ISSN: 1859-2171
e-ISSN: 2615-9562
TNU Journal of Science and Technology 208(15): 161 - 167

NGHIÊN CỨU ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN ĐỂ NGĂN CHẶN TẤN CÔNG THƯ RÁC

Lê Hoàng Hiệp[1]*, Trần Thị Yến[2], Đỗ Đình Lực[1], Nguyễn Văn Vũ[2], Nguyễn Văn Trung[2], Trần Ngọc Trường[3]
[1]Trường Đại học Công nghệ thông tin & Truyền thông – ĐH Thái Nguyên,
[2]Trường Đại học Sư phạm kỹ thuật Nam Định,
[3]Trường Cao đẳng Công nghiệp Thái Nguyên

TÓM TẮT

Trên thực tế có nhiều kỹ thuật dùng để ngăn chặn các cuộc tấn công thư rác (spam email), tuy nhiên hầu hết chưa phương pháp nào có thể ngăn chặn triệt để vì kẻ tấn công ngày càng có các kỹ thuật tinh vi hơn. Trong bài báo này nhóm tác giả tập trung nghiên cứu ứng dụng của công nghệ Blockchain trong việc giảm thiểu và ngăn chặn các cuộc tấn công spam email sử dụng thuật toán $SAGA_{BC}$ (Spam Attack Guard Algorithm Using BlockChain) thông qua thực nghiệm mô phỏng chứng minh tính hiệu quả. Kết quả cho thấy, với các trường hợp người dùng sử dụng $SAGA_{BC}$ để gửi hoặc nhận email, tỉ lệ bị tấn công thư rác giảm xuống rõ rệt so với cách gửi nhận truyền thống.

Từ khóa: *Blockchain; Ứng dụng Blockchain; Tiền mã hóa; Thư rác; Tấn công spam email*

Ngày nhận bài: 17/10/2019; Ngày hoàn thiện: 15/11/2019; Ngày đăng: 27/11/2019

STUDY TO APPLYING BLOCKCHAIN TECHNOLOGY FOR PREVENTING OF SPAM EMAIL

Le Hoang Hiep[1*], Tran Thi Yen[2], Do Dinh Luc[1], Nguyen Van Vu[2], Nguyen Van Trung[2], Tran Ngoc Truong[3]
[1]University of Information and Communication Technology – TNU,
[2]Nam Dinh University of Technology Education,
[3]Thai Nguyen Industrial College

ABSTRACT

In fact, there are many techniques used to prevent spam attacks, but most have not been able to prevent them completely because attackers are getting more sophisticated techniques. In this paper, the authors focus on studying the application of Blockchain technology in reducing and preventing email spam attacks using $SAGA_{BC}$ algorithm through simulation experiments to prove the effectiveness. The results showed that, for the case of users using $SAGA_{BC}$ (Spam Attack Guard Algorithm Using BlockChain) to send or receive email, the rate of spam attacks decreased significantly compared to the traditional way of sending and receiving.

Keywords: *Blockchain; Blockchain application; Cryptocurrencies; Spam; Email spam attack*

Received: 17/10/2019; Revised: 15/11/2019; Published: 27/11/2019

* Corresponding author. *Email: lhhiep@ictu.edu.vn*

1. Giới thiệu

Thư rác, thư linh tinh, hay còn dược dùng dưới tên là spam (Stupid Pointless Annoying Messages) hay spam mail, là các thư điện tử vô bổ thường chứa các loại thông tin không có ích, thậm chí còn có hại cho người dùng như thông tin quảng cáo, email đính kèm virus, thông tin nhạy cảm,…đôi khi, nó dẫn dụ người nhẹ dạ, tìm cách đọc số thẻ tín dụng và các tin tức cá nhân của họ được gửi một cách vô tội vạ và nơi nhận là một danh sách rất dài gửi từ các cá nhân hay các nhóm người và chất lượng của loại thư này thường thấp. Spam email là một trong các phương thức của các cuộc tấn công DDoS (Distributed Denial of Service), là một trong những thách thức an ninh phổ biến nhất mà cả cá nhân và các tổ chức, doanh nghiệp phải đối mặt trong việc đảm bảo an toàn thông tin của họ. Cụ thể hơn *Phishing* là một phương thức lừa đảo nhằm giả mạo các tổ chức có uy tín như ngân hàng, trang web giao dịch trực tuyến và các công ty thẻ tín dụng để lừa người dùng chia sẻ thông tin tài chính như: tên đăng nhập, mật khẩu giao dịch, những thông tin nhạy cảm khác của họ. Phương thức tấn công này còn có thể cài phần mềm độc hại vào thiết bị của người dùng. Chúng thực sự là mối quan ngại lớn nếu người dùng chưa có kiến thức về kiểu tấn công này hoặc thiếu cảnh giác về nó.

Đặc điểm chính của phương thức tấn công spam email đó là: nhúng một liên kết trong một email chuyển hướng người dùng tới một trang web không an toàn và yêu cầu người dùng cung cấp những thông tin nhạy cảm; Giả mạo địa chỉ người gửi trong một email để xuất hiện như một nguồn đáng tin cậy và yêu cầu thông tin nhạy cảm; Đặt một Trojan (mã độc) thông qua một tập tin đính kèm trong email hoặc quảng cáo những thứ (mà kẻ xâm nhập mong muốn) được gửi vào hòm thư của người dùng. Từ đó, kẻ xâm nhập có thể khai thác lỗ hổng và có được thông tin nhạy cảm.

Tấn công DDoS thông qua spam mail là một dạng của tấn công DDoS. Ở dạng này, Attacker (kẻ tấn công) thâm nhập vào mạng bằng một chương trình được đính kèm vào spam mail. Sau khi khởi chạy file đính kèm đó, nguồn tài nguyên của Mail Server sẽ bị cạn kiệt dần bởi một số lượng lớn mail từ các máy khác trong Domain gửi đến gây ra hiện tượng từ chối dịch vụ DoS. Kẻ tấn công đã tạo ra các spam mail vượt qua được bộ lọc spam và chuyển spam mail ấy tới hộp thư của người dùng [1].

Hình 1. *Minh họa Spam Email Attack*

Trên thực tế đã có nhiều nghiên cứu, đưa ra nhiều giải pháp nhằm ngăn chặn việc bị tấn công spam email. Tuy nhiên sự sáng tạo của con người gần như vô hạn, đó là khi người gửi email spam (Spammer) luôn luôn tìm ra được cách mới để có thể tiến hành thực hiện thành công việc chuyển hay gửi các spam email tới hộp thư của người dùng cho dù người dùng có mong muốn hay không.

Trong bài báo này sẽ tập trung nghiên cứu, phân tích các ứng dụng của công nghệ Blockchain như một kỹ thuật [2] nhằm hạn chế hoặc ngăn ngừa các cuộc tấn công spam email.

2. Cơ sở xây dựng giải thuật $SAGA_{BC}$

2.1. Khởi đầu

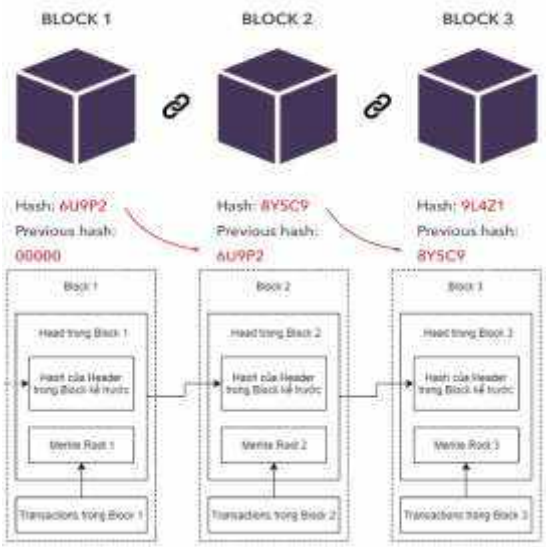
Một email chính thống (không phải spam email) có thể được nhận một cách bình thường từ máy chủ. Tuy nhiên, một số địa chỉ email được sử dụng để spam lại có thể bị từ chối, do đó chỉ có một phần của thư rác gửi đi từ Spammer có thể đến được mục tiêu (nơi nhận). Trong phương pháp được trình bày ở trong thuật toán này, bất kỳ người gửi thư (Sender) nào muốn gửi một email đi đều phải trả một chi phí, chi phí này được gọi là tiền điện tử (Cryptocurrency). Nếu email đó đến được người nhận một cách chính xác, lệ phí đó sẽ được hoàn trả lại cho người gửi. Những người gửi email chính thống (phục vụ cho công việc) sẽ trả một ít chi phí, tuy nhiên những kẻ gửi thư rác (Spammer) sẽ phải trả chi phí nhiều hơn mới có thể thực hiện được

một spam email (hay spam attack). Với phương pháp này sẽ làm giảm các cuộc tấn công spam email bởi lý do như đã nói, đó là kẻ tấn công sẽ phải trả nhiều chi phí cho các cuộc tấn công spam mail (vì số lượng mail rất lớn). Kỹ thuật này gọi là "Spam Attack Guard Algorithm Using BlockChain" (gọi tắt là thuật toán $SAGA_{BC}$).

2.2. Thuật ngữ liên quan

Bởi vì tiền điện tử là một khái niệm tương đối mới, do đó trong bài báo này cần chỉ ra một số khái niệm, thuật ngữ có liên quan tới nghiên cứu này [3]:

+ ***Blockchain***: hay cuốn sổ cái (chuỗi khối), là một hệ thống cơ sở dữ liệu có chứa thông tin, được dùng để lưu trữ thông tin trong các khối (block) thông tin được liên kết với nhau (chain). Cuốn sổ cái (tệp) này không được lưu trữ trong một máy chủ trung tâm như trong một ngân hàng hoặc trong một trung tâm dữ liệu mà ngược lại được phân phối trên toàn thế giới thông qua một mạng lưới các máy tính ngang hàng với vai trò lưu trữ dữ liệu và thực thi các tính toán. Mỗi máy tính này đại diện cho một node của mạng lưới Blockchain và mỗi node đều có một bản sao của tệp sổ cái này. Đồng thời cho phép truyền tải dữ liệu một cách an toàn bằng một hệ thống mã hóa phức tạp và được mở rộng theo thời gian. Công nghệ Blockchain tương đồng với cơ sở dữ liệu, chỉ khác ở việc tương tác với cơ sở dữ liệu.



Hình 2. *Mô tả cấu trúc của công nghệ Blockchain*

+ ***Cryptocurrency***: hay tiền mã hóa là một tài sản kỹ thuật số được thiết kế để làm việc như là một trung gian trao đổi mà sử dụng mật mã để đảm bảo các giao dịch của nó, để kiểm soát việc tạo ra các đơn vị bổ sung và để xác minh việc chuyển giao tài sản. Tiền ảo được phân loại như là một tập con của các loại tiền kỹ thuật số và cũng được phân loại là một tập con của các loại tiền tệ thay thế và các loại tiền ảo. Bitcoin được tạo ra trong năm 2009, là tiền mã hoá đầu tiên. Kể từ đó, nhiều loại tiền mã hóa khác đã được tạo ra. Chúng thường được gọi là altcoin, viết tắt của đồng tiền thay thế.

+ ***Wallet***: Bởi vì các loại tiền điện tử như Bitcoin, Ethereum, Litecoin, ... đều tồn tại dưới dạng kỹ thuật số, cho nên khi muốn lưu trữ hay sử dụng chúng cần phải có một ví lưu trữ riêng, hay còn gọi là ví tiền điện tử. Ví trong Blockchain là một phương tiện lưu trữ tiền điện tử. Bất cứ ai cũng có thể tự do tạo ví miễn phí. Ví được coi là một cơ chế để quản lý tiền điện tử.

+ ***Wallet account***: tài khoản ví là một ID dùng để xác định (nhận dạng) một ví cá nhân của người dùng. Người dùng quản lý tiền điện tử của họ thông qua tài khoản ví.

+ ***Transaction***: là một bản ghi xác thực việc gửi/giao dịch tiền mã hóa từ tài khoản ví của người này tới tài khoản ví của người khác và cần có sự xác thực bằng khóa (key) trong giao dịch.

+ ***Mining (máy đào)***: Khi một Transaction mới được tạo ra bởi một Wallet, nó có thể tạo offline rồi sau đó truyền tải lên Bitcoin Network khi Wallet online (giống như ta viết thư bỏ vào bao thư ở nhà, rồi sau đó mang thư đến mạng lưới chuyển phát bưu điện). Transaction cần phải được Confirm (xác nhận hợp lệ) trước khi được đưa vào Block bởi các máy Mining, các máy Mining có thể là máy vi tính, máy điện thoại, hoặc loại máy chuyên dụng … sử dụng tài nguyên của nó (CPU hoặc GPU) thực hiện các phép toán để xác minh các dữ liệu của Transaction. Các máy Mining tổng hợp đủ số lượng các Transaction vào một Block, sau đó nó sẽ thực hiện việc dò tìm ra một chuỗi Hash thỏa mãn Difficulty Target (độ khó mục tiêu) mà mạng lưới quy

định tại thời điểm đó, việc này gọi là Proof-of-work (bằng chứng làm việc). Sau khi tìm được chuỗi Hash thỏa mãn Difficulty Target, Block đó được xem là Mined (đã được đào), và đưa Block đó vào Blockchain.

2.3. Thiết lập hệ thống, giải thuật

$SAGA_{BC}$ kết hợp với một tài khoản email được liên kết với một tài khoản ví điện tử nhằm ngăn ngừa tấn công spam email. Hiểu đơn giản, một email client (email khách) sẽ có một hoặc nhiều tài khoản email. Một tài khoản ví điện tử sẽ được gán với một hoặc nhiều tài khoản email bởi thuật toán $SAGA_{BC}$.

Email client kết hợp với một tài khoản email sẽ được thiết lập với một tài khoản ví điện tử.

Hệ thống $SAGA_{BC}$ bao gồm các thành phần sau:

- **Cryptocurrency**: Mail Send Coin (**MSC**) là một trong những loại tiền điện tử được triển khai bởi $SAGA_{BC}$. MSC không phải là mã thông báo tiền tệ mà là một loại mã thông báo hữu ích. Bất cứ ai sử dụng $SAGA_{BC}$ cũng có thể sử dụng các loại tiền điện tử hiện có.

- **Mailers (máy gửi):** Trong $SAGA_{BC,}$ một chức năng mở rộng (add-on) của Mailer nói chung được thực hiện:

- ***Hàm quản lý tài khoản (account management function):*** Như được hiển thị trong Hình 3, hàm quản lý tài khoản trích xuất các tài khoản ví đó không chỉ tương ứng với tài khoản email của chủ sở hữu mà còn tương ứng cho một tài khoản email đích.

Email Address	Wallet Account	
user1@ictu.edu.vn	0x1810LQGB	→ Tài khoản ví gửi: 0x2410LQTT
user2@ictu.edu.vn	0x2410LQTT	
user3@ictu.edu.vn	0x24NTBNTT	
user5@ictu.edu.vn	0x2410LQT8	→ Tài khoản ví nhận: 0x2410LQT8
user9@ictu.edu.vn	0x2410LQ9T	

Hình 3. *Trích xuất tài khoản ví*

- ***Hàm yêu cầu xem liệu MSC đã được thanh toán chưa***: hàm này thẩm định một Blockchain về việc liệu MSC có được thanh toán từ ví điện tử phía bên gửi hay không. Bất kỳ dữ liệu đã thu thập từ các kết quả tham chiếu như vậy sẽ được lưu trữ trong hàm này.

- ***Hàm sắp xếp (sorting function)***: Hàm này đánh giá xem email có phải là thư rác hay không theo số lượng MSC đã trả để gửi chúng đi và sắp xếp chúng vào một thư mục email spam.

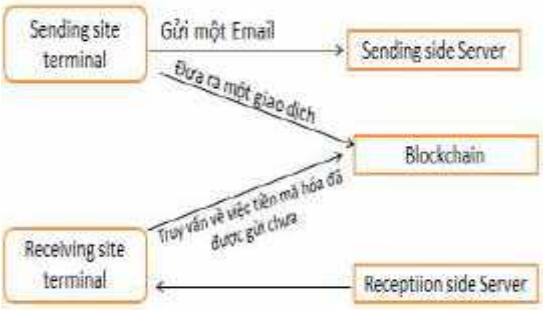
- ***Hàm chuyển tiền (remittance function):*** Hàm chuyển tiền là hàm thanh toán MSC hoạt động từ tài khoản ví tương ứng đến chủ sở hữu tài khoản email mà có liên hệ với tài khoản ví tương ứng với đích đến (nơi nhận) tài khoản email.

- ***Hàm xác nhận (validation function):*** lần đầu tiên email được gửi đến người nhận mới, hàm này xác thực tài khoản ví tương ứng với tài khoản email đích. Sau đó, người gửi thư sẽ kiểm tra tài khoản ví được liên kết và xác định xem họ đã gửi phí MSC cho người nhận chưa. Máy nhận thư kết nối tài khoản ví được thiết lập với máy gửi thư tùy thuộc vào danh tính của tài khoản ví gửi và số tiền phù hợp của MSC đã được thanh toán. Máy gửi thư sau đó gửi phí MSC vào tài khoản ví nhận.

- ***Hàm khai thác (mining function):*** nếu MSC trả tiền không đủ, người dùng có thể bổ sung bằng cách khai thác (đào coin) các giao dịch MSC mà người dùng khác đã phát hành. Một người gửi thư rác cũng có thể bổ sung MSC theo cách tương tự, nhưng chi phí nhiều nhiều hơn cho một người dùng bất hợp pháp để làm như vậy.

2.4. Thủ tục (Procedure) cần tuân thủ khi cả máy gửi và máy nhận sử dụng thuật toán $SAGA_{BC}$:

a. Sending mailers (máy gửi):



Hình 4. *Xác thực tài khoản ví*

Như được hiển thị trong Hình 4, khi một người gửi thư gửi email, nó phát hành một số lượng giao dịch nhất định để gửi MSC vào tài khoản ví tương ứng với tài khoản email đích.

b. Receiving mailers (máy nhận):

Máy nhận thư xác định xem một bức thư email là thư rác dựa trên số lượng MSC đính kèm và sắp xếp thư rác vào thư mục thư rác. Máy nhận thư sau đó sẽ tự động quyết định hoàn phí MSC đã trả tùy theo mức độ mà email đã được xử lý. Nếu tin nhắn bị xóa hoặc được sắp xếp vào thư mục thư rác, phí MSC đã trả phí sẽ không được hoàn lại. Tuy nhiên, nếu tin nhắn (email) không được xử lý trong một khoảng thời gian nhất định, số tiền phí MSC đã thanh toán có thể được hoàn trả vào tài khoản ví.

c. Mining (máy đào):

Các giao dịch đã phát hành được ghi lại ở phần đầu của Blockchain bởi một miner. Tất cả các thực thi liên quan đến giao dịch sau đó được kết thúc.

2.5. Thủ tục (Procedure) cần tuân thủ khi máy gửi hoặc máy nhận không sử dụng thuật toán $SAGA_{BC}$:

a. Khi chỉ có máy gửi sử dụng $SAGA_{BC}$: máy gửi có thể xác định máy nhận có sử dụng $SAGA_{BC}$ hay không dựa vào hàm xác thực (Validation function). Trong trường hợp này, máy gửi có thể gửi một email thông thường mà không phải trả phí giao dịch MSC.

b. Khi chỉ có máy nhận sử dụng $SAGA_{BC}$: Máy nhận có thể xác định máy gửi có sử dụng MSC hay không dựa vào hàm yêu cầu xem liệu MSC đã được thanh toán chưa. Nếu máy gửi không sử dụng $SAGA_{BC}$, máy nhận sẽ biết điều này dựa vào hàm quản lý tài khoản (Account management function). Trong trường hợp này, máy nhận giải quyết các tin nhắn đến như email bình thường sẽ không thể xác thực được đó có phải là thư rác hay không.

c. Khi máy gửi và máy nhận đều không sử dụng $SAGA_{BC}$: trong trường hợp này email được gửi và nhận sẽ sử dụng phương pháp truyền thống như thông thường.

2.6. Dự đoán trước hiệu lực của một cuộc tấn công Spam:

Khi sử dụng thuật toán $SAGA_{BC}$, người gửi email phải đồng thời gửi một khoản phí MSC đến ví nhận nếu muốn thực hiện gửi email. Trên thực tế, Spammer luôn gửi một lượng lớn các thư rác (spam email) khi đó sẽ phải mất tổng chi phí MSC lớn tương ứng. Chính điều này sẽ gây khó khăn khiến Spammer không thể gửi spam email. Khi các email thông thường được nhận một cách chính xác, người gửi email này (không phải Spammer) sẽ không mất phí MSC của họ. Ngay cả khi phí MSC biến mất, họ vẫn có thể phục hồi bởi máy đào (Mining). Bằng cách này người sử dụng $SAGA_{BC}$ sẽ hạn chế nhận được thư rác.

3. Thực nghiệm mô phỏng

Trong phần này sẽ tập trung xác minh việc sử dụng giải thuật $SAGA_{BC}$ có thể ngăn chặn tấn công spam dựa trên việc mô phỏng minh họa. Việc mô phỏng này sẽ không bao gồm người gửi email mà không sử dụng $SAGA_{BC}$ [4], [5], [6].

3.1. Mô hình thực nghiệm:

Như trong hình 5 hiển thị các kế hoạch mô phỏng.

(1). Thiết lập ban đầu (Initial setting): số lượng người sử dụng $SAGA_{BC}$ được chỉ định là "N". Giá trị ban đầu của MSC mà tất cả người dùng đang có được chỉ định là "M". Số Spammer được chỉ định là "S" và số người dùng (người gửi email bình thường) được chỉ định là "N-S".

(2). Gửi email và MSC (Sending emails and MSCs): một người sử dụng $SAGA_{BC}$ bình thường gửi một email và một MSC tới một địa chỉ được lựa chọn từ danh sách người dùng (ngoại trừ địa chỉ riêng của người dùng và địa chỉ của người gửi thư rác). Nếu người dùng bình thường không có bất kỳ MSC nào thì email không thể được gửi đến một địa chỉ đích bằng cách sử dụng $SAGA_{BC}$.

(3). Hoàn trả (Refunds): Không có email nào đã gửi bởi người dùng bình thường (N-S) là thư rác. Chi phí 1 MSC đã gửi tới ví nhận được hoàn trả tới ví đã thiết lập với email người dùng.

(*4). Vòng lặp cho người dùng thông thường (Loop for genuine users):* Mô phỏng thực

hiện lặp lại kế hoạch (1), (2) và (3) bên trên cho (N-S).

(5). Gửi email và MSC (Sending emails and MSCs): Một Spammer sử dụng $SAGA_{BC}$ để gửi một tin nhắn spam và một MSC tới một địa chỉ được chọn từ danh sách người sử dụng khác (ngoại trừ địa chỉ riêng của Spammer. Nếu ví thiết lập với tài khoản của Spammer không có MSC thì Spammer không thể gửi được tin nhắn spam).

(6). Hoàn trả (Refunds): bất kỳ email nào được gửi bởi Spammer thì được coi là thư rác, do đó MSC mà Spammer đã gửi đến ví nhận thì sẽ không được hoàn trả.

(7). Lợi nhuận (Profit): Spammer kiếm được lợi nhuận *b* thông qua xác suất *p* trên mỗi tin nhắn rác đã gửi. Spammer thu được số tiền của MSC như nhau thông qua lợi nhuận *b* kiếm được từ mining.

(***8).Vòng lặp gửi spam (Loop for sending spam):*** thực nghiệm mô phỏng lặp kế hoạch (5), (6) và (7) với số lần là *T*. Trong đó, *T* được chọn ngẫu nhiên từ các số tự nhiên thỏa mãn $0T < N$. Cụ thể là mỗi Spammer sẽ gửi *T* lần tin nhắn rác đến một tài khoản email ngoại trừ tài khoản email của chính họ và không bị chồng chéo đơn vị thời gian cho mỗi lần gửi.

Hình 5. *Kế hoạch cho thực nghiệm mô phỏng*

(9).Vòng lặp cho Spammer (Loop for Spammer): thực hiện lặp các kế hoạch từ (5) đến (8) cho tất cả Spammer.

(10). Vòng lặp trong đơn vị lần (Loop in unit time): các kế hoạch từ (2) đến (9) được coi là một đơn vị thời gian (*t*) và được lặp lại.

3.2. Tham số mô phỏng

Trong mô phỏng này, các tham số được thiết lập như sau: N=10.000 ($M \subset$ 980, 1000, 1020), ($S \subset$ 300, 500, 700). Xác suất phân phối *P* của lợi nhuận *G* được tính như sau:

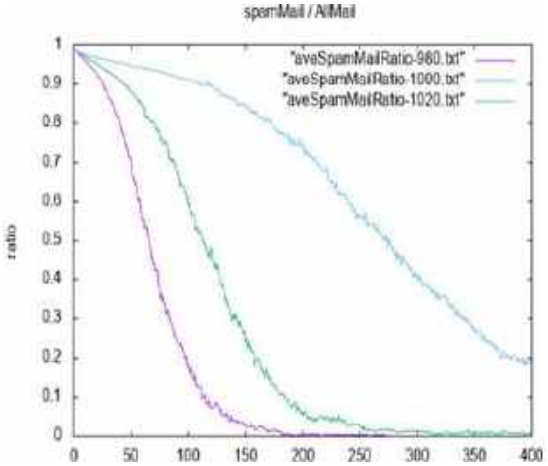
$$P = 1000 \times (C)^{(-X)}$$

Trong đó hằng số *C* là (27) và (*X*) là số phân phối đồng nhất ngẫu nhiên thỏa mãn $0 < X < 330$.

3.3. Kết quả thực nghiệm

Mô phỏng này được thực hiện 100 lần cho một trong ba loại giá trị ban đầu của MSC, thỏa mãn $S = 500$. Hình 6 cho thấy sự thay đổi của mức trung bình trong mỗi 100 lần chạy từ ba điều kiện ($M \subset$ 980, 1000, 1020). Trục ngang của hình cho biết đơn vị thời gian *t*. Trục dọc của hình biểu thị tỷ lệ spam cho tất cả các email đã được gửi.

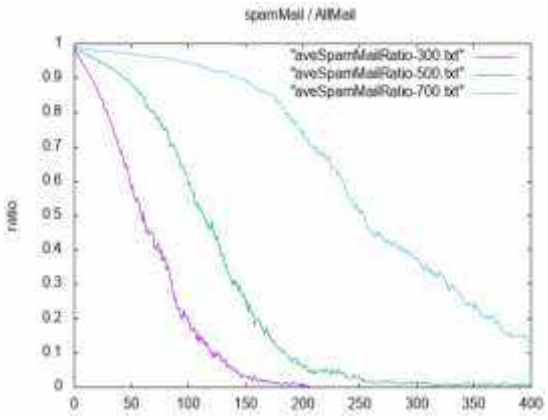
Hình 6 cũng cho thấy tỷ lệ thư rác đối với tất cả các email được gửi giảm một cách rõ ràng mặc dù tốc độ giảm này khác nhau cho một trong ba loại giá trị ban đầu của MSC.



Hình 6. *Kết quả mô phỏng ($M \subset$ 980, 1000, 1020)*

Mô phỏng tiếp theo được thực hiện 100 lần cho một trong ba số Spammer, thỏa mãn (M = 1000) như Hình 7 cho thấy sự thay đổi của giá trị trung bình thông qua một trên 100 mô phỏng với ba điều kiện ($S \subset$ 300, 500, 700).

Hình 7 cũng cho thấy tỷ lệ spam đối với tất cả các email được gửi giảm một cách rõ ràng, mặc dù tốc độ giảm này khác nhau cho một trong số ba loại lợi nhuận mà Spammer thu về.



Hình 7. *Kết quả mô phỏng (S ⊂ 300, 500, 700)*

4. Kết luận

Kết quả mô phỏng cho thấy $SAGA_{BC}$ có thể ngăn chặn thư rác một cách hiệu quả hơn các phương pháp ngăn chặn thư rác truyền thống. Bởi vì việc ngăn chặn thư rác diễn ra trong cả máy chủ gửi và bộ lọc của máy chủ nhận. Hơn nữa cũng có những lợi thế khác biệt trong việc sử dụng $SAGA_{BC}$ như sau:

- Ngay cả khi máy chủ gửi của người dùng giống như của Spammer, $SAGA_{BC}$ có thể ngăn chặn tấn công spam vì $SAGA_{BC}$ xác định xem một email là thư rác hoặc có tính hợp pháp hay không trong mỗi tài khoản email.

- Ngay cả khi Spammer chuyển sang một máy chủ gửi khác, $SAGA_{BC}$ sẽ ngăn ngừa Spammer thực hiện điều này trừ khi Spammer mua lại MSC.

- Vì email đến (nhận được) được trả phí MSC bởi ví của người gửi, máy chủ nhận và máy nhận không cần xem xét tới nội dung của một email như vậy sẽ có một lượng tải (workload) nhỏ.

- Người gửi email có sự đảm bảo rằng những tin nhắn sẽ không bị phân loại giống như thư rác miễn là có sự trả phí MSC.

Kết quả mô phỏng cho thấy rằng tấn công spam sẽ giảm xuống khi người dùng gửi email sử dụng $SAGA_{BC}$ khi đó sẽ có sự bảo toàn như một công cụ bảo vệ.$SAGA_{BC}$ đã tạo ra những bất lợi cho Spammer, Spammer đương nhiên sẽ không sử dụng nó. Tuy nhiên, với người dùng thông thường muốn đảm bảo rằng các email mà họ nhận được đã trả phí MSC thì luôn là email thật, không phải spam email.

TÀI LIỆU THAM KHẢO

[1]. Jae Yeon Jung, Emil sit, "An empirical study of spam traffic and the use of DNS Black Lists", *ACM SIGCOMM Internet Measurement Conferences 2010, Melbourne, Australia*, pp. 370-375, 2010.

[2]. A. K. M. Meera, "Cryptocurrencies From Islamic Perspectives: The Case Of Bitcoin", *Buletin Ekonomi Moneter Dan Perbankan*, Vol. 20, No. 4, pp. 443-460, 2018.

[3]. Keizer SoZe, *Cryptocurrencies and Blockchain Technology*, Sabi Shepherd Ltd, USA, 2017.

[4]. Calton Pu, Steve webb, "Observed trends in spam construction techniques: A case study of spam evolution", *CEAS 2006, California, USA*, pp. 104-112.

[5]. Dhinaharan Nagamalai, Cynthia.D, Jae Kwang Lee, "A Novel Mechanism to defend DDoS Attacks caused by spam", *International Journal of Smart Home*, Vol. 1, No. 2, pp 83-96, 2007.

[6]. J. Herbert and A. Litchfield, "A Novel Method for Decentralised Peer-to-peer Software License Validation Using Cryptocurrency Blockchain Technology", ACSC 2015, Sydney-Australia, Vol. 27.