(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0053942**

(51)[2019.01] G08B 13/00

(13) **B**

(21) 1-2020-04910

(22) 26/08/2020

(45) 25/11/2025 452

(43) 25/01/2022 406A

(73) Công ty Cổ phần Onyx Việt Nam (VN)
Số 121 Phố Vương Thừa Vũ, Phường Khương Trung, Quận Thanh Xuân, Thành Phố Hà Nội

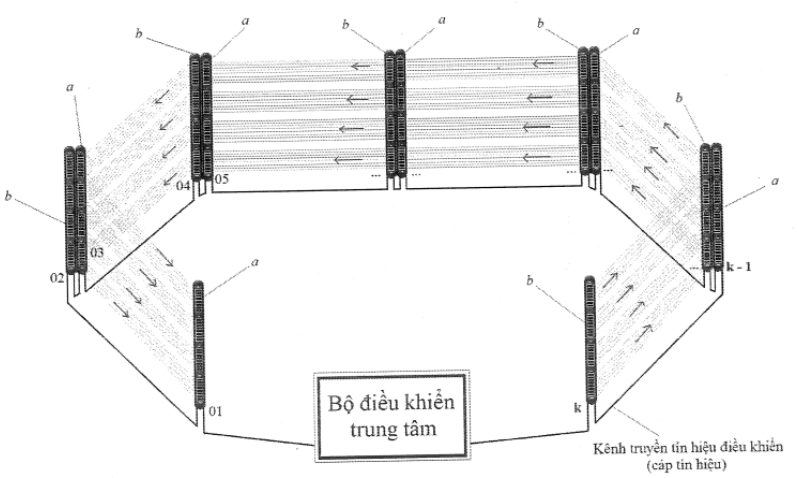
(72) Nguyễn Khương Tuấn (VN); Trần Tiến Trung (VN).

(54) PHƯƠNG PHÁP PHÁT HIỆN XÂM NHẬP SỬ DỤNG HỆ MÃ HÓA XUNG VÀ HỆ THỐNG HÀNG RÀO ĐIỆN TỬ THÔNG MINH SỬ DỤNG PHƯƠNG PHÁP NÀY

(21) 1-2020-04910

(57) Sáng chế đề xuất phương pháp phát hiện xâm nhập bằng cách sử dụng chùm tia mã hóa phát xung theo các chu trình liên tiếp, trong đó, ở mỗi mắt xích gồm các cặp đèn thu/phát, đèn phát phát tia hồng ngoại hoặc laser truyền dữ liệu được mã hóa từ cột phát sang đèn thu trên cột thu dưới dạng xung mảnh để tạo thành một mạng lưới tia mã hóa. Khi có tấn công bằng hình thức rọi đèn liên tục vào đèn thu hoặc có vật cắt ngang mạng lưới tia, hệ thống sẽ nhận biết và phát tín hiệu cảnh báo về trung tâm. Sáng chế còn có thể xác định một cách tương đối kích thước đối tượng xâm nhập và cách thức xâm nhập (bằng cách vượt qua hàng rào hay bằng tấn công chiếu tia). Sáng chế cũng đề xuất hệ thống hàng rào thông minh sử dụng các phương pháp này.

Hình 1.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp phát hiện xâm nhập sử dụng hệ mã hóa xung và hệ thống hàng rào điện tử thông minh sử dụng các phương pháp này. Phương pháp phát hiện xâm nhập và hàng rào điện tử thông minh được đề xuất theo sáng chế này có thể được áp dụng trong các lĩnh vực kỹ thuật: hàng rào chống trộm, hệ thống cảnh báo xâm nhập cho hộ gia đình hay các đơn vị có chu vi cần bảo vệ rộng lớn như nhà máy, xí nghiệp, khu công nghiệp, trang trại, kho bãi, các cơ quan, trụ sở có nhu cầu an ninh bảo mật cao hay thậm chí là đường biên giới.

Tình trạng kỹ thuật của sáng chế

Các thiết bị chống trộm, phát hiện xâm nhập hiện nay, cụ thể là các loại hàng rào chống trộm điện tử, thường sử dụng công nghệ chùm tia hồng ngoại hoặc laser để phát hiện xâm nhập. Hệ thống này phát tín hiệu cảnh báo xâm nhập khi có vật thể chắn ngang chùm tia nối hai cột của hàng rào, khiến tín hiệu không tới được đèn thu. Phương pháp sử dụng chùm tia hồng ngoại hoặc laser trong tình trạng kỹ thuật đã biết có cơ chế hoạt động đơn giản là thu, phát chùm tia không chứa dữ liệu mã hóa. Do đó, tồn tại lỗ hổng bảo mật cho phép sự xâm nhập bằng cách sử dụng chùm tia giả mạo chiếu liên tục vào đèn thu để đánh lừa hệ thống hàng rào, bằng cách đó, dù cho có sự xâm nhập nhưng hệ thống vẫn không phát hiện ra do đèn thu vẫn nhận được chùm tia tương tự như chùm tia do đèn phát phát ra.

Hơn nữa, hệ thống hàng rào điện tử trong trạng thái kỹ thuật đã biết dù có phát hiện xâm nhập thì cũng không thể xác định được kích thước của vật thể xâm nhập.

Do đó, có nhu cầu để giải quyết vấn đề nêu trên, và sáng chế phương pháp đề xuất phương pháp phát hiện xâm nhập bằng cách sử dụng chùm tia laser hoặc hồng ngoại, khác biệt ở chỗ chùm tia có chứa thông tin mã hóa khiến cho cách "đánh lừa" hệ thống bằng cách chiều tia giả mạo vào đèn thu không thể thực hiện được, bằng cách đó nâng cao hiệu quả phát hiện xâm nhập. Sáng chế cũng đề xuất hệ thống hàng rào thông minh sử dụng phương pháp này.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là phát hiện hành vi xâm nhập một cách triệt để, chống lại các phương pháp bẻ khóa hàng rào từ tội phạm công nghệ cao mà các phương pháp và thiết bị chống trộm hiện tại chưa xử lý được.

Để đạt được mục đích nêu trên, sáng chế đề xuất phương pháp xác định xâm nhập sử dụng hệ mã hóa xung và hệ thống hàng rào điện tử thông minh sử dụng các phương pháp này.

Phương pháp phát hiện xâm nhập sử dụng hệ mã hóa xung theo sáng chế này bao gồm:

Chu trình thứ nhất (chu trình trước)

Bước 1: Khi hàng rào được kích hoạt, bộ điều khiển trung tâm sẽ gửi gói tin kiểm tra đến tất cả các cột theo phương thức chuyển tiếp.

Gói tin kiểm tra được chuyển đến cột đầu tiên có số thứ tự là 01, cột 01 sẽ ghi nhận địa chỉ của mình là 01 rồi hồi đáp bằng gói tin kiểm tra Ack 01 cho bộ điều khiển trung tâm, đồng thời chuyển tiếp gói tin kiểm tra cho cột tiếp theo 02; tương tự, cột 02 sẽ phản hồi cho bộ điều khiển trung tâm và chuyển tiếp gói tin kiểm tra sang cột 03; ...cột cuối cùng trong hệ thống là cột k cũng sẽ hồi đáp về bộ điều khiển trung tâm qua các cột trước đó, đồng thời trực tiếp chuyển tiếp gói tin kiểm tra về bộ điều khiển trung tâm.

Nếu cột nào không phản hồi hoặc không chuyển tiếp gói tin, bộ điều khiển trung tâm sẽ ghi nhận cột đó là cột lỗi và gửi gói tin theo hướng ngược lại; khi nhận được gói tin truyền theo hướng ngược lại, các cột cũng phản ứng giống như trong trường hợp gói tin truyền theo chiều thuận cho đến khi gặp cột không phản hồi, và ghi nhận cột đó là cột lỗi.

Đoạn hàng rào được xác định bởi hai cột lỗi (không phản hồi) sẽ được ghi nhận là đoạn hàng rào bị lỗi, trong khi phần còn lại của hàng rào vẫn hoạt động bình thường.

Bước 2: Bộ điều khiển trung tâm tính toán và gửi một gói tin tới tất cả các cột trong hệ thống, gồm các thông tin về Kỷ nguyên thời gian (epoch); Seed256; và PIN256 trong trường hợp người dùng thiết lập lại mã PIN.

Bước 3: Trên cơ sở gói tin tại Bước 2, bộ vi xử lý trên các cột tính toán tham số Cypherkey và lưu trữ để sử dụng trong tất cả các chu trình thuộc chiều dài kỷ nguyên, theo đó: CypherKey = SHA256 (MasterKey, PIN256, Seed256), đồng thời, bộ vi xử lý trên cột thu của mỗi mắt xích sẽ sản sinh ra một câu đố bảo mật với dung lượng 32 bit (token32) được sinh ra một cách ngẫu nhiên và truyền câu đố đó cho cột phát qua kênh truyền tín hiệu điều khiển.

Bước 4: Bộ vi xử lý trên cột thu và cột phát cùng tính toán kết quả **h** dựa trên tham số CypherKey và câu đố bảo mật token 32 tại Bước 3 theo công thức:

h = Hash256(token32)=SHA256(CypherKey, token32)

Bước 5: Kết quả **h** tính được tại Bước 4 sẽ được cột phát truyền đến cột thu thông qua lưới tia hồng ngoại hoặc laser theo nguyên tắc truyền từng bit cho đến khi truyền hết toàn bộ kết quả; trong đó, đèn thứ nhất trên cột phát sẽ phát 1 bit tín hiệu đến đèn thu tương ứng trên cột thu; sau đó, lần lượt các đèn tiếp theo, mỗi đèn sẽ phát 1 bit tín hiệu; khi đèn cuối cùng phát 1 bit tín hiệu thì quay lại đèn thứ nhất và quy trình được lặp lại cho đến khi toàn bộ kết quả tính toán tại Bước 4 đã được truyền hết sang cho cột thu.

Bước 6: Bộ vi xử lý trên cột thu tiếp nhận thông tin truyền đến từ cột phát, so sánh dữ liệu nhận được từ cột phát thông qua các đèn phát với kết quả mà bộ vi xử lý trên cột thu tính được bằng cách so sánh theo từng bit:

- Nếu kết quả nhận được theo từng bit từ cột phát trùng với kết quả mà bộ vi xử lý trên cột thu tính được, hệ thống sẽ coi là an toàn;

- Nếu kết quả nhận được từ cột phát theo từng bit sai khác với kết quả mà bộ vi xử lý trên cột thu tính được, bit đó sẽ được coi là bit lỗi, khi đó hệ thống giám sát lỗi sẽ đếm từng bit lỗi để đưa ra kết luận lỗi là do nhiễu, do các vật thể nhỏ xâm nhập, do đó không cảnh báo; hoặc do bị tấn công theo kiểu chiếu tia hoặc do có đối tượng xâm nhập, do đó phát tín hiệu cảnh báo.

Kết thúc chu trình thứ nhất, chuyển sang chu trình tiếp theo.

Chu trình tiếp theo

Chu trình tiếp theo sẽ khởi động ở một thời điểm ngẫu nhiên sao cho kết quả **h** ở chu trình tiếp theo được tính toán và lưu trữ trong tại cột thu và cột phát trước khi chu trình liền trước kết thúc, trong đó:

- Nếu việc thực hiện toàn bộ chu trình trước vẫn nằm trong chiều dài của kỷ nguyên thì chu trình tiếp theo bắt đầu lại từ Bước 3: theo đó, CypherKey vẫn được giữ nguyên; trong mỗi mắt xích, cột thu sẽ gửi tới cột phát một câu đố bảo mật dung lượng 32 bit (token32) ngẫu nhiên mới qua kênh truyền tín hiệu điều khiển; các bước sau vẫn được tiến hành tuần tự như ở chu trình đầu tiên;

- Nếu việc thực hiện chu trình trước đã đi hết chiều dài của kỷ nguyên thì chu trình trước vẫn tiếp tục thực hiện đến cuối cùng như bình thường; khi hết chiều dài kỷ nguyên, chu trình tiếp sẽ bắt đầu lại ở Bước 2: theo đó, Bộ điều khiển trung tâm gửi gói tin mới có chứa thông tin về Seed256 mới cho tất cả các cột tính lại CypherKey để thay thế cho Cypherkey trong chu trình trước; đồng thời, cột thu vẫn gửi cho cột phát trong một mắt xích một câu đố bảo mật dung lượng 32 bit (token32) mới qua đường truyền cáp; các bước sau vẫn được tiến hành tuần tự như ở chu trình đầu tiên.

Trong một phương án, sau khi Bước 4 kết thúc, kết quả tính toán **h** đã được cặp cột thu và cột phát xác định và truyền tới cột thu (bước 5) để cột thu so sánh kết quả nhận được với kết quả do bộ vi xử lý của cột thu tự tính (bước 6) và hoàn tất một tiểu quy trình.

Khác biệt ở chỗ, hệ thống chưa bắt đầu chu trình tiếp theo ngay mà bắt đầu một tiểu quy trình tiếp theo, theo đó, bộ vi xử lý của cột thu và cột phát sẽ biến đổi kết quả **h** thành một kết quả $\mathbf{h}^{(1)}$ sử dụng sàng hoán vị CR32 theo công thức sau:

$$h^{(1)} = CR32.Swap(h)$$

Sau đó, kết quả tính toán $\mathbf{h}^{(1)}$ được truyền tới cột thu (bước 5) để cột thu so sánh kết quả nhận được với kết quả do bộ vi xử lý của cột thu tự tính (bước 6), kết thúc tiểu quy trình tiếp theo.

Tiểu quy trình nêu trên sẽ được lặp lại **n** lần, theo đó, kết quả $\mathbf{h}^{(n)}$ được tính bằng cách hoán vị bằng sàng hoán vị CR32 đối với kết quả **h** liền trước đó, tức là $\mathbf{h}^{(n-1)}$.

Trong một phương án ưu tiên, **n** nằm trong khoảng từ 200 đến 2000.

Trong một phương án ưu tiên khác, trong đó, **n** bằng 256.

Trong một phương án, nếu trong mỗi phiên truyền, số lượng bit 1 nhiều hơn hoặc bằng số lượng bit 0 được truyền trong phiên thì việc truyền diễn ra bình thường; nếu số lượng bit 1 ít hơn số lượng bit 0 được truyền trong phiên thì quy trình "đảo bit" đối với lượng dữ liệu được truyền trong phiên truyền sẽ được kích hoạt sao cho lượng bit 1 trong mỗi phiên truyền luôn lớn hơn lượng bit 0.

Trong một phương án, cứ sau một khoảng thời gian định trước, các cột sẽ gửi một gói tin điểm danh tới bộ điều khiển trung tâm để điểm danh; nếu hết thời gian định trước mà bộ điều khiển trung tâm không nhận được gói tin điểm danh của cột nào thì hệ thống sẽ ghi nhận cột đó bị lỗi và báo động.

Trong một phương án ưu tiên, thời gian định trước để gửi gói tin điểm danh là 10 giây.

Trong một phương án, kết quả **h** tính được tại Bước 4 sẽ được đồng thời truyền tới nhiều mô đun trong cùng một mắt xích, mỗi mô đun có nhiều cặp đèn thu/phát.

Trong phương án ưu tiên, mỗi mô đun có 8 cặp đèn thu/phát.

Trong một phương án, việc truyền dữ liệu bằng lưới tia sử dụng kỹ thuật xung mảnh 1%.

Trong một phương án, các đèn phát trên cột phát luân phiên sử dụng hai hoặc nhiều tần số sóng mang xen kẽ nhau. Trong một phương án ưu tiên, các đèn phát trên cột phát sử dụng luân phiên hai tần số 38khz và 56khz xen kẽ nhau.

Trong một phương án, các gói tin được truyền trên kênh truyền tín hiệu điều khiển được mã hóa bằng hàm EncryptData và được xác thực bằng hàm Hash32.

Trong một phương án, sáng chế cũng đề xuất phương pháp xác định kích thước đối tượng xâm nhập và cách thức xâm nhập, bao gồm:

Bước 1: Bộ vi xử lý trên cột thu so sánh dữ liệu nhận được từ cột phát với dữ liệu cột thu tính được, nếu dữ liệu được truyền của mỗi cặp đèn thu/phát không khớp nhau, cột thu sẽ ghi nhận đó là một lỗi tại vị trí đèn thu/phát tương ứng;

Bước 2: Bộ vi xử lý trên cột thu đánh giá lỗi, trong đó:

- Nếu dữ liệu mà cột thu nhận được từ cột phát trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được thì hệ thống ghi nhận là hoạt động bình thường;

- Nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được (có lỗi) nhưng thời gian tồn tại lỗi liên tiếp tại mỗi vị trí ngắn hơn giá trị định trước thì hệ thống ghi nhận là nhiễu và không phát tín hiệu cảnh báo;

- Nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được (có lỗi), trong đó, một hoặc nhiều đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 1 trong thời gian dài hơn giá trị định trước thì hệ thống ghi nhận là bị tấn công bằng phương pháp chiếu tia và phát tín hiệu cảnh báo;

- Nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được (có lỗi), trong đó, một hoặc nhiều đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 0 trong thời gian dài hơn giá trị định trước thì hệ thống ghi nhận là có vật xâm nhập qua hàng rào và hệ thống sẽ tính toán để ước lượng chiều cao S và chiều sâu D tương đối của vật xâm nhập:

Nếu vật có chiều cao và/hoặc chiều sâu lớn hơn giá trị định trước thì hệ thống sẽ phát tín hiệu báo động, kèm theo giá trị chiều cao và chiều sâu ước tính của vật đã xâm nhập.

Nếu vật có chiều cao thấp hơn và chiều sâu nhỏ hơn giá trị định trước thì hệ thống sẽ coi đó là các vật xâm nhập nhỏ không đáng quan tâm, không phát tín hiệu cảnh báo.

Trong một phương án, giá trị thời gian ghi nhận lỗi định trước là 5,5 mili giây.

Trong một phương án, tín hiệu cảnh báo được truyền trên kênh truyền tín hiệu điều khiển được xác thực bằng hàm Hash32.

Sáng chế cũng đề xuất Hệ thống hàng rào thông minh sử dụng phương pháp xác định xâm nhập và phương pháp xác định kích thước đối tượng xâm nhập và cách thức xâm nhập nêu trên, trong đó, hệ thống bao gồm:

(i) Bộ điều khiển trung tâm, kết nối nối tiếp với tất cả các cột trong hệ thống bằng kênh truyền tín hiệu điều khiển theo một vòng tròn khép kín, trong đó, bộ điều khiển trung tâm kết nối với cột thu 01, cột thu 01 sẽ được nối nối tiếp với cột phát 02 … cột phát cuối cùng k sẽ nối với cột thu liền trước k-1 và nối trở lại vào bộ điều khiển trung tâm bằng kênh truyền tín hiệu điều khiển;

Trên cột thu 01 sẽ chỉ có đèn thu; trên cột 02 chỉ có đèn phát; cột tiếp theo chỉ có đèn thu … đến cột cuối cùng chỉ có đèn phát;

(ii) Mỗi cặp cột, gồm cột thu a và cột liền kề b là cột phát tạo thành một mắt xích của hệ thống hàng rào điện tử, trong đó:

- trên cột thu a có chứa mô đun đèn thu tín hiệu laser hoặc hồng ngoại, mỗi mô đun gồm nhiều đèn, được bố trí dọc thân cột hướng về hướng cột phát liền kề b sao cho tương ứng với mỗi đèn phát trên cột phát liền kề b sẽ có một đèn thu trên cột thu trước đó a; trên cột thu a còn có bộ vi xử lý chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước và so sánh với tín hiệu mã hóa nhận được từ đèn thu; và

- trên cột phát liền kề b với một cột thu a có chứa mô đun đèn phát tín hiệu laser hoặc hồng ngoại, mỗi mô đun gồm nhiều đèn được bố trí dọc thân cột hướng về cột thu liền trước đó a sao cho tương ứng mỗi đèn thu sẽ có một đèn phát; trên cột phát liền kề b có bộ vi xử lý chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước và gửi kết quả giải mã thông qua đèn phát tới đèn thu;

(iii) kênh truyền tín hiệu điều khiển để truyền "câu đố", chính là token32, từ cột thu tới cột phát trong cùng một mắt xích;

trong đó, cột phát liền kề b sẽ đặt sát và úp lưng vào cột thu tiếp theo a;

trong đó, công thức cài đặt trước trong phần mềm nhúng để giải mã của bộ vi xử lý của cột thu trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã của bộ vi xử lý của cột phát.

Trong một phương áp, cột phát liền kề b và cột thu tiếp theo a được ghép vào với nhau thành một cột duy nhất.

Trong một phương án, kênh truyền tín hiệu điều khiển là cáp tín hiệu.

Trong một phương án, trên cặp cột thu a và cột phát b tại mỗi mắt xích có nhiều mô đun, mỗi mô đun gồm nhiều đèn thu/phát. Trong một phương án ưu tiên, số đèn thu/phát của mỗi mô đun là 8.

Mô tả vắn tắt các hình vẽ

Hình 1. là sơ đồ khối minh họa khái quát hệ thống hàng rào điện tử thông minh theo phương án của sáng chế.

Hình 2. là hình minh họa một mắt xích trong hệ thống hàng rào điện tử thông minh gồm một cột thu và một cột phát với 4 mô đun, mỗi mô đun có 8 đèn, theo một phương án của sáng chế.

Hình 3. là lưu đồ minh họa cách thức hoạt động cơ bản của hệ thống hàng rào điện tử thông minh theo phương án của sáng chế.

Hình 4. là lưu đồ minh họa việc phóng đại kết quả h trong n lần bằng cách áp dụng sàng hoán vị CR32.

Hình 5. là hình minh họa phương pháp phát tia sử dụng kỹ thuật xung mảnh 1% (ThinPulse) của sáng chế so với phương pháp phát tia sử dụng tần số sóng mang có độ rộng xung 50%.

Hình 6. là phương pháp phát hiện kích thước đối tượng xâm nhập và cách thức xâm nhập theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Sau đây, sáng chế sẽ được mô tả chi tiết với các phương án. Phương án thực hiện sáng chế sau đây được đưa ra làm ví dụ nhằm mục đích bộc lộ toàn bộ sáng chế với người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng. Tuy nhiên, các ví dụ không làm giới hạn sáng chế. Sáng chế bao gồm tất cả các biến thể, các phép tương đương và các lựa chọn thay thế thuộc tinh thần và phạm vi của sáng chế.

Cần phải hiểu rằng, nếu không có chỉ dẫn khác, các thuật ngữ được dùng trong bản mô tả nên được hiểu là đã được người có hiểu biết trung bình về lĩnh vực kỹ thuật này hiểu rõ và sử dụng rộng rãi. Các thuật ngữ được sử dụng trong bản mô tả sáng chế là nhằm mục đích mô tả các phương án cụ thể và không phải là để giới hạn. Các thuật ngữ chỉ các tham số, hàm số, thuật toán, hay đường truyền, ví dụ như CypherKey, PIN, Seed, Hash32, token32… được dùng để phân biệt các tham số, hàm số, thuật toán và các đường truyền khác nhau và không làm giới hạn sáng chế. Các mô tả đã biết hoặc có thể làm lu mờ các điểm quan trọng của sáng chế sẽ được bỏ qua.

Để hỗ trợ cho việc làm rõ bản chất của sáng chế, trong Bản mô tả này có sử dụng một số thuật ngữ như sau:

1. Kỷ nguyên thời gian (epoch): epoch là đơn vị đo thời gian do hệ thống tự thiết lập ngẫu nhiên và có độ dài không cố định, có thể là một ngày tới một tháng. Độ dài của epoch (EpochLength) được tính như sau:

*EpochLength = 1 ngày + random(30*24)*giờ*

Khi hết thời gian EpochLength, hệ thống tự quy định lại và bắt đầu epoch mới. Việc độ dài epoch là ngẫu nhiên và do hệ thống tự quyết định thời điểm chuyển epoch mới cũng khiến cho các phương pháp tấn công dự báo trở nên khó khăn.

2. Hàm SHA256: là một mã một chiều bất đối xứng được coi là an toàn và được sử dụng rộng rãi cho các ứng dụng bảo mật hiện nay.

3. Hàm băm hash256: là một mã một chiều bất đối xứng được xây dựng từ hàm SHA256, có công thức như sau:

hash256 = SHA256([CypherKey, data])

Trong đó, CypherKey là tham số bí mật; data là thông tin cần băm. Tham số data và hash256 có thể công khai nhưng không thể truy tìm ngược lại CypherKey từ data và hash256. Trong khi đó, ứng với mỗi tham số data sẽ tạo ra một kết quả hash tương ứng, do đó không thể tính ra được kết quả hash nếu không biết CypherKey.

4. Hàm Hash32: Là một mã một chiều bất đối xứng, được tính toán bằng cách lấy 32 bit đầu tiên của hàm hash256 theo công thức như sau:

Hash32 = hash256([CypherKey, data]) [0..31]

Hàm Hash32 được sử dụng để xác thực dữ liệu truyền qua đường truyền cáp vật lý giữa các cột của hàng rào (PackTransfer).

5. Hàm EncryptData: Là một mã hai chiều bất đối xứng, sử dụng mã AES256, là một mã hai chiều bất đối xứng có độ an toàn rất cao, được tính toán theo công thức như sau:

EncryptData = AES256(CypherKey, data)

Trong đó, CypherKey được dữ bí mật, EncryptData có thể công khai nhưng việc tìm ngược lại data gần như là không thể vì cần hàng ngàn năm với siêu máy tính hiện tại để thực hiện tấn công mã AES256.

6. Tham số bí mật (CypherKey) là một dãy dài 256 bit được tính theo công thức như sau:

CypherKey = SHA256 (MasterKey, PIN256, Seed256)

Trong đó :

- MasterKey là khóa chính dài 256 bit. Đây là tham số được nhà sản xuất hàng rào định nghĩa và được bộ điều khiển trung tâm và các cột lưu giữ trong bộ nhớ NVM của chip xử lý chính (MCU) dưới sự bảo vệ bằng phần cứng chống đọc ra từ bên ngoài có độ an toàn cao.

- PIN256 là gói dữ liệu gồm 32 byte (256 bit), lưu trữ mật khẩu do người dùng đặt (mã PIN) với độ dài tối đa là 60 chữ số bằng mã nhị phân BCD 4 bit cho mỗi chữ số từ 0 - 9. Cụ thể, trong 256 bit, 16 bit được dùng để lưu chiều dài thực và 240 bit được dùng để lưu các chữ số BCD. Mỗi khi hệ thống hàng rào khởi động hoặc người dùng thay đổi mã PIN, bộ điều khiển trung tâm sẽ gửi gói tin bảo mật PIN352 đến tất cả các cột của hàng rào để sử dụng làm một phần cho tham số bí mật CypherKey trong suốt kỷ nguyên hoạt động. PIN256 được mã hóa và bảo mật trong bộ nhớ NVM của bộ điều khiển trung tâm và các cột. Tuy nhiên, sáng chế không bị giới hạn tại đây và số byte của PIN256 có thể thay đổi.

- Seed256 là gói dữ liệu 32 byte (256 bit), lưu trữ một chuỗi 32 chữ số gọi là Seed, được tạo ra từ việc hoán vị ngẫu nhiên chuỗi số gồm 32 số tự nhiên từ 0 - 31. Mỗi chữ số của Seed được lưu trong mã nhị phân 5 bit. Do đó, Seed có thể được coi là Seed256. Mỗi khi bắt đầu một kỷ nguyên (epoch), bộ điều khiển trung tâm tạo ra Seed mới bằng cách triển khai sàng hoán vị

ngẫu nhiên CR32 gồm 32 byte đối với các phần tử có giá trị từ 0 - 31 (CR32[0..31]). Để triển khai sàng hoán vị CR32, sáng chế sử dụng hàm CR32.Generate, CR32.Swap. Seed256 chính là CR32 được tạo ra, gồm 32 byte (mỗi byte gồm 8 bit) tổng cộng 256 bit. Gói tin Seed256 được bộ điều khiển trung tâm gửi bảo mật đến tất cả các cột của hàng rào để sử dụng làm một thành phần cho tham số bí mật CypherKey trong suốt kỷ nguyên đó. Seed256 được mã hóa và bảo mật trong bộ nhớ NVM của bộ điều khiển trung tâm và các cột. Tuy nhiên, sáng chế không bị giới hạn tại đây và số byte của Seed256 có thể thay đổi.

CypherKey được sử dụng làm khóa bí mật để xác thực dữ liệu trao đổi giữa các cột trong mỗi phiên bằng hàm hash256 và mã hóa dữ liệu trên đường truyền mạng bằng hàm AES256. Đồng thời, CypherKey được dùng để xác thực các gói tin cảnh báo và các gói tin thông báo trạng thái bình thường mà các cột gửi cho bộ điều khiển trung tâm để ngăn chặn các gói tin giả mạo.

Tính chất của CypherKey là có độ dài cố định, tốc độ mã hóa đồng đều giống nhau trong mỗi phiên làm việc giữa các cột. Hơn nữa, do được cấu tạo từ ba thành phần: mã của nhà sản xuất (MasterKey), mã của người dùng (PIN256) và mã ngẫu nhiên thay đổi theo kỷ nguyên thời gian chỉ có hệ thống biết (Seed256), bất kỳ ai không nắm được đầy đủ các thành phần này của CypherKey đều không thể giải các câu đố mã hóa truyền giữa các cột, ngay cả người lập trình cho hàng rào cũng không thể bẻ khóa.

7. Hàm CR32 được xây dựng theo cách:

- Bắt đầu từ phần tử thứ i = 0; Gán tập đánh dấu V = rỗng
- Gieo ngẫu nhiên phần tử thứ i:
    - Gieo ngẫu nhiên r = random(0..31) sao cho r không thuộc V, nếu r thuộc V thì gieo lại lần khác cho đến khi r không thuộc V.
    - Gán CR32[i] := r ; và bổ sung r vào tập đánh dấu V.
- Tăng i thêm 1: i := i + 1; nếu i < 32 thì tiếp tục bước gieo ngẫu nhiên phần tử thứ i

8. Hàm CR32.Swap(data[32]) được xây dựng theo cách:

- Data là một dãy 32 byte dữ liệu

Với mỗi phần tử thứ i của data, thay thế bằng phần tử thứ CR32[i] của data; tức là hoán vị 32 phần tử trong data theo thứ tự mô tả trong CR32.

9. Token32: là một số được hệ thống sinh ra ngẫu nhiên, có dung lượng 32 bit được dùng để trao đổi câu đố giữa hai cột liền kề, được tính như sau:

token32 = random(0 .. $2^{32} - 1$)

Gói tin chứa tham số này được cột thu gửi cho cột phát qua đường truyền cáp và không được chuyển tiếp. Mỗi khi một mắt xích (gồm một cặp cột thu và cột phát hướng về nhau) truyền hết thông tin trong một quy trình, cột thu gửi sang cột phát của mắt xích đó một gói tin Token, chứa token32. Dựa trên token32 mới, bộ vi xử lý trên cột thu và cột phát của mắt xích sẽ tính ra kết quả **h** có dung lượng 256 bit để truyền từ cột phát sang cột thu bằng đường truyền tia trong quy trình mới.

Vì token32 là số ngẫu nhiên 32 bit có thể công khai, nên không cần mã hóa; nhưng được truyền đi trong gói tin có xác thực nhằm tránh giả mạo.

Tham chiếu tới Hình 1. là sơ đồ khối minh họa khái quát hệ thống hàng rào điện tử thông minh theo phương án của sáng chế.

Hệ thống hàng rào điện tử thông minh theo sáng chế này gồm các thành phần chính như sau:

(i) Bộ điều khiển trung tâm, kết nối nối tiếp với tất cả các cột trong hệ thống bằng kênh truyền tín hiệu điều khiển theo một vòng tròn khép kín, trong đó, bộ điều khiển trung tâm kết nối với cột thu 01, cột thu 01 sẽ được nối nối tiếp với cột phát 02 … cột phát cuối cùng k sẽ nối với cột thu liền trước k-1 và nối trở lại vào bộ điều khiển trung tâm bằng kênh truyền tín hiệu điều khiển. Kênh truyền tín hiệu điều khiển có thể là cáp tín hiệu, hoặc đường truyền vô tuyến khác.

Trên cột thu 01 sẽ chỉ có đèn thu; trên cột 02 chỉ có đèn phát; cột tiếp theo chỉ có đèn thu … đến cột cuối cùng chỉ có đèn phát;

(ii) Mỗi cặp cột, gồm cột thu a và cột liền kề b hướng về nhau là cột phát tạo thành một mắt xích của hệ thống hàng rào điện tử, cột phát liền kề b sẽ đặt sát và úp lưng vào cột thu tiếp theo a. Cột thu tiếp theo a sẽ hợp với cột thu liền kề tiếp sau đó b thành một mắt xích tiếp theo. Bằng cách đó, hàng rào có thể kéo dài không giới hạn.

- Trên cột thu a có chứa mô đun đèn thu tín hiệu laser hoặc hồng ngoại, mỗi mô đun gồm nhiều đèn, được bố trí dọc thân cột hướng về hướng cột phát liền kề b sao cho tương ứng với mỗi đèn phát trên cột phát liền kề b sẽ có một đèn thu trên cột thu trước đó a; trên cột thu a còn có bộ vi xử lý chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước và so sánh với tín hiệu mã hóa nhận được từ đèn thu.

- Trên cột phát liền kề b với một cột thu a có chứa mô đun đèn phát tín hiệu laser hoặc hồng ngoại, mỗi mô đun gồm nhiều đèn được bố trí dọc thân cột hướng về cột thu liền trước đó a sao cho tương ứng mỗi đèn thu sẽ có một đèn phát; trên cột phát liền kề b có bộ vi xử lý chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước và gửi kết quả giải mã thông qua đèn phát tới đèn thu.

(iii) kênh truyền tín hiệu điều khiển để truyền "câu đố", chính là token32, từ cột thu tới cột phát trong cùng một mắt xích;

Trong đó, công thức cài đặt trước trong phần mềm nhúng để giải mã của bộ vi xử lý của cột thu trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã của bộ vi xử lý của cột phát. Cột thu tiếp theo a với cột phát liền kề b được đặt sát nhau và úp lưng vào nhau.

Trong một phương áp của sáng chế, cột phát liền kề b và cột thu tiếp theo a được ghép vào với nhau thành một cột duy nhất có cả hai chức năng thu và phát ở hai mặt của cột. Tuy nhiên, mặc dù hai cột này có hợp nhất với nhau nhưng trên thực tế, nó vẫn hoạt động như hai cột có chức năng thu/phát độc lập như mô tả ở trên.

Hình 2. là hình minh họa một mắt xích trong hệ thống hàng rào điện tử thông minh gồm một cột thu và một cột phát theo phương án của sáng chế.

Trong một phương án, trên cặp cột thu a và cột phát b tại mỗi mắt xích có nhiều mô đun, mỗi mô đun gồm nhiều đèn thu/phát.

Nhiều đèn thu trên cột thu và nhiều đèn phát trên cột phát hợp thành một mô đun. Trong một phương án, số đèn thu và đèn phát trong một mô đun là 8. Trong một phương án ưu tiên khác, số đèn thu và đèn phát bố trí trên thân cột gồm nhiều mô đun đèn, mỗi mô đun có 8 đèn.

- Giữa cột thu và cột phát nối với nhau bằng một kênh truyền tín hiệu điều khiển dùng để truyền "câu đố", chính là token32, từ cột thu tới cột phát. Kênh truyền tín hiệu điều khiển có thể là cáp tín hiệu, hoặc đường truyền vô tuyến khác.

- Tất cả các cột trong hệ thống hàng rào đều được đồng bộ về thời gian.

Nhờ cấu trúc đoàn tàu khép kín, thông tin có thể được truyền từ bộ điều khiển trung tâm tới các cột theo hai hướng: hướng thuận (theo chiều kim đồng hồ) và hướng ngược (ngược chiều kim đồng hồ). Theo phương án của sáng chế, hướng truyền ưu tiên là hướng thuận. Khi sử dụng hướng ngược để truyền tin, phải lựa chọn thời điểm và đảm bảo rằng thời điểm truyền tin là an toàn và tránh va chạm với các gói tin truyền theo hướng thuận trên đường truyền. Để tránh va chạm, các khe thời gian có thể được định trước sao cho khi truyền theo hướng ngược các gói tin ngược không bị va chạm với gói tin theo hướng thuận trên đường truyền.

Với cách bố trí hệ thống như trên, khi gặp sự cố như mất điện, mất liên lạc hoặc đứt cáp giữa hai cột bất kỳ, bộ điều khiển trung tâm có thể phát hiện ra và báo cho người sử dụng. Khi đó, phần còn lại của hàng rào vẫn có thể hoạt động bình thường. Sáng chế có các gói tin báo hiệu cho phép tự động đánh địa chỉ các cột, thường xuyên cập nhật trạng thái hoạt động, cảnh báo xâm nhập, báo động. Đồng thời, sáng chế có các gói tin bảo mật truyền các dữ liệu tại thời điểm quan trọng, ví dụ thay đổi mã PIN, thay đổi Seed sau mỗi epoch.

Hình 3. là lưu đồ minh họa cách thức hoạt động cơ bản của hệ thống hàng rào điện tử thông minh theo phương án của sáng chế.

Sáng chế được đề xuất hoạt động theo các chu trình với các bước như sau:

Chu trình thứ nhất (chu trình trước)

Bước 1: Khi hàng rào được kích hoạt, bộ điều khiển trung tâm sẽ gửi gói tin kiểm tra đến tất cả các cột theo phương thức chuyển tiếp, gọi là gói tin Track.

Gói tin Track được chuyển đến cột đầu tiên có số thứ tự là 01, cột 01 sẽ ghi nhận địa chỉ của mình là 01 rồi hồi đáp bằng gói tin hồi đáp Ack 01 cho bộ điều khiển trung tâm, đồng thời chuyển tiếp gói tin kiểm tra cho cột tiếp theo 02. Tương tự, cột 02 sẽ phản hồi cho bộ điều khiển trung tâm và chuyển tiếp gói tin kiểm tra sang cột 03. Cột cuối cùng trong hệ thống là cột (k) cũng sẽ hồi đáp về bộ điều khiển trung tâm qua các cột trước đó, đồng thời trực tiếp chuyển tiếp gói tin kiểm tra về bộ điều khiển trung tâm. Như vậy, gói tin kiểm tra sẽ đi hết một vòng hàng rào khép kín. Kết thúc quá trình này, các cột được tự động đánh địa chỉ, và bộ điều khiển trung tâm vẽ được bản đồ kết nối giữa các cột theo từng địa chỉ.

Trong quá trình truyền gói tin kiểm tra, nếu gặp sự cố như cột không phản hồi, hoặc không thể chuyển tiếp gói tin, bộ điều khiển trung tâm sẽ ghi nhận cột đó là cột lỗi và gửi gói tin theo hướng ngược lại. Khi nhận được gói tin truyền theo hướng ngược lại, các cột cũng phản ứng giống như trong trước hợp gói tin truyền theo chiều thuận cho đến khi gặp cột không phản hồi, và ghi nhận cột đó là cột lỗi.

Đoạn hàng rào được xác định bởi hai cột lỗi (không phản hồi) sẽ được ghi nhận là đoạn hàng rào bị lỗi, trong khi phần còn lại của hàng rào vẫn hoạt động bình thường.

Trong một phương án của sáng chế, cứ sau một khoảng thời gian định trước, gọi là T_{check}, các cột sẽ gửi một gói tin tới bộ điều khiển trung tâm, gọi là gói tin điểm danh. Theo một phương án ưu tiên của sáng chế, $T_{check} = 10$ giây, theo đó, cứ mỗi 10 giây các cột lại điểm danh với bộ điều khiển trung tâm một lần. Nếu hết thời gian T_{check} mà bộ điều khiển trung tâm không nhận được gói tin điểm danh của cột nào thì hệ thống sẽ ghi nhận cột đó bị lỗi.

Trong khi chưa đến thời điểm điểm danh, nếu cột phát hiện ra lỗi hay báo động, lập tức cột sẽ gửi gói tin cảnh báo về trung tâm đi theo cả 2 hướng.

Bước 2: Bộ điều khiển trung tâm tính toán và gửi một gói tin, gọi là gói tin Epoch đầu tiên (GenesisEpoch) cho tất cả các cột mà gói tin này chứa các thông tin để thiết lập hệ thống hàng rào, gói tin Epoch gồm các thông tin như sau :

(i) Kỷ nguyên thời gian (epoch);

(ii) Seed256

(iii) PIN256: Mã PIN mới (nếu người dùng thiết lập lại mã PIN)

Trong một phương án ưu tiên, gói tin Epoch được mã hóa bằng hàm EncryptData trước khi truyền.

Bước 3: Trên cơ sở gói tin tại Bước 2 kết hợp với tham số MasterKey cài sẵn trên từng cột, Bộ vi xử lý trên các cột tính toán chỉ số Cypherkey, theo đó:

CypherKey = SHA256 (MasterKey, PIN256, Seed256)

(xem thêm: phần định nghĩa CypherKey ở phía trên)

Tham số Cypherkey được tính ra sẽ được lưu trữ và sử dụng trong tất cả các chu trình thuộc chiều dài kỷ nguyên (epoch).

Cùng trong bước này, bộ vi xử lý trên cột thu của mỗi mắt xích sẽ sản sinh ra một câu đố bảo mật với dung lượng 32 bit (token32) được sinh ra một cách ngẫu nhiên và truyền câu đố đó cho cột phát qua kênh truyền tín hiệu điều khiển.

Trong một phương án ưu tiên, câu đố bảo mật được mã hóa bằng hàm EncryptData trước khi truyền.

Bước 4: Bộ vi xử lý trên cột thu và cột phát cùng tính toán kết quả **h** dựa trên tham số CypherKey đã do Bộ Điều khiển trung tâm tính ra tại Bước 3, kết hợp với câu đố bảo mật token32 tại Bước 3.

Kết quả **h** đươc cột thu và cột phát tính toán theo công thức sau:

h = Hash256(token32)=SHA256(CypherKey, token32).

Vì sử dụng cùng thuật toán và cùng câu đố bảo mật nên kết quả **h** mà hai cột tính được sẽ trùng nhau. Ngược lại, do bên xâm nhập chỉ có thể "nghe trộm" được câu đố bảo mật nhưng không biết được gói tin mà bộ điều khiển trung tâm gửi cho các cột ngay từ đầu nên không thể tính được CypherKey. Hơn nữa, Do hash256 được xây dựng từ hàm SHA256 cấu thành bởi tham số bí mật CypherKey như được mô tả ở trên, nên mã **h** có tính bảo mật rất cao, hầu như không thể tính ngược lại tham số CypherKey từ việc "nghe trộm" kết quả được truyền từ cột phát sang cột thu bằng mạng lưới tia (ở bước 5 dưới đây).

Bước 5: Kết quả **h** tính được tại Bước 4 sẽ được cột phát truyền đến cột thu thông qua lưới tia với hệ thống đèn phát laser hoặc hồng ngoại theo nguyên tắc truyền từng bit cho đến khi truyền hết toàn bộ kết quả.

Trong đó, đèn thứ nhất trên cột phát sẽ phát 1 bit tín hiệu đến đèn thu tương ứng trên cột thu; sau đó, lần lượt các đèn tiếp theo, mỗi đèn sẽ phát 1 bit tín hiệu; khi đèn cuối cùng phát 1 bit tín hiệu thì quay lại đèn thứ nhất và quy trình được lặp lại cho đến khi toàn bộ kết quả tính toán tại Bước 4 đã được truyền hết sang cho cột thu.

Hệ thống có thể có một hoặc nhiều mô đun, trong mỗi mô đun có nhiều đèn. Trong một phương án, hệ thống có một mô đun gồm 8 cặp đèn thu/phát. Do khoảng cách giữa các đèn không được lớn quá vì nếu vậy thì có thể sẽ không phát hiện được các vật thể đi vào khoảng

không nằm giữa hai tia truyền, trong một phương án ưu tiên, khoảng cách giữa các đèn là 10cm; trong trường hợp đó, chiều cao của mô đun chỉ là 80cm. Trong thực tiễn, nhiều hàng rào đòi hỏi chiều cao lớn hơn, vì vậy, theo một phương án ưu tiên của sáng chế, trên cột phát có nhiều mô đun, mỗi mô đun có 8 đèn phát tia hồng ngoại hoặc laser độc lập, trên cột thu có số lượng mô đun đèn thu tương ứng. Trong phương án này, kết quả h tính được tại Bước 4 sẽ được đồng thời truyền tới tất cả các mô đun, mỗi mô đun có 8 cặp đèn thu/phát; bằng cách đó, mạng lưới tia được tạo bởi các lưới tia sẽ có độ cao mong muốn. (Xem Hình 2)

Các đèn phát sẽ được phát bằng các tần số dân dụng như 38kHz, 56kHz … Trong một phương án ưu tiên, tần số mà các đèn phát sử dụng sẽ được thay đổi giữa các cột xen kẽ nhau, ví dụ đèn thứ nhất sử dụng tần số 38kHz thì đèn số hai sử dụng tần số 56kHz, đèn số ba lại sử dụng tần số 38kHz….. Nhờ phương pháp này, cường độ phát của 1 cột có thể tăng lên chồng lấn sang 1 cột thu ở xa hơn, cho phép hệ thống hoạt động trong điều kiện thời tiết khắc nghiệt hơn, ví dụ: khi trời mưa tia hồng ngoại bị hấp thu bớt bởi các giọt nước mưa, nhờ cường độ phát dư nên phần chưa bị hấp thụ đủ để hệ thống vẫn hoạt động bình thường.

Các mắt thu trên các cột có thể là các loại mắt thu dân dụng với chi phí thấp và nguồn cung ứng linh kiện sẵn có.

Trong một phương án ưu tiên của sáng chế, việc truyền thông tin bằng lưới tia có sử dụng kỹ thuật xung mảnh 1%, gọi là kỹ thuật ThinPulse, khác biệt với các xung trong tình trạng kỹ thuật đã biết có tần số sóng mang có độ rộng xung 50%. Nhờ đó, tia có thể được phát trong chế độ bão hòa với thời gian ngắn và cường độ mạnh.

Hình 5. là hình minh họa phương pháp phát tia sử dụng kỹ thuật xung mảnh 1% (ThinPulse) của sáng chế so với phương pháp phát tia sử dụng tần số sóng mang có độ rộng xung 50%.

Khoảng cách chùm tia đi phụ thuộc vào mật độ năng lượng của chùm tia hay cường độ của chùm tia, chứ không phụ thuộc vào thời gian chiếu rọi lâu hay ngắn. Vì thế, trong tình trạng kỹ thuật đã biết, tia được phát với tần số sóng mang có độ rộng xung 50%, phần lớn năng lượng của chùm tia không giúp ích cho việc thu tín hiệu từ khoảng cách xa. Thay vào đó, trong phương án ưu tiên của sáng chế này, việc áp dụng phương pháp ThinPulse sẽ tăng cường độ phát xạ của chùm tia lên gấp năm lần và giảm độ rộng xung đi 50 lần khiến cho hệ thống phát xa gấp năm với mức năng lượng tiêu thụ giảm đi 10 lần ($1 \times 50 = 10 \times (5 \times 1)$), tức là hiệu suất tăng tới 50 lần. Nhờ đó, hàng rào tiêu thụ rất ít năng lượng và có thể triển khai với các dạng năng lượng tái tạo tại chỗ như năng lượng mặt trời, năng lượng gió,…

Bước 6: Bộ vi xử lý trên cột thu tiếp nhận thông tin truyền đến từ cột phát, so sánh dữ liệu nhận được từ cột phát thông qua các đèn phát với kết quả mà bộ vi xử lý trên cột thu tính

được bằng cách so sánh theo từng bit, tức là so mỗi bit thu được từ các đèn phát với một bit tương ứng tính được bằng bộ vi xử lý trên cột thu.

- Nếu kết quả nhận được theo từng bit từ cột phát trùng với kết quả mà bộ vi xử lý trên cột thu tính được, hệ thống sẽ coi là an toàn.

- Nếu kết quả nhận được từ cột phát theo từng bit sai khác với kết quả mà bộ vi xử lý trên cột thu tính được, bit đó sẽ được coi là bit lỗi, khi đó hệ thống giám sát lỗi sẽ đếm từng bit lỗi để đưa ra kết luận lỗi là do nhiễu, do các vật thể nhỏ xâm nhập, do đó không cảnh báo; hoặc do bị tấn công theo kiểu chiếu tia hoặc do có đối tượng xâm nhập, do đó phát tín hiệu cảnh báo.

Kết thúc chu trình thứ nhất.

Chu trình tiếp theo

Chu trình tiếp theo sẽ khởi động ở một thời điểm ngẫu nhiên sao cho kết quả **h** ở chu trình tiếp theo được tính toán và lưu trữ trong tại cột thu và cột phát trước khi chu trình liền trước kết thúc. Tùy theo tình huống, chu trình tiếp theo sẽ khởi động từ Bước 3 hoặc Bước 2, cụ thể như sau:

Trường hợp 1: Trong trường hợp việc thực hiện toàn bộ chu trình trước vẫn nằm trong chiều dài của kỷ nguyên (Epoch_Length) thì chu trình tiếp theo bắt đầu lại từ Bước 3. Theo đó, CypherKey được tạo ra từ Seed256, PIN256 do Bộ Điều khiển trung tâm gửi trong chu trình trước và Masterkey cài sẵn trên cột vẫn được giữ nguyên; cột thu sẽ gửi tới cột phát một câu đố bảo mật dung lượng 32 bit (token32) ngẫu nhiên mới qua kênh truyền tín hiệu điều khiển. Các bước sau vẫn được tiến hành tuần tự như ở chu trình đầu tiên, cụ thể là bộ vi xử lý trên cột thu và cột phát tính toán kết quả dựa trên Cypherkey của chu trình trước, kết hợp với câu đố bảo mật mới (Bước 4). Do đó, ứng với mỗi chu trình tiếp theo sẽ có một kết quả mới. Kết quả này sẽ được truyền từ cột phát sang cột thu (Bước 5) và so sánh để đưa ra kết luận là có phát tín hiệu cảnh báo hay không (Bước 6).

Trường hợp 2: Trong trường hợp việc thực hiện chu trình trước đi hết chiều dài của kỷ nguyên (Epoch_length) thì khi thời gian của kỷ nguyên cũ hết, chu trình tiếp theo thay vì bắt đầu ở Bước 3 sẽ bắt đầu lại ở Bước 2. Theo đó, Bộ điều khiển trung tâm tính toán và gửi một gói tin mới có chứa thông tin về Seed256 mới cho tất cả các cột để tính lại CypherKey mới, thay thế cho Cypherkey trong chu trình trước. Đồng thời, giữa mỗi cặp cột thu và cột phát, cột thu gửi cho cột phát một câu đố bảo mật dung lượng 32 bit (token32) mới qua đường truyền cáp. Như vậy, trong trường hợp này, toàn bộ thông tin cần thiết để tính toán ra kết quả, gồm Cypherkey và token32, đều hoàn toàn thay đổi so với chu trình trước.

Mặt khác, chu trình trước vẫn tiếp tục thực hiện đến cuối cùng như bình thường, gồm truyền thông tin kết quả tính toán (Bước 5) và so sánh để đưa ra kết luận có phát tín hiệu cảnh báo hay không (Bước 6).

Bằng cách đó, việc truyền thông tin thông qua mạng lưới tia được thực hiện liên tục, không gián đoạn và thông tin mã hóa được truyền trên mạng lưới cũng liên tục thay đổi, khiến cho các hình thức tấn công bằng chiếu đèn liên tục hoặc giải mã thông tin truyền qua mạng lưới tia không thể thực hiện được.

Do kết quả tính toán **h** tại Bước 4 có dung lượng 256 bit, dẫn đến thời gian truyền thông tin mã hóa tại Bước 5 diễn ra trong thời gian tương đối ngắn. Trong một phương án, mỗi bit dữ liệu truyền hết trong 455 micro giây, tức là để truyền hết một **h** dung lượng 256 bit sẽ mất 116,5 mili giây (455 micro giây x 256 bit). Như vậy, các chu trình phải thực hiện lặp lại liên tục trong khoảng thời gian ngắn, gây quá tải hệ thống hoặc bắt buộc hệ thống phải có năng lực xử lý lớn và dùng nhiều năng lượng, do đó, làm tăng chi phí đầu tư mua sắm thiết bị và tăng chi phí cho năng lượng, không đáp ứng yêu cầu về kinh tế.

Để giải quyết vấn đề nêu trên, cần một phương pháp tăng dung lượng tính toán một cách nhanh chóng, dễ dàng nhưng vẫn đáp ứng được yêu cầu bảo mật để bất cứ bên thứ ba nào cũng không thể giải mã được hệ thống. Vì vậy, trong một phương án ưu tiên, sáng chế đề xuất phương pháp tăng dung lượng kết quả tính toán tại Bước 4 bằng cách áp dụng sàng hoán vị CR32, bằng cách đó, kết quả tính toán được tăng thêm này cũng được mã hóa đến mức không thể dự đoán được bằng các máy tính trong tình trạng kỹ thuật hiện tại. Cụ thể, trong một phương án ưu tiên của sáng chế, sáng chế được đề xuất bổ sung thêm một bước nữa sau Bước 4, gọi là Bước 4a.

Tham chiếu tới Hình 4, lưu đồ minh họa việc phóng đại kết quả **h** trong **n** lần bằng cách áp dụng sàng hoán vị CR32.

Sau khi Bước 4 kết thúc, kết quả tính toán **h** đã được cặp cột thu và cột phát xác định, bước 4a sẽ bắt đầu. Theo đó, tùy thuộc vào nhu cầu của người sử dụng, kết quả tính toán **h** có dung lượng 256 bit tại Bước 4 có thể được khuếch đại thành **n** kết quả $\mathbf{h}^{(n)}$, mỗi kết quả từ **h** đến $\mathbf{h}^{n}$ đều có dung lượng 256 bit, bằng cách sử dụng sàng hoán vị CR32, bằng cách đó có thể tăng dung lượng thông tin mã hóa được truyền từ cột phát sang cột thu và kéo dài thời gian truyền dữ liệu từ cột phát sang cột thu qua mạng lưới tia. Cụ thể như sau:

Bước 4a:

Sau khi Bước 4 kết thúc, kết quả tính toán **h** đã được cặp cột thu và cột phát tính toán và truyền tới cột thu (Bước 5) để cột thu so sánh kết quả nhận được với kết quả do bộ vi xử lý của cột thu tự tính (Bước 6) và hoàn tất một tiểu quy trình (sub-section).

Tuy nhiên, khác với quy trình cơ bản nêu ở phần trên, hệ thống chưa bắt đầu chu trình tiếp theo ngay mà bộ vi xử lý của cột thu và cột phát sẽ biến đổi kết quả **h** thành một kết quả $\mathbf{h}^{(1)}$ sử dụng sàng hoán vị CR32 theo công thức sau:

$$h^{(1)} = CR32.Swap(h)$$

Sau đó, kết quả tính toán $\mathbf{h}^{(1)}$ được truyền tới cột thu (Bước 5) để cột thu so sánh kết quả nhận được với kết quả do bộ vi xử lý của cột thu tự tính (Bước 6), kết thúc tiểu quy trình tiếp theo.

Tiểu quy trình nêu trên sẽ được lặp lại **n** lần. theo đó, kết quả $\mathbf{h}^{(n)}$ được tính bằng cách hoán vị bằng sàng hoán vị CR32 đối với kết quả **h** liền trước đó, tức là $\mathbf{h}^{(n-1)}$.

Về lý thuyết, Bước 4a có thể có số lần khuếch đại không giới hạn, tức là **n** có thể lớn vô cùng. Tuy nhiên, nếu **n** quá lớn thì thời gian truyền hết tất cả thông tin mã hóa trong các tiểu quy trình kéo dài quá lâu, dẫn đến rủi ro tin tặc (hacker) có đủ thời gian thu được kết quả truyền bằng mạng lưới tia để phân tích và phá mã, từ đó có thể phát ra các chùm tia mã hóa giả mạo để đánh lừa hệ thống. Ngược lại, nếu tham số **n** quá nhỏ thì thời gian truyền hết thông tin mã hóa trong các tiểu quy trình quá ngắn, dẫn đến việc bộ xử lý trên cột thu phải liên tục sản sinh ra token32, đồng thời bộ vi xử lý trên cột thu và cột phát phải tính toán mã **h** mới, gây quá tải hệ thống.

Do đó, tham số **n** được đề xuất theo một phương án của sáng chế này nằm trong khoảng từ 200 đến 2000. Trong một phương án ưu tiên, tham số n bằng 256, tương ứng với việc cột phát truyền toàn bộ thông tin mã hóa của tất cả các tiểu quy trình trong một chu trình hết khoảng 20 giây.

Trong Bước 5 (truyền kết quả **h** có dung lượng 256 bit qua mạng lưới tia), khi bộ vi xử lý của mỗi cặp cột thu và cột phát tính ra kết quả **h** có dung lượng 256 bit, kết quả **h** này sẽ được truyền từ cột phát sang cột thu lần lượt từ đèn phát thứ nhất đến đèn phát thứ **n**, sau đó quay lại đèn phát thứ nhất cho đến khi toàn bộ kết quả được truyền hết. Mỗi lần truyền dữ liệu từ đèn phát thứ nhất đến đèn phát thứ **n** được tính là một **phiên truyền**. Như vậy, tùy thuộc vào số cặp đèn thu/phát, toàn bộ kết quả **h** này sẽ được truyền qua (x) phiên truyền, được tính bằng cách lấy 256 bit chia cho số cặp đèn thu/phát được sử dụng. Ví dụ, trong một phương án ưu tiên, số cặp đèn thu/phát là 8, do đó, số phiên truyền cần thiết để truyền hết toàn bộ 256 bit kết quả **h** là: x = 256 : 8 = 32 phiên truyền.

Trong một phương án khác, số cặp đèn thu/phát là 7, do đó số phiên truyền để truyền hết toàn bộ 256 bit kết quả **h** là x = 256 : 7 = 36 dư 4 bit. Như vậy, số phiên truyền được xác định là 36, còn 4 bit dư được bỏ qua, không truyền.

Quá trình truyền dữ liệu mô tả ở trên có một nhược điểm là sẽ có những phiên truyền, toàn bộ hoặc phần lớn bit 0 sẽ được truyền trong phiên. Nói cách khác, trong phiên truyền đó, tất cả hoặc phần lớn các đèn tắt (truyền bit bằng 1 thì đèn bật, truyền bit bằng 0 thì tắt), dẫn đến nếu có vật xâm nhập qua hàng rào đúng thời điểm đó, hệ thống không phát hiện ra.

Để khắc phục nhược điểm này, trong một phương án ưu tiên của sáng chế, việc "đảo bít" được đề xuất trong Bước 5 của sáng chế. Cụ thể như sau:

Nếu trong mỗi phiên truyền, số lượng bit 1 nhiều hơn số lượng bit 0 được truyền trong phiên thì việc truyền diễn ra bình thường; nếu bộ vi xử lý trên cột thu và cột phát nhận thấy rằng số lượng bit 1 ít hơn số lượng bit 0 được truyền trong phiên thì hệ thống sẽ tự động áp dụng quy trình "đảo bit" đối với lượng dữ liệu được truyền trong phiên truyền sao cho lượng bit 1 trong mỗi phiên truyền luôn lớn hơn lượng bit 0. Khái niệm "đảo bit" được hiểu là nếu một bit có giá trị bằng 0 thì đổi thành 1 và ngược lại, nếu một bit có giá trị bằng 1 thì đổi thành 0.

Ví dụ của việc đảo bit trong một trường hợp cụ thể như sau:

Bảng 1. Số bit theo kết quả tính được theo mỗi phiên truyền

Số bit / Phiên truyền	1	2	3	4	5	6	7	8	Tỉ lệ bit 0/bit 1
1	0	1	0	0	1	1	1	1	<50%
2	0	0	1	0	0	0	0	1	>50%
3	1	1	0	1	0	1	1	0	<50%
4	1	0	0	1	1	0	1	0	=50%
5	0	0	0	0	0	0	0	0	>50%
....	...	...	...	...	...	...	...	...	...
31	0	1	1	0	0	0	0	0	>50%
32	1	1	0	1	0	1	1	0	<50%

Bảng 2. Số bit đã được "đảo bít" và phát theo mỗi phiên truyền

Số bit / Phiên truyền	1	2	3	4	5	6	7	8	Ghi chú
1	0	1	0	0	1	1	1	1	Giữ nguyên
2	1	1	0	1	1	1	1	0	Đã đảo bit
3	1	1	0	1	0	1	1	0	Giữ nguyên
4	1	0	0	1	1	0	1	0	Giữ nguyên
5	1	1	1	1	1	1	1	1	Đã đảo bit
....	...	...	...	...	...	...	...	...	...
31	1	0	0	1	1	1	1	1	Đã đảo bit
32	1	1	0	1	0	1	1	0	Giữ nguyên

Việc đảo bit kết quả nhằm mục đích làm cho dữ liệu được truyền trên mạng lưới tia trong mỗi phiên truyền có số lượng tia được truyền nhiều nhất, bởi vì khi dữ liệu được truyền có giá trị bit bằng 0 thì đèn phát không phát; khi dữ liệu được truyền có giá trị bit bằng 1 thì đèn phát sẽ phát. Như vậy, nếu giá trị của dữ liệu được truyền có quá nhiều giá trị bit bằng 0 thì xuất hiện rủi ro khi đối tượng xâm nhập qua hàng rào nhưng nó không phát hiện ra vì lúc đó đèn phát không phát nên có đối tượng xâm nhập hay không thì hệ thống vẫn ghi nhận dữ liệu được truyền đúng.

Việc đảo bit trong từng phiên truyền đã loại trừ hoàn toàn khả năng có đối tượng xâm nhập vào đúng khoảng thời gian giá trị bit của dữ liệu được truyền bằng 0, tức là đèn phát tắt, kết quả là hệ thống không phát hiện ra.

Hàng rào thông minh theo sáng chế này có mức độ bảo mật rất cao, có khả năng vượt trội trong phát hiện xâm nhập và phát hiện tấn công bằng các phương pháp chiếu đèn hoặc giả mạo thông tin. Ngay cả khi các đối tượng thu được thông tin trên đường truyền tia và/hoặc đường truyền hữu tuyến thì các thông tin này cũng không thể sử dụng được do đã được mã hóa. Mặt khác, các đối tượng cũng không thể phát tia giả mạo thông tin, vì các thông tin truyền bằng tia đã được mã hóa SHA256, trừ khi biết được CypherKey là mật mã sử dụng để mã hóa, trong khi đó tấn công CypherKey là việc rất khó do cần phải biết đồng thời ba tham số là mã của nhà sản xuất (MasterKey), mã của người sử dụng (PIN256), mã ngẫu nhiên thay đổi theo epoch không thể đoán trước (Seed256) chỉ có hệ thống biết.

Các đối tượng muốn xâm nhập không thể dùng biện pháp thu thông tin được truyền qua mạng lưới tia để phát lại hòng lừa hệ thống vì thông tin được truyền thay đổi liên tục không lặp lại, không thể dự báo trước và không thể tính ngược lại được Cypherkey (đó là tính chất của mã một chiều SHA);

Khi xuất hiện vật thể che đường truyền tia, hoặc có hacker giả mạo thông tin, ví dụ đơn giản như rọi tia liên tục vào cột thu, cột thu sẽ thu được thông tin sai; từ đó biết có vấn đề trên đường truyền này, và phân tích tình huống để đưa ra kết luận.

Trong thực tế, các đối tượng xâm nhập có thể tấn công hệ thống hàng rào thông minh theo các cấp độ như sau:

Tấn công cấp độ 1: Không biết CypherKey, không tiếp xúc trực tiếp với hàng rào, không thể nghe lén token32.

Ở cấp độ này, tin tặc (hacker) không có bảng mã nên không thể giả mạo dữ liệu truyền qua các chùm tia trong mỗi phiên. Cũng không thể thu lại tín hiệu trên đường truyền hòng tìm ra quy luật lặp lại, vì dữ liệu truyền trên đường truyền ở mỗi phiên là khác nhau và thông tin được phân bố rất gần với phân bố đều (ngẫu nhiên).

Tấn công cấp độ 2: không biết CypherKey, tiếp xúc trực tiếp với hàng rào, nghe lén được token32 vì token32 được truyền không mã hóa trên đường truyền cáp.

Ở cấp độ này, tin tặc tấn công hệ thống hàng rào bằng cách giả mạo dữ liệu truyền qua các chùm tia trong mỗi phiên.

Tuy nhiên, để thực hiện được phương pháp tấn công này, tin tặc phải tấn công mã SHA256 với CypherKey dài 256 bits. Cách duy nhất hiệu quả là tấn công BruteForce cho 2^{256}

trường hợp trong vòng một epoch cỡ một ngày đến một tháng, tương đương cỡ 10^{70} phép băm SHA256 trong vòng một giây. Cho tới nay, khả năng tính toán này chưa tồn tại, ngay cả cộng gộp tất cả siêu máy tính và các thiết bị điện tử rời rạc cũng chưa đủ. Tức là không thể tấn công.

Tấn công cấp độ 3: không biết CypherKey, nhưng bằng cách nào đó biết được mã PIN của người dùng, đồng thời bằng cách nào đó biết được mã MasterKey của nhà sản xuất và đã đọc toàn bộ tài liệu lập trình hệ thống; nhưng không biết Seed256.

Lưu ý rằng điều kiện này rất khó đạt được, nhưng giả định rằng có khả năng xảy ra.

Đồng thời, tin tặc tiếp xúc trực tiếp với hàng rào, nghe lén được token32.

Để thực hiện được tấn công này, tin tặc phải tấn công mã SHA256 với CypherKey mà chưa biết Seed256. Như đã mô tả ở trên, Seed256 là tham số được tạo ra bằng cách hoán vị ngẫu nghiên 32 phần tử do hệ thống tự động sinh ra theo mỗi epoch.

Cách duy nhất hiệu quả là tấn công Brute Force cho 32! trường hợp hoán vị Seed256 trong vòng một epoch cỡ một ngày đến một tháng; tương đương cỡ 10^{30} phép băm SHA256 trong một giây. Cho tới nay, sức mạnh tính toán này chưa tồn tại, ngay cả cộng gộp tất cả siêu máy tính và các thiết bị điện tử rời rạc cũng chưa đủ. Tức là không thể tấn công.

Điều này hàm ý rằng, ngay cả nhà sản xuất hay người vận hành hệ thống cũng không có năng lực tấn công mật mã vào hệ thống này.

Tóm lại, với hệ thống hàng rào thông minh được đề xuất theo sáng chế này, các phương pháp tấn công đều phải giải được câu đố bảo mật giữa các cột. Bất kỳ ai không nắm được đầy đủ ba thành phần của CypherKey gồm: mã của nhà sản xuất (MasterKey), mã của người sử dụng (PIN256), mã ngẫu nhiên thay đổi theo epoch không thể đoán trước (Seed256) đều không thể vượt qua được hàng rào.

Giải pháp kỹ thuật được đề xuất theo sáng chế này còn khác biệt ở chỗ nó có thể nhận biết một cách tương đối chính xác đối tượng xâm nhập qua hàng rào để xác định đó là nhiễu thông thường, vật nhỏ xâm nhập, xâm nhập điện tử hay vật có nguy cơ mất an ninh xâm nhập, bằng cách phân tích sai số giữa thông tin nhận được từ mạng lưới tia và kết quả do bộ vi xử lý mà cột thu tự tính.

Hình 6. là phương pháp phát hiện kích thước đối tượng xâm nhập và cách thức xâm nhập theo phương án của sáng chế.

Phương pháp phát hiện kích thước đối tượng xâm nhập và cách thức xâm nhập theo sáng chế này cụ thể như sau:

Bước i: Bộ vi xử lý trên cột thu so sánh dữ liệu nhận được từ cột phát với dữ liệu cột thu tính được. Nếu nhận sai dữ liệu truyền từ một chùm tia, cột thu sẽ ghi nhận đó là một lỗi truyền tại mắt thu tương ứng.

Bước ii: Bộ vi xử lý trên cột thu đánh giá lỗi, đưa ra một trong các kết luận sau:

(i) hệ thống hoạt động bình thường;

(ii) hệ thống bị nhiễu;

(iii) hệ thống bị tấn công; hoặc

(iv) Hệ thống bị vật thể che chắn (có xâm nhập) và báo về cho bộ điều khiển trung tâm.

Trong đó:

- Nếu dữ liệu mà cột thu nhận được từ cột phát trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được thì hệ thống ghi nhận là hoạt động bình thường;

- Nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được nhưng thời gian có sự sai khác ở những lần thu liên tiếp nhau của một hoặc một vài đèn thu ngắn hơn giá trị định trước thì hệ thống ghi nhận là nhiễu và không phát tín hiệu cảnh báo.

Trong một phương án của sáng chế, giá trị định trước là 5,5 mili giây, tức là thời gian mà một hoặc một số đèn thu nhận tín hiệu sai khác liên tiếp dưới 5,5 mili giây thì hệ thống ghi nhận là nhiễu;

- Nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được, trong đó, một hoặc một số đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 1 trong thời gian dài hơn giá trị định trước và dữ liệu được truyền này là sai khác với kết quả tính toán được thì hệ thống ghi nhận là bị tấn công bằng phương pháp chiếu tia và phát tín hiệu cảnh báo.

Trong một phương án của sáng chế, giá trị định trước là 5,5 mili giây;

- Nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được, trong đó, một hoặc một số đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 0 trong thời gian dài hơn giá trị định trước và dữ liệu được truyền này là sai khác với kết quả tính toán được thì hệ thống ghi nhận là có vật xâm nhập qua hàng rào. Căn cứ vào số lượng và thời gian đèn ghi nhận giá trị bit được truyền sai bằng 0 liên tiếp vượt quá thời gian định trước, và một giả định định trước về tốc độ của vật xâm nhập, hệ thống sẽ ước lượng được chiều cao S và chiều sâu D tương đối của vật xâm nhập. Theo đó, chiều cao của vật xâm

nhập S được coi như bằng với độ dài của các đèn thu liền nhau bị ghi nhận giá trị bit được truyền bằng 0 bị lỗi; chiều sâu của vật xâm nhập được ước lượng bằng thời gian các đèn đó bị lỗi nhân với vận tốc định trước, theo một phương án được đặt cố định là 8m/s (*khoảng 30km/h, là vận tốc của các vật có tốc độ tương đối nhanh như người chạy, chim, sóc... có thể đạt được*).

Nếu vật có chiều cao và/hoặc chiều sâu lớn hơn giá trị định trước thì hệ thống sẽ phát tín hiệu báo động, kèm theo thông số của vật đã xâm nhập.

Nếu vật có chiều cao thấp và chiều sâu nhỏ hơn giá trị định trước thì hệ thống sẽ coi đó là các vật xâm nhập nhỏ không đáng quan tâm, không phát tín hiệu cảnh báo.

Nói chung, tùy từng cấu hình của hàng rào, đối tượng bảo vệ của hàng rào và thực tế địa hình, địa vật, môi trường ... mà người sử dụng có thể tùy biến tốc độ giả định định trước của vật xâm nhập, giá trị S (chiều cao) và D (chiều sâu) phù hợp.

Ví dụ, trong hàng rào thông minh theo sáng chế này có 04 mô đun, mỗi mô đun có 8 cặp đèn thu/phát, mỗi đèn trong mô đun đặt cách nhau 10 cm; các mô đun đặt cách nhau 30cm để tạo thành hàng rào/mạng lưới tia cao gồm 32 tia, cao 4,1m (xem Hình 2.). Tham số tốc độ giả định định trước của vật xâm nhập là 8m/s, tức là tốc độ của một người chạy nhanh hoặc tốc độ của các loài động vật như chim, chuột.

Nếu hệ thống ghi nhận bit lỗi liên tiếp có giá trị bằng 0 trong thời gian 0,0375 giây, tức là 375 mili giây, của các tia thứ ba từ dưới lên đến tia thứ mười ba, thì hệ thống sẽ coi là đã có một vật cao 1,2 m và sâu 0,3m (8m/s *0,075s) xâm nhập qua hàng rào và phát tín hiệu báo động.

Vì hệ thống không thể biết được tốc độ của vật xâm nhập nên phải đặt trước một tốc độ giả định, trong ví dụ này là 8m/s. Như vậy, hệ thống có thể coi 1 vật di chuyển chậm (ví dụ, một người đi bộ tốc độ thực tế 2 m/s) có chiều sâu bằng với 1 vật có chiều sâu lớn hơn nhiều nhưng di chuyển nhanh (ví dụ, mô tô chạy với tốc độ 32m/s). Do đó, nếu như hệ thống có thể xác định khá chuẩn xác chiều cao S của vật xâm nhập thì chiều sâu của vật xâm nhập D chỉ là tham số ước tính mà thôi.

Hiệu quả đạt được của sáng chế:

Hàng rào điện tử theo sáng chế này có cơ chế kết nối đoàn tàu khép kín (train-loop): tự động đánh địa chỉ. Yếu tố này khiến hàng rào có thể mở rộng gần như không giới hạn phạm vi bảo vệ thông qua số lượng các cột triển khai được.

Hàng rào điện tử theo sáng chế này có cơ chế trao đổi câu đố mật mã công khai giữa các cột. Yếu tố này cho phép hàng rào chống được tấn công mật mã, phát hiện được tin tặc xâm nhập.

Sáng chế đề xuất cơ chế khuếch đại hàm băm, cho phép hàng rào có thể được triển khai trên các chip điều khiển không quá mạnh, giá thành rẻ; mà vẫn đảm bảo tính bảo mật của hệ thống.

Bên cạnh đó, sáng chế còn có cơ chế đảm bảo mật độ bit 1 trong khối dữ liệu mã hóa trong mỗi phiên truyền luôn lớn hơn 50%, trước khi truyền luân phiên từng bit trên hàng rào theo chế độ quét mành. Yếu tố này cho phép hàng rào có thể được triển khai truyền luân phiên từng bit trên hàng rào theo chế độ quét mành mà không tạo ra lỗ hổng hàng rào khi có nhiều bít 0 liên tiếp trong dữ liệu mã hóa.

Sáng chế cũng đề xuất cơ chế truyền luân phiên từng bit trên hàng rào theo chế độ quét mành theo từng mô đun, mỗi mô đun có 8 cặp đèn thu/phát và cơ chế cho phép truyền đồng thời kết quả h tính toán được cho tất cả các mô đun của hàng rào, cho phép hàng rào có thể mở rộng theo chiều cao bằng cách mở rộng thêm nhiều mô đun.

Sáng chế đề xuất cơ chế chìa khóa mật mã bao gồm nhiều thành phần (CypherKey ba thành phần), thay đổi chìa khóa mật mã theo từng kỷ nguyên Epoch, cho phép hàng rào bảo mật đảm bảo tính bảo mật cao ngay cả đối với nhà sản xuất, tôn trọng tự do và chủ quyền đối với chủ sở hữu của hàng rào.

Hàng rào điện tử theo sáng chế này có cơ chế phát hiện được tấn công bảo mật, bên cạnh việc phát hiện ra nhiễu, động vật nhỏ và các đối tượng xâm nhập; đồng thời có thể ước lượng tương đối chính xác chiều cao (S) và chiều sâu (D) của đối tượng xâm nhập.

Bên cạnh đó, sáng chế còn đề xuất cơ chế hoạt động độc lập trong từng epoch giữa các cột, khiến cho hàng rào có thể kéo dài gần như không giới hạn, bởi cấu trúc này không yêu cầu bộ điều khiển trung tâm phải gia tăng sức mạnh khi số lượng các cột gia tăng.

Hàng rào điện tử theo sáng chế này còn có cơ chế phát xung mảnh bão hòa, giúp nâng cao hiệu suất sử dụng năng lượng, từ đó, cho phép sử dụng các nguồn năng lượng tái tạo như: năng lượng mặt trời, năng lượng gió, năng lượng sóng biển...

YÊU CẦU BẢO HỘ

1. Phương pháp phát hiện xâm nhập, bao gồm:

chu trình thứ nhất (chu trình trước):

bước 1: khi hàng rào được kích hoạt, bộ điều khiển trung tâm sẽ gửi gói tin kiểm tra đến tất cả các cột theo phương thức chuyển tiếp,

gói tin kiểm tra được chuyển đến cột thu đầu tiên có số thứ tự 01, cột thu (01) sẽ ghi nhận địa chỉ của mình là (01) rồi hồi đáp bằng gói tin Ack (01) cho bộ điều khiển trung tâm, đồng thời chuyển tiếp gói tin kiểm tra cho cột phát tiếp theo (02); tương tự, cột phát (02) sẽ phản hồi cho bộ điều khiển trung tâm và chuyển tiếp gói tin kiểm tra sang cột thu (03); cột cuối cùng trong hệ thống là cột phát (k) cũng sẽ hồi đáp về bộ điều khiển trung tâm qua các cột trước đó, đồng thời trực tiếp chuyển tiếp gói tin kiểm tra về bộ điều khiển trung tâm;

nếu cột nào không phản hồi hoặc không chuyển tiếp gói tin, bộ điều khiển trung tâm sẽ ghi nhận cột đó là cột lỗi và gửi gói tin theo hướng ngược lại; khi nhận được gói tin truyền theo hướng ngược lại, các cột cũng phản ứng giống như trong trường hợp gói tin truyền theo chiều thuận cho đến khi gặp cột không phản hồi, và ghi nhận cột đó là cột lỗi;

đoạn hàng rào được xác định bởi hai cột lỗi (không phản hồi) sẽ được ghi nhận là đoạn hàng rào bị lỗi, trong khi phần còn lại của hàng rào vẫn hoạt động bình thường;

bước 2: bộ điều khiển trung tâm tính toán và gửi một gói tin tới tất cả các cột trong hệ thống, gồm các thông tin như sau:

(iv) kỷ nguyên thời gian (Epoch);

(v) seed256; và

(vi) PIN256 (nếu người dùng thiết lập lại mã PIN);

bước 3: trên cơ sở gói tin tại bước 2 và MasterKey cài sẵn trên từng cột thu, bộ vi xử lý trên các cột tính toán tham số Cypherkey và lưu trữ để sử dụng trong tất cả các chu trình thuộc chiều dài kỷ nguyên, theo đó:

CypherKey = SHA256 (MasterKey, PIN256, Seed256)

đồng thời, bộ vi xử lý trên cột thu của mỗi mắt xích sẽ sản sinh ra một câu đố bảo mật được sinh ra một cách ngẫu nhiên với dung lượng 32 bit (token32) và truyền câu đố đó cho cột phát qua kênh truyền tín hiệu điều khiển;

bước 4: bộ vi xử lý trên cột thu và cột phát cùng tính toán kết quả **h** dựa trên CypherKey và câu đố bảo mật token32 tại bước 3 theo công thức:

h = Hash256(token32)=SHA256(CypherKey, token32)

bước 5: kết quả **h** tính được tại bước 4 sẽ được cột phát truyền đến cột thu thông qua lưới tia hồng ngoại hoặc laser theo nguyên tắc truyền từng bit cho đến khi toàn bộ kết quả được

truyền hết; trong đó, đèn thứ nhất trên cột phát sẽ phát 1 bit tín hiệu đến đèn thu tương ứng trên cột thu; sau đó, lần lượt các đèn tiếp theo, mỗi đèn sẽ phát 1 bit tín hiệu; khi đèn cuối cùng phát 1 bit tín hiệu thì quay lại đèn thứ nhất và quy trình được lặp lại cho đến khi toàn bộ kết quả tính toán tại bước 4 đã được truyền hết sang cho cột thu;

bước 6: bộ vi xử lý trên cột thu tiếp nhận thông tin truyền đến từ cột phát, so sánh dữ liệu nhận được từ cột phát thông qua các đèn phát với kết quả mà bộ vi xử lý trên cột thu tính được bằng cách so sánh theo từng bit;

- nếu kết quả nhận được theo từng bit từ cột phát trùng với kết quả mà bộ vi xử lý trên cột thu tính được, hệ thống sẽ coi là an toàn;

- nếu kết quả nhận được từ cột phát theo từng bit sai khác với kết quả mà bộ vi xử lý trên cột thu tính được, bit đó sẽ được coi là bit lỗi, khi đó hệ thống giám sát lỗi sẽ đếm từng bit lỗi để đưa ra kết luận lỗi là do nhiễu, do các vật thể nhỏ xâm nhập, do đó không cảnh báo; hoặc do bị tấn công theo kiểu chiếu tia hoặc do có đối tượng xâm nhập, do đó phát tín hiệu cảnh báo;

kết thúc chu trình thứ nhất, chuyển sang chu trình tiếp theo;

chu trình tiếp theo

chu trình tiếp theo sẽ khởi động ở một thời điểm ngẫu nhiên sao cho kết quả **h** ở chu trình tiếp theo được tính toán và lưu trữ trong tại cột thu và cột phát trước khi chu trình liền trước kết thúc, trong đó:

- nếu việc thực hiện toàn bộ chu trình trước vẫn nằm trong chiều dài của kỷ nguyên thì chu trình tiếp theo bắt đầu lại từ bước 3: theo đó, CypherKey vẫn được giữ nguyên; cột thu sẽ gửi tới cột phát một câu đố bảo mật dung lượng 32 bit (token32) ngẫu nhiên mới qua kênh truyền tín hiệu điều khiển; các bước sau vẫn được tiến hành tuần tự như ở chu trình đầu tiên;

- nếu việc thực hiện chu trình trước đã đi hết chiều dài của kỷ nguyên thì chu trình trước vẫn tiếp tục thực hiện đến cuối cùng như bình thường; khi hết chiều dài kỷ nguyên, chu trình tiếp sẽ bắt đầu lại ở bước 2: theo đó, Bộ điều khiển trung tâm gửi gói tin mới có chứa thông tin về Seed256 mới cho tất cả các cột để tính lại CypherKey để thay thế cho Cypherkey trong chu trình trước; đồng thời, cột thu vẫn gửi cho cột phát trong một mắt xích một câu đố bảo mật dung lượng 32 bit (token32) mới qua đường truyền cáp; các bước sau vẫn được tiến hành tuần tự như ở chu trình đầu tiên.

2. Phương pháp phát hiện xâm nhập theo điểm 1, trong đó, sau khi bước 4 kết thúc, kết quả tính toán **h** đã được cặp cột thu và cột phát xác định và truyền tới cột thu (bước 5) để cột thu so sánh kết quả nhận được với kết quả do bộ vi xử lý của cột thu tự tính (bước 6) và hoàn tất tiểu quy trình đầu tiên,

khác biệt ở chỗ, trước khi tiểu quy trình đầu tiên kết thúc, hệ thống chưa bắt đầu chu trình tiếp theo ngay mà bắt đầu một tiểu quy trình tiếp theo, theo đó, bộ vi xử lý của cột thu và cột phát sẽ biến đổi kết quả **h** thành một kết quả $\mathbf{h^{(1)}}$ sử dụng sàng hoán vị CR32 theo công thức sau:

$$h^{(1)} = CR32.Swap(h)$$

sau đó, kết quả tính toán $\mathbf{h^{(1)}}$ được truyền tới cột thu (bước 5) để cột thu so sánh kết quả nhận được với kết quả do bộ vi xử lý của cột thu tự tính (bước 6), kết thúc tiểu quy trình tiếp theo;

tiểu quy trình nêu trên sẽ được lặp lại **n** lần, theo đó, kết quả $\mathbf{h^{(n)}}$ được tính bằng cách hoán vị bằng sàng hoán vị CR32 đối với kết quả **h** liền trước đó, tức là $\mathbf{h^{(n-1)}}$.

3. Phương pháp phát hiện xâm nhập theo điểm 2, trong đó, n nằm trong khoảng từ 200 đến 2.000.

4. Phương pháp phát hiện xâm nhập theo điểm 2, trong đó, n bằng 256.

5. Phương pháp phát hiện xâm nhập theo điểm 1, trong đó, nếu trong mỗi phiên truyền, số lượng bit 1 nhiều hơn hoặc bằng số lượng bit 0 được truyền trong phiên thì việc truyền diễn ra bình thường; nếu số lượng bit 1 ít hơn số lượng bit 0 được truyền trong phiên thì quy trình "đảo bit" đối với lượng dữ liệu được truyền trong phiên truyền sẽ được kích hoạt sao cho lượng bit 1 trong mỗi phiên truyền luôn lớn hơn lượng bit 0.

6. Phương pháp phát hiện xâm nhập theo điểm 1, trong đó, cứ sau một khoảng thời gian định trước, các cột sẽ gửi một gói tin điểm danh tới bộ điều khiển trung tâm để điểm danh; nếu hết thời gian định trước mà bộ điều khiển trung tâm không nhận được gói tin điểm danh của cột nào thì hệ thống sẽ ghi nhận cột đó bị lỗi và báo động.

7. Phương pháp phát hiện xâm nhập theo điểm 6, trong đó, thời gian định trước để gửi gói tin điểm danh là 10 giây.

8. Phương pháp phát hiện xâm nhập theo điểm 1, trong đó, kết quả **h** tính được tại bước 4 sẽ được đồng thời truyền tới nhiều mô đun, mỗi mô đun có nhiều cặp đèn thu/phát, để tạo ra mạng lưới tia với độ cao mong muốn.

9. Phương pháp phát hiện xâm nhập theo điểm 8, trong đó, mỗi mô đun có 8 cặp đèn thu/phát.

10. Phương pháp phát hiện xâm nhập theo điểm bất kỳ từ điểm 1, trong đó, việc truyền dữ liệu bằng lưới tia trong bước 5 sử dụng kỹ thuật xung mảnh 1%.

11. Phương pháp phát hiện xâm nhập theo điểm 1, trong đó, các cột phát luân phiên sử dụng nhiều tần số sóng mang xen kẽ.

12. Phương pháp phát hiện xâm nhập theo điểm 11, trong đó, các cột phát luân phiên sử dụng luân phiên hai tần số 38khz và 56khz xen kẽ nhau.

13. Phương pháp phát hiện xâm nhập theo điểm 1, trong đó, các gói tin được truyền trên kênh truyền tín hiệu điều khiển được mã hóa bằng hàm EncryptData và được xác thực bằng hàm hash32.

14. Phương pháp phát hiện xâm nhập theo điểm 1, trong đó, tại bước 6, kích thước đối tượng xâm nhập và cách thức xâm nhập được xác định theo cách thức như sau:

bước i: bộ vi xử lý trên cột thu so sánh dữ liệu nhận được từ cột phát với dữ liệu cột thu tính được, nếu dữ liệu được truyền của mỗi cặp đèn thu/phát không khớp nhau, cột thu sẽ ghi nhận đó là một lỗi tại vị trí đèn thu/phát tương ứng;

bước ii: bộ vi xử lý trên cột thu đánh giá lỗi, trong đó:

- nếu dữ liệu mà cột thu nhận được từ cột phát trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được thì hệ thống ghi nhận là hoạt động bình thường;

- nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được (có lỗi) nhưng thời gian tồn tại lỗi liên tiếp tại mỗi vị trí ngắn hơn giá trị định trước thì hệ thống ghi nhận là nhiễu và không phát tín hiệu cảnh báo;

- nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được (có lỗi), trong đó, một hoặc nhiều đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 1 trong thời gian dài hơn giá trị định trước thì hệ thống ghi nhận là bị tấn công bằng phương pháp chiếu tia và phát tín hiệu cảnh báo;

- nếu dữ liệu mà cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của cột thu tính toán được (có lỗi), trong đó, một hoặc nhiều đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 0 trong thời gian dài hơn giá trị định trước thì hệ thống ghi nhận là có vật xâm nhập qua hàng rào và hệ thống sẽ tính toán để ước lượng chiều cao (S) và chiều sâu (D) tương đối của vật xâm nhập, dựa trên một tham số giả định định trước về tốc độ của vật xâm nhập:

nếu vật có chiều cao thấp hơn và chiều sâu nhỏ hơn giá trị định trước thì hệ thống sẽ coi đó là các vật xâm nhập nhỏ không đáng quan tâm, không phát tín hiệu cảnh báo;

nếu vật có chiều cao và/hoặc chiều sâu lớn hơn giá trị định trước thì hệ thống sẽ phát tín hiệu báo động, kèm theo giá trị chiều cao và chiều sâu ước tính của vật đã xâm nhập.

15. Phương pháp xác định kích thước đối tượng xâm nhập và cách thức xâm nhập theo điểm 14, trong đó giá trị thời gian tồn tại lỗi định trước là 5,5 mili giây.

16. Hệ thống hàng rào điện tử thông minh sử dụng phương pháp phát hiện xâm nhập theo điểm bất kỳ trong các điểm từ 1 đến 15, hệ thống này bao gồm:

(i) bộ điều khiển trung tâm, kết nối với tất cả các cột trong hệ thống bằng kênh truyền tín hiệu điều khiển theo một vòng tròn khép kín, trong đó, bộ điều khiển trung tâm kết nối với cột thứ nhất, cột thứ nhất sẽ được nối nối tiếp với cột thứ hai... cột cuối cùng (k) sẽ nối với cột liền trước (k-1) và nối trở lại vào bộ điều khiển trung tâm bằng kênh truyền tín hiệu điều khiển;

trên cột thứ nhất có nhiều đèn thu; trên cột thứ hai có nhiều đèn phát; trên cột tiếp theo có nhiều đèn thu ...; cột cuối cùng (k) có nhiều đèn phát;

(ii) mỗi cặp cột, gồm cột thu (a) và cột phát liền kề (b) tạo thành một mắt xích của hệ thống hàng rào điện tử,

- trên cột thu (a) có chứa mô đun đèn thu tín hiệu laser hoặc hồng ngoại, mỗi mô đun gồm nhiều đèn, được bố trí dọc thân cột hướng về hướng cột phát liền kề (b) sao cho tương ứng với mỗi đèn phát trên cột phát liền kề (b) sẽ có một đèn thu trên cột thu trước đó (a); trên cột thu (a) còn có bộ vi xử lý chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước và so sánh với tín hiệu mã hóa nhận được từ đèn thu;

- trên cột phát liền kề (b) với một cột thu (a) có chứa mô đun đèn phát tín hiệu laser hoặc hồng ngoại, mỗi mô đun gồm nhiều đèn được bố trí dọc thân cột hướng về cột thu liền trước đó (a) sao cho tương ứng mỗi đèn thu sẽ có một đèn phát; trên cột phát liền kề (b) có bộ vi xử lý chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước và gửi kết quả giải mã thông qua đèn phát tới đèn thu để tạo thành mạng lưới tia;

(iii) kênh truyền tín hiệu điều khiển để truyền "câu đố", chính là token32, từ cột thu tới cột phát trong cùng một mắt xích;

trong đó, cột phát liền kề (b) sẽ đặt sát và úp lưng vào cột thu tiếp theo (a);

trong đó, công thức cài đặt trước trong phần mềm nhúng để giải mã của bộ vi xử lý của cột thu trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã của bộ vi xử lý của cột phát.

17. Hệ thống hàng rào điện tử thông minh theo điểm 16, trong đó, cột phát liền kề (b) và cột thu tiếp theo (a) được ghép vào với nhau thành một cột duy nhất.

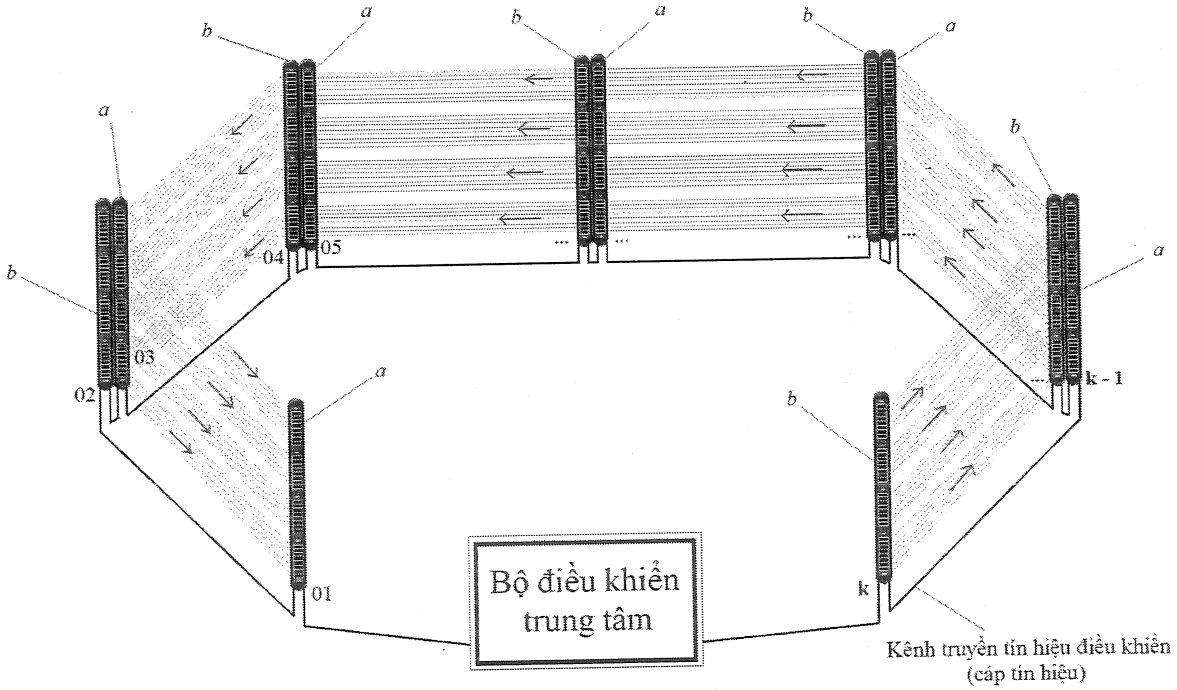
18. Hệ thống hàng rào điện tử thông minh theo điểm 16, trong đó, kênh truyền tín hiệu điều khiển là cáp tín hiệu.

19. Hệ thống hàng rào điện tử thông minh theo điểm 16, trong đó, mô đun gồm nhiều đèn thu/phát.

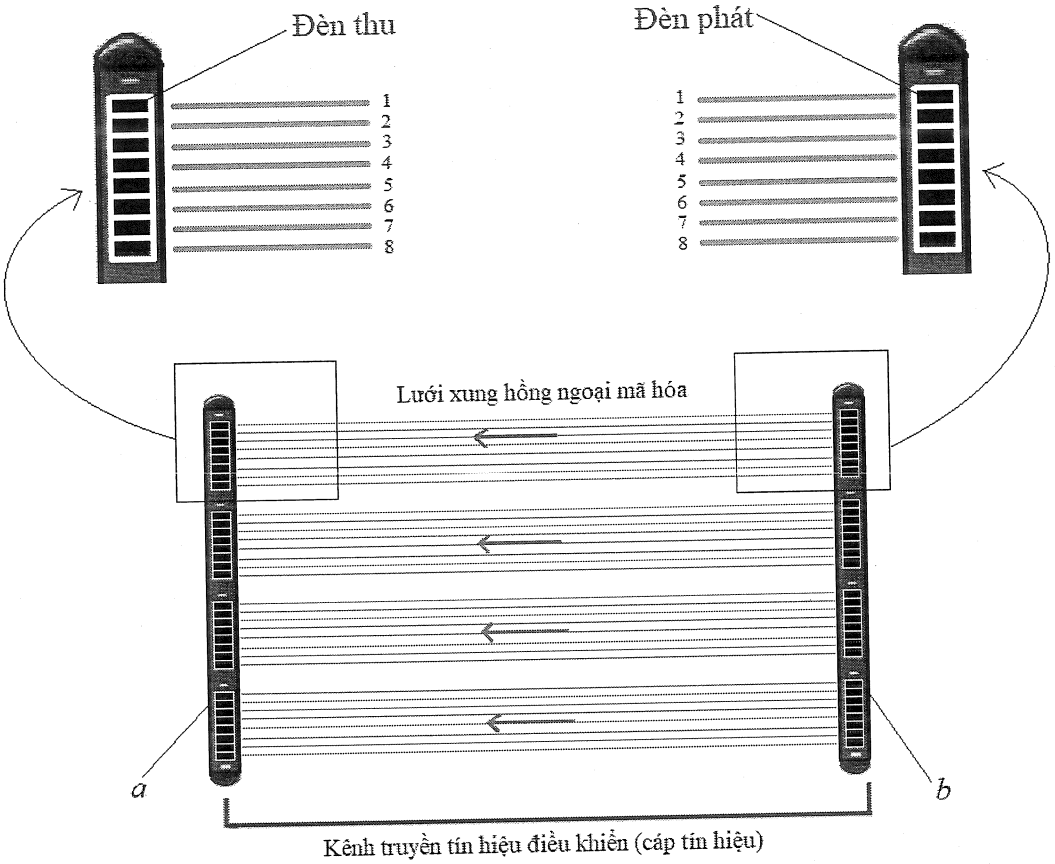
20. Hệ thống hàng rào điện tử thông minh theo điểm 19, trong đó, số đèn thu/phát của mô đun là 8.

21. Hệ thống hàng rào điện tử thông minh theo điểm 16, trong đó, trên cặp cột thu và cột phát tại mỗi mắt xích có nhiều mô đun.

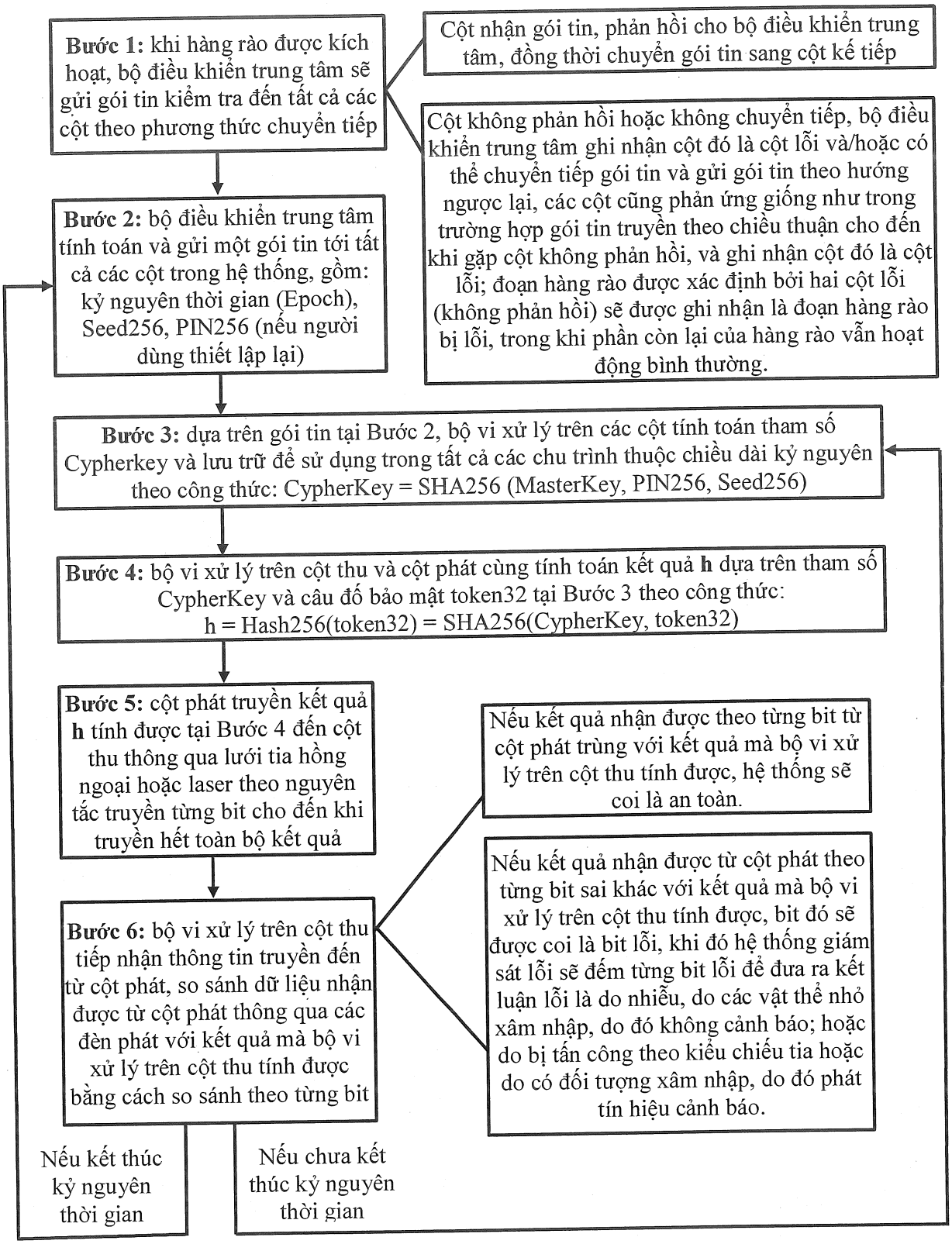
Hình 1.


a
b
01
02
03
04
05
k
k - 1
Bộ điều khiển trung tâm
Kênh truyền tín hiệu điều khiển (cáp tín hiệu)

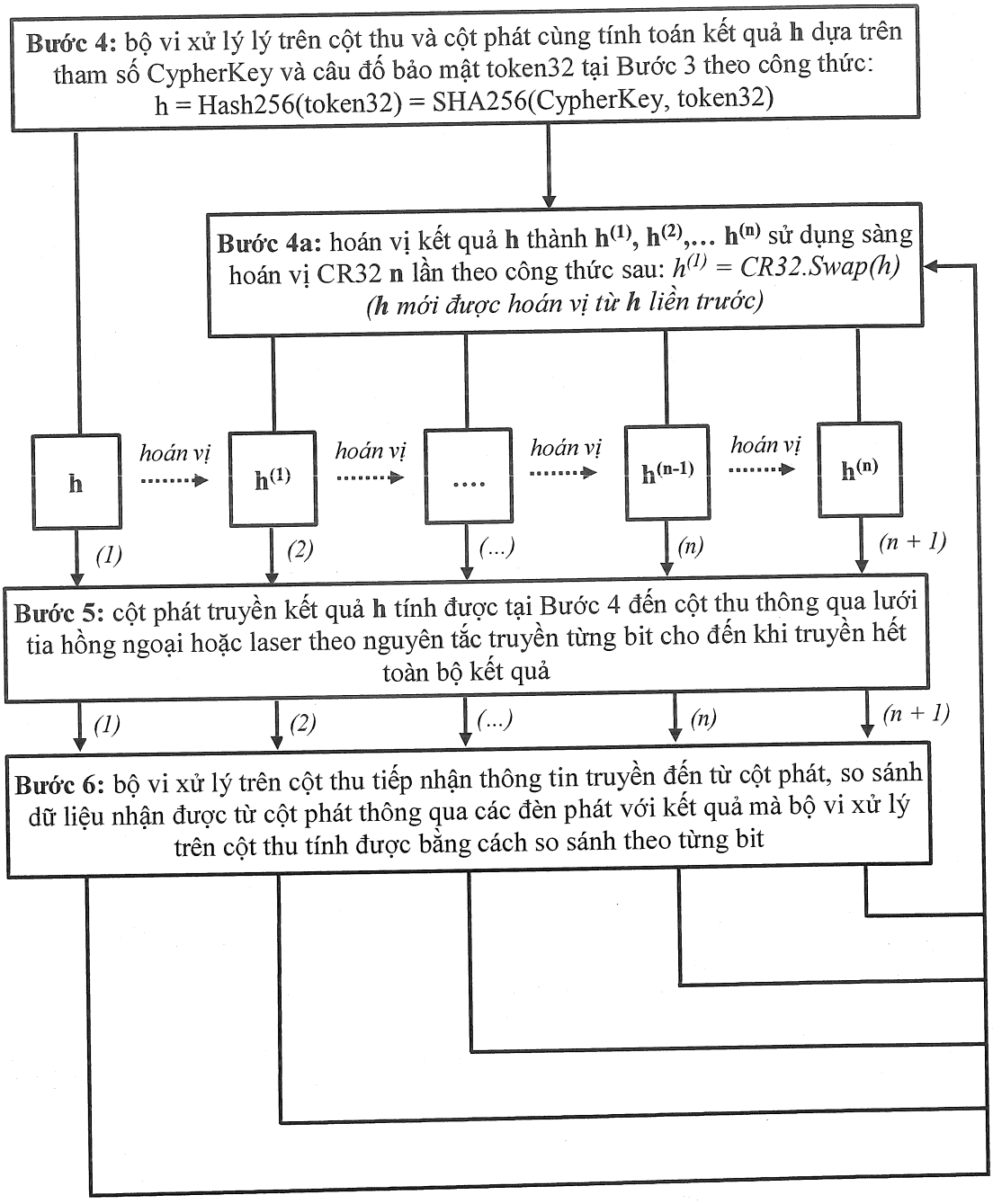
Hình 2.


Đèn thu
1
2
3
4
5
6
7
8
Đèn phát
1
2
3
4
5
6
7
8
Lưới xung hồng ngoại mã hóa
a
b
Kênh truyền tín hiệu điều khiển (cáp tín hiệu)

Hình 3.

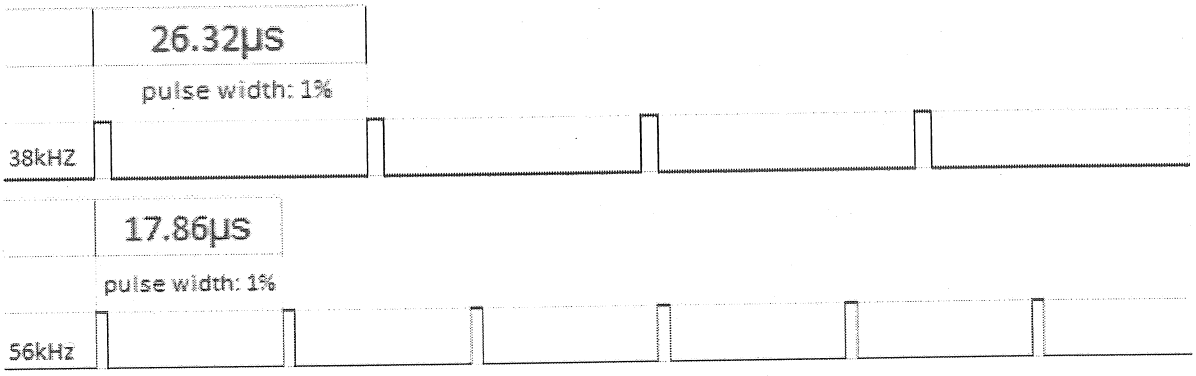

Bước 1: khi hàng rào được kích hoạt, bộ điều khiển trung tâm sẽ gửi gói tin kiểm tra đến tất cả các cột theo phương thức chuyển tiếp
Cột nhận gói tin, phản hồi cho bộ điều khiển trung tâm, đồng thời chuyển gói tin sang cột kế tiếp
Cột không phản hồi hoặc không chuyển tiếp, bộ điều khiển trung tâm ghi nhận cột đó là cột lỗi và/hoặc có thể chuyển tiếp gói tin và gửi gói tin theo hướng ngược lại, các cột cũng phản ứng giống như trong trường hợp gói tin truyền theo chiều thuận cho đến khi gặp cột không phản hồi, và ghi nhận cột đó là cột lỗi; đoạn hàng rào được xác định bởi hai cột lỗi (không phản hồi) sẽ được ghi nhận là đoạn hàng rào bị lỗi, trong khi phần còn lại của hàng rào vẫn hoạt động bình thường.
Bước 2: bộ điều khiển trung tâm tính toán và gửi một gói tin tới tất cả các cột trong hệ thống, gồm: kỷ nguyên thời gian (Epoch), Seed256, PIN256 (nếu người dùng thiết lập lại)
Bước 3: dựa trên gói tin tại Bước 2, bộ vi xử lý trên các cột tính toán tham số Cypherkey và lưu trữ để sử dụng trong tất cả các chu trình thuộc chiều dài kỷ nguyên theo công thức: CypherKey = SHA256 (MasterKey, PIN256, Seed256)
Bước 4: bộ vi xử lý trên cột thu và cột phát cùng tính toán kết quả **h** dựa trên tham số CypherKey và câu đố bảo mật token32 tại Bước 3 theo công thức:
h = Hash256(token32) = SHA256(CypherKey, token32)
Bước 5: cột phát truyền kết quả **h** tính được tại Bước 4 đến cột thu thông qua lưới tia hồng ngoại hoặc laser theo nguyên tắc truyền từng bit cho đến khi truyền hết toàn bộ kết quả
Nếu kết quả nhận được theo từng bit từ cột phát trùng với kết quả mà bộ vi xử lý trên cột thu tính được, hệ thống sẽ coi là an toàn.
Nếu kết quả nhận được từ cột phát theo từng bit sai khác với kết quả mà bộ vi xử lý trên cột thu tính được, bit đó sẽ được coi là bit lỗi, khi đó hệ thống giám sát lỗi sẽ đếm từng bit lỗi để đưa ra kết luận lỗi là do nhiễu, do các vật thể nhỏ xâm nhập, do đó không cảnh báo; hoặc do bị tấn công theo kiểu chiếu tia hoặc do có đối tượng xâm nhập, do đó phát tín hiệu cảnh báo.
Bước 6: bộ vi xử lý trên cột thu tiếp nhận thông tin truyền đến từ cột phát, so sánh dữ liệu nhận được từ cột phát thông qua các đèn phát với kết quả mà bộ vi xử lý trên cột thu tính được bằng cách so sánh theo từng bit
Nếu kết thúc kỷ nguyên thời gian
Nếu chưa kết thúc kỷ nguyên thời gian

Hình 4.

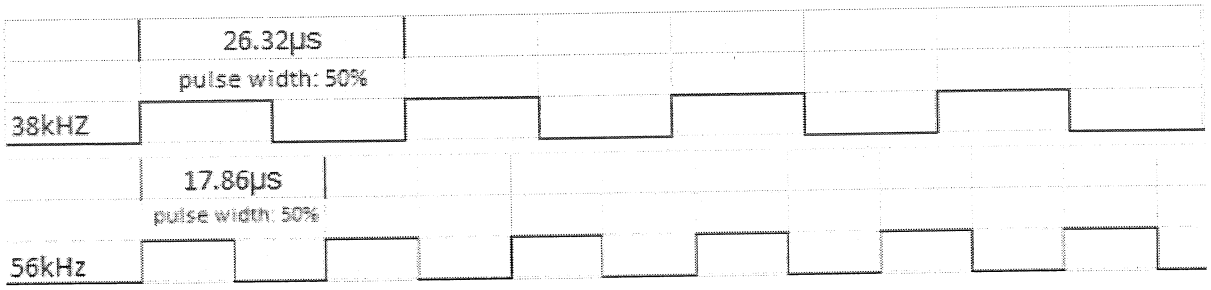

Bước 4: bộ vi xử lý lý trên cột thu và cột phát cùng tính toán kết quả **h** dựa trên tham số CypherKey và câu đố bảo mật token32 tại Bước 3 theo công thức: h = Hash256(token32) = SHA256(CypherKey, token32)
Bước 4a: hoán vị kết quả **h** thành $\mathbf{h^{(1)}}$, $\mathbf{h^{(2)}}$,... $\mathbf{h^{(n)}}$ sử dụng sàng hoán vị CR32 **n** lần theo công thức sau: $h^{(1)} = CR32.Swap(h)$ *(**h** mới được hoán vị từ **h** liền trước)*
h
hoán vị
$\mathbf{h^{(1)}}$
hoán vị
....
hoán vị
$\mathbf{h^{(n-1)}}$
hoán vị
$\mathbf{h^{(n)}}$
(1)
(2)
(...)
(n)
(n + 1)
Bước 5: cột phát truyền kết quả **h** tính được tại Bước 4 đến cột thu thông qua lưới tia hồng ngoại hoặc laser theo nguyên tắc truyền từng bit cho đến khi truyền hết toàn bộ kết quả
(1)
(2)
(...)
(n)
(n + 1)
Bước 6: bộ vi xử lý trên cột thu tiếp nhận thông tin truyền đến từ cột phát, so sánh dữ liệu nhận được từ cột phát thông qua các đèn phát với kết quả mà bộ vi xử lý trên cột thu tính được bằng cách so sánh theo từng bit

Hình 5.

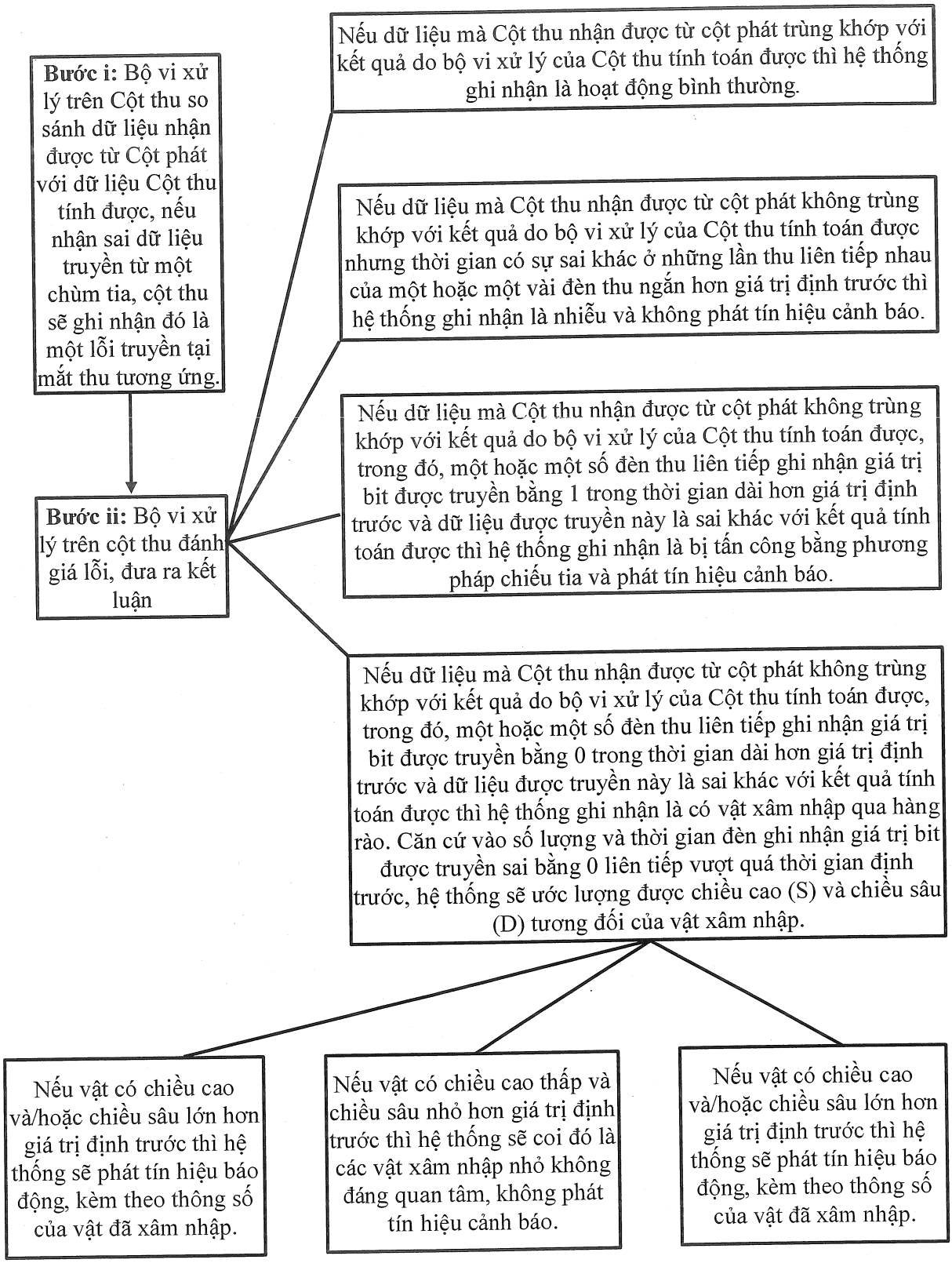
Phương pháp phát tia sử dụng kỹ thuật xung mảnh 1% (ThinPulse) của sáng chế:



Phương pháp phát tia sử dụng tần số sóng mang có độ rộng xung 50% thông thường:



Hình 6.


Bước i: Bộ vi xử lý trên Cột thu so sánh dữ liệu nhận được từ Cột phát với dữ liệu Cột thu tính được, nếu nhận sai dữ liệu truyền từ một chùm tia, cột thu sẽ ghi nhận đó là một lỗi truyền tại mắt thu tương ứng.
Bước ii: Bộ vi xử lý trên cột thu đánh giá lỗi, đưa ra kết luận
Nếu dữ liệu mà Cột thu nhận được từ cột phát trùng khớp với kết quả do bộ vi xử lý của Cột thu tính toán được thì hệ thống ghi nhận là hoạt động bình thường.
Nếu dữ liệu mà Cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của Cột thu tính toán được nhưng thời gian có sự sai khác ở những lần thu liên tiếp nhau của một hoặc một vài đèn thu ngắn hơn giá trị định trước thì hệ thống ghi nhận là nhiễu và không phát tín hiệu cảnh báo.
Nếu dữ liệu mà Cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của Cột thu tính toán được, trong đó, một hoặc một số đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 1 trong thời gian dài hơn giá trị định trước và dữ liệu được truyền này là sai khác với kết quả tính toán được thì hệ thống ghi nhận là bị tấn công bằng phương pháp chiếu tia và phát tín hiệu cảnh báo.
Nếu dữ liệu mà Cột thu nhận được từ cột phát không trùng khớp với kết quả do bộ vi xử lý của Cột thu tính toán được, trong đó, một hoặc một số đèn thu liên tiếp ghi nhận giá trị bit được truyền bằng 0 trong thời gian dài hơn giá trị định trước và dữ liệu được truyền này là sai khác với kết quả tính toán được thì hệ thống ghi nhận là có vật xâm nhập qua hàng rào. Căn cứ vào số lượng và thời gian đèn ghi nhận giá trị bit được truyền sai bằng 0 liên tiếp vượt quá thời gian định trước, hệ thống sẽ ước lượng được chiều cao (S) và chiều sâu (D) tương đối của vật xâm nhập.
Nếu vật có chiều cao và/hoặc chiều sâu lớn hơn giá trị định trước thì hệ thống sẽ phát tín hiệu báo động, kèm theo thông số của vật đã xâm nhập.
Nếu vật có chiều cao thấp và chiều sâu nhỏ hơn giá trị định trước thì hệ thống sẽ coi đó là các vật xâm nhập nhỏ không đáng quan tâm, không phát tín hiệu cảnh báo.
Nếu vật có chiều cao và/hoặc chiều sâu lớn hơn giá trị định trước thì hệ thống sẽ phát tín hiệu báo động, kèm theo thông số của vật đã xâm nhập.