC** can make certain statements based on the role of Trusted Authorities.

The primary objective of the protocol is for *principal S* to securely obtain a delegation key from *principal C*, which means *principal C* is authorizing *principal S* to serve as a delegate by allocating a set of rights that belongs to **C** with **S** for a given period, defined as **T**. However, it is equally important to note that this protocol is not designed to delegate accountability among principals since the transferred rights to *principal S* still belong to *principal C*. Consequently, it is infeasible to analyze accountability within principals, thereby necessitating the proposal of a new framework in this paper.

It is important to note that from now onwards, this work will be using Cyrillic Capital Letter Omega **Ѡ** to represent the messages in the diagram like **$Ѡ_1$, $Ѡ_2$, …, $Ѡ_N$.**

C. Reformulating the Deletion-Based Sequenced Packet Exchange (SPX)

This section, reformulated the protocol description given above based on the notations adopted by Kailar's logic in [20]. It targets the statements or goals mentioned earlier, such as *(KS, Authenticates S), (K_{Del} Authenticates C during T) and (KC Authenticates C)* in the protocol description, which express the semantics of **$Ѡ_2$**, **$Ѡ_3$**, and **$Ѡ_5$**, respectively, and this has a great significance to the subsequent analysis of the protocol. The following denotes the protocol message interpretation based on Kailar's notation and the protocol's relevant messages.

1) C Receives (((K$_S$, Authenticates S) SignedWith K_{TA1}^{-1}) SignedWith K_{CDC}^{-1}).

2) S Receives (((K$_{Del}$, Authenticates C during T) SignedWith K_C^{-1})).

3) S Receives (((K$_C$, Authenticates C) SignedWith K_{TA2}^{-1}) SignedWith K_{CDC}^{-1}).

However, irrespective of the chronological ordering of the above messages, it should be noted that the Ѡ$_5$ "*S Receives (((Kc, Authenticates C) SignedWith K_{TA2}^{-1}) SignedWith K_{CDC}^{-1})"* which derives the key K$_C$ for authenticating the signature of Ѡ$_3$ has to come first during the analysis stage as a result of Ѡ$_3$ needing the key K$_C$ for signature authentication.

V. Analysis of the SPX Protocol

The analysis will start with SPX without delegation, and the objective of this section is to justify if the SPX protocol without delegation will be able to still prove accountability among principals by using the delegation key (K$_{Del}$) as mentioned earlier based on Kailar's framework, denoted as "*S CanProve (K_{Del} Authenticates C)*." In this case, both the delegate and the delegator's objective is to prove what they are answerable for and the answerability of the other principal. Nevertheless, because the same key (K$_{Del}$) is used to authenticate both the delegator and the delegate, there will not be any accountability. For instance, the Goal "*S CanProve (K_{Del} Authenticates C)*" where *S* is the delegator and C is the delegate, will hold the principal S accountable for C's actions even though she has delegated all the rights to C because the key K$_{Del}$ authenticates S, therefore losing accountability in this process. As a result, this paper concludes that SPX, without support for delegation, cannot guarantee accountability among the principals involved. The following section provides the analysis of the improved Delegation-Based SPX protocol.

A. Summary of the Proposed Delegation-Based Accountability Protocol

After comprehensive research on protocols proposed for delegation tokens such as in [21]–[23], this paper proposed an optimized protocol, which has the functionality of allowing principals to delegate certain individual rights to other principals, which also means the delegation of a principal's accountability to another principal who is responsible in the event something went wrong during a transaction. In this approach, the author makes some assumptions such as;

1) The ability of principals to have access to digital signature services and generate public key pairs.

2) The inclusion of authentication keys within the public keys attain by principals for the verification of digital signatures.

3) Excluding principal authentication, this is assumed to be handled at the start of the protocol. Therefore, below are some of the explanations for the terms and concepts introduced for the proposed protocol.

- Firstly, **R** is the grantor, while **R̄** is the Grantee.
- The sets of delegated rights to be executed are represented by **Ψ** as mentioned earlier.
- The period of the delegation token **T** is represented by **TS.**
- The key pairs authentication for Grantor and Grantee are represented by ($\mathbf{K_R}$, $\mathbf{K_R^{-1}}$) and ($\mathbf{K_{\bar{R}}}$, $\mathbf{K_{\bar{R}}^{-1}}$) respectively.
- The delegation key pairs ($\mathbf{K_{Del}}$, $\mathbf{K_{Del}^{-1}}$), is the use by the Grantee to execute the list of rights in **Ψ.**
- Finally, **Ḿ, Ḿ′,** and **Ḿ″** will be described within the proposed protocol listed below.

The proposed delegation-based accountability protocol is listed as follows, and its represented by $\lambda_1, \lambda_2, \ldots, \lambda_N$.

[λ_1]: R → R̄: R, R̄, Ḿ, K_R^{-1} (Ḿ)

[λ_2]: R̄ → R: R̄, R, Ḿ′, $K_{\bar{R}}^{-1}$ (Ḿ′)

[$\lambda 3$]: R → R̄: T = [R, R̄, Ḿ″, K_R^{-1} (Ḿ″)

In the first message (**[λ_1]**), the **Ḿ** signifies that "**R** wishes to delegate to **R̄** accountability for **Ψ.**" Similarly, **Ḿ′** equally signifies that "**R̄** accepts **Ψ** and she will exercise **Ψ** using $\mathbf{K_{Del}}$" in the second message (**[λ_2]**), and finally, **Ḿ″** signifies [**Ψ, TS,** $\mathbf{K_R}$, and $\mathbf{K_{Del}}$] in the final message (**[λ_3]**), where **TS** signifies the delegation token's time span. Moreover, to mitigate phishing attacks, in λ_3, the essential $\mathbf{K_R^{-1}}$ is used to represent the grantor instead of using the name "**R**" this is because even an attacker succeeded in masquerading as **R**, he cannot delegate the grantor's accountability because he did not know $\mathbf{K_R^{-1}}$. Similarly, **R̄** is only allowed to execute the set of rights in **Ψ** by the approval of the grantor (**R**).

In conclusion, there are quite a few assumptions made based on the referenced papers on delegations' tokens which might not be included in this paper. Therefore, the reader can refer to these articles for a better understanding of some of the conditions imposed based on delegation tokens [21], [23].

B. Initial State Assumptions

The needed initial assumptions are listed below for our accountability analysis. Note that **R** and **R̄** represent the Grantor and the Grantee, respectively, as indicated above, whereas the Greek Capital Letter Xi (**Ξ**) is used to represent the assumptions such as $\Xi_1, \Xi_2, \ldots, \Xi_N$.

[Ξ_1]: R CanProve (K_R Authenticates R);

[Ξ_2]: R̄ CanProve ($K_{\bar{R}}'$ Authenticates R̄);

[Ξ_3]: R̄ CanProve (K_{Del} Authenticates R̄);

[Ξ_4]: R̄ CanProve (R CanExecute Ψ);

[Ξ_5]: R CanProve (R̄ IsTrustedOn (K_{Del} Authenticates R̄);

[Ξ_6]: R CanProve ($K_{\bar{R}}'$ Authenticates R̄);

[$\Xi 7$]: R̄ CanProve (KR Authenticates R);

This paper denotes that assumptions Ξ_1, Ξ_2, and Ξ_3, to be associated with asymmetric keys, which means that the association of principals to statements can be proved with the help of public-key certificates. Moreover, Ξ_4 assumes that Grantee CanProve Grantor is able to execute the set of rights listed in Ψ**.** However, even though R been the grantor is delegating the grantee been R̄**,** the grantee has to be convinced the delegated rights belong to R.

Similarly, Ξ_5 is assumed to be trusted during the announcement of its delegation key because he is accountable for the message signed with this key. Lastly, this paper's objective, as mentioned earlier, is not on the authentication of principals but on the delegation. Therefore, the author makes Ξ_6 and Ξ_7 based on the assumption that before the delegation protocol starts, the primary goals of a public key distribution protocol were reached as implemented in the certificate distribution center of the SPX protocol [19].

C. Objectives and Improved Delegation-Based Accountability Protocol

The following denotes the improved protocol message interpretation based on Kailar's notation and the protocol's relevant messages.

1) R̄ Receives ((R wishes to delegate to R̄ accountability for Ψ) SignedWith K_R^{-1}).
2) R Receives ((K_{Del}, Authenticates R̄) SignedWith $K_{\bar{R}}'^{-1}$).
3) R̄ Receives ((delegation of Ψ to R̄′) SignedWith K_R^{-1}).

Similarly, below are the main Objectives and explanations, which will be used together with the *inference rules* of Kailar logic, the assumptions made, and the protocol messages during the accountability analysis to attain the goals listed below. Thus, this works represents the goals as Greek Capital Letter Pi (Π) such as $\Pi_1, \Pi_2, \ldots \Pi_N$, and the first goal of our accountability analysis is:

[Π_1]: R̄ CanProve (R̄ CanExecute Ψ with K_{Del})

If our analysis can prove the above goal with the application of the new proposed postulate **[Ỹ]**, and the Inference postulate, the results of the analysis can show more general facts that;

R̄′ CanProve (R̄ CanExecute Ψ).

Finally, to ensure accountability between the Grantor and the Grantee, the analysis in this paper wants to prove that the Grantor can prove the delegation key "K_{Del}" is used to authenticate the Grantee because R cannot be accountable for "*R̄′ CanExecute Ψ using* K_{Del}." Therefore, the second goal of this paper's analysis will be as follows;

[Π_2]: R CanProve (K_{Del} Authenticates R′)

D. Analysis of the Improved Delegation-Based Accountability Protocol

The author starts the delegation accountability analysis by applying the **sign** postulate on $\mathbf{G_3}$ and **A7** to obtain the following results, which will help us in the next step of the analysis, it is important to note that the sign postulates are represented by $\boldsymbol{\lambda_1, \lambda_2, \ldots, \lambda_N}$.

[λ_1]: R CanProve (R Says (delegation of Ψ to R))

Therefore, in attaining the above results, we will use the ***Conjunction (Conj)*** postulate on assumptions Ξ_3, Ξ_4, and the λ_1 attained above, the final results after the above process are;

[λ_2]: R CanProve (R CanExecute Ψ,

R Says (delegation of Ψ to R),

K_{Del} Authenticates R)

Finally, we will have to use the *Inference (Inf)* and the [$\ddot{\mathbf{X}}$] postulate on λ_2 to obtain **[Π_1]**.

[Π_1]: R CanProve (R CanExecute Ψ with K_{Del})

Note that at this stage of the analysis, we have proven our first goal as stated above, which means that the grantee can prove he or she is accountable for executing the actions or rights listed in **Ψ** using the key $\mathbf{K_{Del}}$. Furthermore, now we can use the sign postulate and apply it to $\mathbf{G_2}$ and Ξ_6 to show the results below, which will help us achieve our final goal. Therefore, applying λ_2 on $\mathbf{G_2}$ and Ξ_6, we have the following;

[λ3]: R CanProve (R Says (KDel Authenticates R))

In conclusion, our Π_2 is deduced by Trust postulates using λ_3 and Ξ_5 as the basis. Consequently, we conclude that our analysis shows that the improved protocol achieves its objectives, such as empowering the *Grantor R* and the *Grantee R̄* to hold each other accountable for their actions made after the protocol. For instance, the *Grantor (R)* can prove that the delegation key K_{Del} *authenticates R̄*.

VI. Conclusion

The increasing security and privacy threat on the internet has made accountability a significant necessity in almost all electronic commerce transactions. Identifying protocol messages that need to provide accountability assurances during the design of electronic commerce protocols or other internet transaction-related protocols should be regarded with great significance and mainly to avoid disputes among participants in a given transaction. This paper raises the importance of accountability, especially in electronic transactions. Additionally, we introduce in detail a framework to analyze accountability of delegation-based SPX protocol. Delegation allows transfers of a set of rights to another principal to execute, such as from a delegator to a delegate. The result of our study proved that the critical issues of accountability associated with the transferred rights are disregarded or ignored by many. Finally, the paper recommends consideration of accountability during the design of protocols, especially for electronic commerce, in order to prevent possible dispute among participants during a transaction. For future work, the Author intends to explore Kailar's framework to analyze more protocols.

Acknowledgment

The authors would like to thank all the reviewers for their insightful comments that significantly help us to improve this manuscript. Special thanks to Prof Wang Xue Ming for the guidance and supervision over the past years. Dr. Mbemba Hydara, thanks for the insightful comments, contribution, and advice. Eva Lee Redding, thanks for all the support over the past years.

References

[1] Raguseo, "Big data technologies: An empirical investigation on their adoption, benefits and risks for companies," Int. J. Inf. Manage., vol. 38, no. 1, pp. 187–195, Feb. 2018, doi: 10.1016/J.IJINFOMGT.2017.07.008.

[2] H. Hasan et al., "Secure lightweight ECC-based protocol for multi-agent IoT systems," Int. Conf. Wirel. Mob. Comput. Netw. Commun., vol. 2017-October, 2017, doi: 10.1109/WiMOB.2017.8115788.

[3] R. Pradeep, N. R. Sunitha, V. Ravi, and S. Verma, "Formal Verification of Authentication and Confidentiality for TACACS+ Security Protocol using Scyther," 2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019, pp. 1–6, 2019, doi: 10.1109/ICCCNT45670.2019.8944623.

[4] C. Wang, N. Shu, and H. Wang, "Formal analysis of a model for electronic payment systems," vol. 116, no. Ceie 2016, pp. 613–620, 2017.

[5] L. Gong, R. Needham, and R. Yahalom, "Reasoning about Belief in Cryptographic Protocols," 1990.

[6] Y. Zhang and V. Varadharajan, "A logic for modeling the dynamics of beliefs in cryptographic protocols," Proc. - 24th Australas. Comput. Sci. Conf. ACSC 2001, pp. 215–222, 2001, doi: 10.1109/ACSC.2001.906645.

[7] R. Kunnemann, I. Esiyok, and M. Backes, "Automated verification of accountability in security protocols," Proc. - IEEE Comput. Secur. Found. Symp., vol. 2019-June, pp. 397–413, 2019, doi: 10.1109/CSF.2019.00034.

[8] C. Techapanupreeda, R. Chokngamwong, C. Thammarat, and S. Kungpisdan, "Accountability in Internet Transactions Revisited," pp. 378–382, 2014.

[9] D. E. Corporation, P. Alto, D. E. Corporation, and O. K. Square, "A Semantic for a Logic of Authentication," pp. 201–216, 1991.

[10] T. S. Fun, L. Yu, S. Alias, and N. M. Rusli, "Accountability Analysis of Mobile Payment Protocol," Int. Conf. Comput. Eng. Netw. Secur., no. November 2014, 2012.

[11] S. Kungpisdan, "Modelling , Design , and Analysis of Secure Mobile Payment Systems," Master Thesis, 2005.

[12] S. Kungpisdan, B. Srinivasan, and P. D. Le, "Lightweight mobile credit-card payment protocol," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2904, pp. 295–308, 2003, doi: 10.1007/978-3-540-24582-7_22.

[13] C. Techapanupreeda and S. Kungpisdan, "A secure accountability protocol based on public key encryption," IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, pp. 2491–2495, 2017, doi: 10.1109/TENCON.2016.7848482.

[14] T. S. Fun, L. Yu, S. Alias, and N. M. Rusli, "Accountability Analysis of Mobile Payment Protocol," 2012.

[15] C. Techapanupreeda, R. Chokngamwong, C. Thammarat, and S. Kungpisdan, "An accountability model for Internet transactions," Int. Conf. Inf. Netw., vol. 2015-Janua, pp. 127–132, 2015, doi: 10.1109/ICOIN.2015.7057869.

[16] P. Kungpisdan, Supakorn, Yongyuth, "Practical Reasoning about Accountability in Electronic Commerce Protocols," Proceedings of the 4th International Conference Seoul on Information Security and Cryptology. https://dl.acm.org/doi/10.5555/646283.687998 (accessed Sep. 01, 2020).

[17] B. Meng, F. Shao, and W. Huang, "A computer-assisted framework for accountability of electronic payment protocol in computational model," Int. J. Adv. Comput. Technol., vol. 3, no. 4, pp. 49–65, May 2011, doi: 10.4156/ijact.vol3.issue4.6.

[18] B. Meng, "Computer aided verification of accountability in electronic payment protocol with cryptoverif," Int. J. Adv. Comput. Technol., vol. 3, no. 3, pp. 68–88, 2011, doi: 10.4156/ijact.vol3.issue3.7.

[19] J. J. Tardo and K. Alagappan, "SPX: Global authentication using public key certificates," J. Comput. Secur., vol. 1, no. 3–4, pp. 295–316, 1992, doi: 10.3233/JCS-1992-13-406.

[20] R. Kailar, "Reasoning about accountability in protocols for electronic commerce," Proc. IEEE Comput. Soc. Symp. Res. Secur. Priv., pp. 236–250, 1995, doi: 10.1109/secpri.1995.398936.

[21] M. R. Low and B. Christianson, "Self authenticating proxies," Comput. J., vol. 37, no. 5, pp. 422–428, 1994, doi: 10.1093/comjnl/37.5.422.

[22] K. R. Sollins, "Cascaded Authentication.," Proc. Symp. Secur. Priv., pp. 156–163, 1988.

[23] M. Gasser and E. McDermott, "An architecture for practical delegation in a distributed system," Proc. Symp. Secur. Priv., pp. 20–30, 1990, doi: 10.1109/risp.1990.63835.