Journal of educational equipment: Applied research, Volume 1, Issue 298 (October 2023)
ISSN 1859 - 0810

Sơ đồ quản lý khóa mạng cảm biến không dây từ góc độ phân cụm

Mai Trung Đông*, Nguyễn Thị Trang Nguyên*
**Học viện Hành chính Quốc gia*
Received: 25/8/2023; Accepted: 6/9/2023; Published: 19/9/2023

Abstract: *Society is increasingly developing in terms of application of diverse information systems in all fields of science, industry, agriculture, economic and trade, finance, healthcare, ... which all promote security and safety. Key management has become a key security issue in the operation of wireless sensor networks today. This article studies key management solutions for wireless sensor networks from a clustering perspective. Through a brief analysis based on the relevant issues present in today's key management solutions, the application of hierarchical routing protocols is explained and then a sensor network key management solution is proposed. new wireless transformer. It is found that by using the clustering information as clustering in the base station to complete the key distribution, it can be included in the secure communication clustering between network nodes and can be applied on a large scale. Large scale for network security system of unlimited sensors.*

Keywords: *Clustering perspective; Wireless sensors; Manage network keys*

1. Giới thiệu

Hiện nay cảm biến mạng không dây được sử dụng rộng rãi trong quân sự hóa, cứu hộ khẩn cấp và cứu trợ thiên tai cũng như công tác an ninh khu vực. Trong quá trình sử dụng kết nối mạng để truyền dữ liệu thường phát sinh những vấn đề nguy hiểm như trộm cắp có ác ý hoặc bị kẻ thù giả mạo [1]. Các nút cảm biến có khả năng bị bẻ khóa bởi những người có động cơ thầm kín, do đó không thể đảm bảo an ninh vận hành chung của mạng. Liệu mạng có thể an toàn hơn hay không có thể được áp dụng cho mạng cảm biến không dây [2]. Để đảm bảo thực hiện an ninh mạng tốt hơn, thường cần phải xây dựng một hệ thống an ninh mạng tương ứng. Việc xây dựng quản lý khóa là cơ sở đảm bảo an ninh cho mạng cảm biến không dây, bao trùm toàn bộ vòng đời của khóa. Bản thân các cảm biến không dây có nhiều đặc điểm, chẳng hạn như năng lượng hạn chế, khả năng tính toán và không gian lưu trữ hạn chế cũng như không có khả năng đảm bảo an ninh vật lý trong các nút mạng; Năng lượng và băng thông truyền thông tương đối hạn chế [3].

2. Nội dung nghiên cứu

2.1. Giải pháp quản lý khóa mạng cảm biến vô hạn dựa trên phối cảnh phân cụm

2.1.1. Ý tưởng xây dựng kế hoạch quản lý

Khi nền công nghệ thông tin mạng của nước ta tiếp tục đổi mới và phát triển, sự phát triển của nhiều ngành công nghệ thông tin như truyền thông, máy tính, cảm biến cũng đang dần tăng tốc. Việc ứng dụng và phát triển rộng rãi của công nghệ mạng cảm biến không dây cũng dần dần mở rộng quy mô phát triển mạng tổng thể. Giao thức định tuyến phân cấp chiếm vị trí thống trị trong các mạng cảm biến không dây và thực hiện việc hợp nhất các nút dữ liệu cảm biến khác nhau ở các đầu cụm khác nhau trong việc lựa chọn cụm, do đó nó có thể đạt được mục đích tiết kiệm năng lượng một cách hiệu quả. Trong ứng dụng thực tế của cảm biến không dây, do quy mô tổng thể tương đối lớn [4], việc phân cụm và kết hợp nhiều bước nhảy thường xảy ra để dữ liệu thu thập cuối cùng có thể được truyền đến trạm gốc. Trong mạng cảm biến không dây, ba giai đoạn được thực hiện bằng cách xây dựng khóa phiên: Gán khóa, chia sẻ khóa và tạo khóa. Sơ đồ quản lý khóa mạng cảm biến không dây được xây dựng trong nghiên cứu này trước tiên đảm bảo rằng vị trí của trạm gốc là tuyệt đối an toàn và nguy cơ vi phạm tổng thể là tương đối nhỏ [5]. Đây thường là tiền đề cho sơ đồ phân phối khóa được thực hiện bởi hầu hết các khóa. Cần phải hoàn thành việc lưu trữ trước các khóa phiên Cki và chức năng Hash dựa trên các nút cảm biến mạng khác nhau. Khóa phiên Cki đóng vai trò là khóa mã hóa trong nút mạng và khóa phiên giữa các nút khác nhau sẽ tương ứng với mã định danh nút NID. Các khóa phiên nút mạng khác nhau thường tồn tại cùng nhau, do đó, các khóa phiên nút liên quan sẽ được lấy cho các nút khác nhau. Hàm Hash chủ yếu được sử

dụng giữa hai nút chung có thể có cùng khóa, khóa giao tiếp phiên được triển khai đảm bảo tính nhất quán của hàm Hash giữa các khóa giao tiếp của nút [6].

2.1.2. Giai đoạn phân phối khóa

Trong quá trình thực hiện phân phối khóa mạng, thường được chia thành hai bước: Trạm cơ sở tự phân phối khóa dưới dạng cụm và nút trưởng phân phối khóa dưới dạng nút trong cụm.

a. Trạm gốc phân bổ khóa cho cụm

Trong giai đoạn phân phối khóa, trạm gốc thực hiện việc truyền tín hiệu xung đồng bộ đến các nút mạng khác nhau, từ đó đạt được sự đồng bộ hóa đồng hồ giữa trạm gốc và các nút. Với sự trợ giúp của nhãn thời gian, nhãn thời gian có thể được sử dụng để đồng bộ hóa các đồng hồ giữa các nút và trạm gốc, khoảng cách được xác định [7]. Việc lựa chọn cụm trưởng có thể được hoàn thành trong mạng cảm biến với sự trợ giúp của giao thức phân cụm, sau đó nút trưởng cụm mới có thể gửi thông tin đến trạm gốc, thông báo cho trạm gốc về thông tin cụm trưởng tương ứng và khoảng cách giữa nút và trạm cơ sở. Trạm gốc cũng có thể sử dụng khoảng cách giữa các nút chủ khác nhau để phân bổ danh tính cụm giữa các nút chủ cụm khác nhau [8]. Việc xác định nút giữa các nút chủ khác nhau có liên quan chặt chẽ đến mã định danh của nút chủ. Những người đứng đầu cụm khác nhau cũng có thể khám phá các thành viên cụm của riêng họ và các nút liên quan trong gói đĩa bên trong nút tại trạm nhận dạng của cụm của chính họ kịp thời dưới tác động của quảng bá. Các nút mạng khác nhau chủ yếu sử dụng hai hoặc nhiều nút trưởng cụm để xuất bản các nút quảng bá thông tin liên quan. Các nút mạng khác nhau cũng có thể sử dụng các nút cổng để có được mối quan hệ lân cận vị trí giữa chúng và các cụm, đồng thời xuất bản nhận dạng cụm CLID của riêng chúng một cách kịp thời. 9]. Trạm gốc phân bổ mã định danh khóa KID làm khóa trong không gian khóa S. Sau khi chỉ định kích thước nhóm khóa trong các cụm khác nhau, trạm gốc sẽ hoàn thành việc liên lạc giữa các cụm khác nhau theo khoảng cách khác nhau giữa các cụm và trạm gốc khác nhau. phân bổ. Trong quá trình phân bổ các ký hiệu khóa khác nhau, trạm cơ sở nên kiểm tra thông tin thông báo liên quan mà nó đã nhận được để có được số cụm lân cận có liên quan. Số cụm liền kề tương ứng có ảnh hưởng trực tiếp quyết định đến tỷ lệ phân bổ khóa đạt được giữa các cụm. Số cụm đã hoàn thành việc phân phối các ký hiệu khóa cũng ảnh hưởng đến tỷ lệ các khóa liền kề trong nhóm khóa của cụm Quyết định. Sau khi các nhóm khóa giữa các cụm khác nhau được phân bổ, trạm cơ sở có thể mã hóa các ký hiệu khóa được phân bổ bởi các cụm khác nhau và gửi chúng đến nút chủ cụm sau khi mã hóa các khóa tương ứng.

b. Cụm trưởng phân bổ khóa cho các nút trong cụm

Cụm trưởng không phân bổ các nút từ toàn bộ nhóm khóa mà nó lưu trữ mà phân bổ ngẫu nhiên các nút từ các nút cụm khác nhau trong nhóm khóa. Điều này làm giảm hiệu quả việc lưu trữ khóa trong cụm cho các nút khác nhau. Không gian liên quan được tiêu thụ giúp cải thiện tính bảo mật một cách hiệu quả và tính bảo mật của toàn bộ nhóm khóa. Nếu các khóa được phân phối giữa các nút khác nhau hoặc không gian chiếm giữ bởi một nút tương đối lớn thì có thể xảy ra tình huống một hoặc nhiều nút bị chiếm, do đó nên tránh không gian bị chiếm giữ bởi bộ lưu trữ khóa của các nút trong các cụm khác nhau ... Nếu quá nhỏ, nếu không sẽ dẫn đến xác suất thiết lập liên lạc an toàn giữa các nút khác nhau trong cụm thấp, dễ xảy ra tình trạng "đảo an ninh".

Nút cổng là cơ sở cho giao tiếp an toàn, chủ yếu được sử dụng cho các nút trong cụm, đồng thời áp đặt trực tiếp các nguyên tắc phân phối khóa đặc biệt, khác với phân phối nút thông thường. Trong quá trình xây dựng cụm, cần đảm bảo cụm nào sẽ được kết nối với các nút cổng khác nhau và đảm bảo rằng giao tiếp giữa các cụm có thể giải mã và xác minh các chức năng. Các nút cổng khác nhau cũng phải được kết nối chặt chẽ với các nút trưởng của các cụm khác nhau, do đó việc phân phối khóa nút của cổng có nguồn gốc từ các cụm kết nối khóa khác nhau. Bằng cách giả sử rằng kích thước không gian của các nút khác nhau trong cụm là k, khi đó số cụm cụ thể được kết nối bởi các nút cổng khác nhau là L, do đó, các khóa giữa các cụm L trở thành không gian khóa được phân bổ bởi nút cổng.

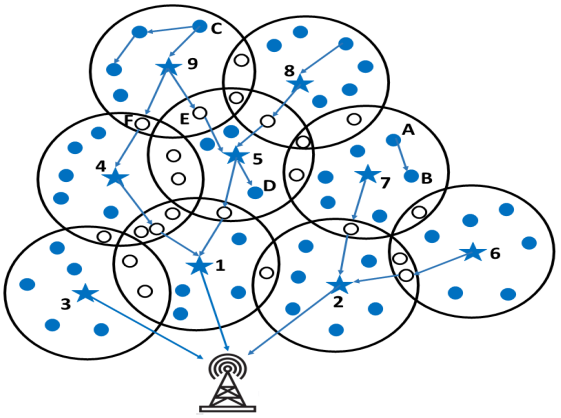
2.2. Xây dựng khóa đường dẫn

Để xây dựng các khóa bằng nhau giữa hai nút chung, bằng cách hoàn thành đường dẫn lưu trữ trước của hàm Hash trên các nút khác nhau, sau đó sử dụng phương thức nội bộ của sơ đồ phân phối trước khóa ngẫu nhiên, có thể đạt được sự sắp xếp KID giữa nhiều khóa. Giao tiếp nhiều mặt đạt được giữa hai nút khóa chung trong các cụm khác nhau và chúng có thể giao tiếp với các nút có cùng khóa giữa hai nút khác nhau này. Để giảm năng lượng tiêu thụ giữa các nút chủ, trong quá trình giao tiếp nút trong cụm, cần tránh chọn nút giữa làm nút chủ cụm càng nhiều càng tốt. Ở chế độ truy vấn trạm gốc, trạm gốc

cũng phải gửi yêu cầu truy vấn đến các nút khác nhau một cách kịp thời và thông tin liên quan được thu thập giữa các nút khác nhau có thể được gửi đến trạm gốc thông qua nút trưởng.

2.3. Ví dụ về quản lý khóa mạng cảm biến không dây

Bằng cách giả sử rằng các nút mạng cảm biến không dây được chia thành 9 cụm (hình 2.1), giả định rằng giá trị N là 9 và kích thước nhận dạng CLID giữa các cụm khác nhau được xác định bởi khoảng cách giữa cụm trưởng và cụm trạm cơ sở. Sau khi hoàn thành việc phân bổ số cụm nhận dạng CLID, có ba cụm liền kề là 4, 5 và 8, nhưng không có cụm nào trong số ba cụm này được phân bổ nhóm khóa nút. Bằng cách phân bổ nhóm khóa S9 cho cụm 9 trong không gian khóa S, nhóm khóa sau đó được mã hóa và gửi đến nút chủ của cụm 9. Cụm 8 có ba cụm liền kề: 5, 7 và 9. Khi cụm 9 hoàn thành việc phân bổ nhóm khóa, khóa S9 có thể được trích xuất ngẫu nhiên từ nhóm khóa để khám phá phân bổ cụ thể của nhóm khóa (được hiển thị trong bảng 2.1).



Sơ đồ 2.1. Mạng ví dụ

Lưu ý: ★ Đại diện cho nút chủ cụm

○ Đại diện cho nút cổng

● Đại diện cho nút trong cụm

Bảng 2.1. Phân bổ nhóm khóa

Nhóm khóa	S1	S2	S3	S4	S5	S6	S7	S8	S9	Hiện hành
S9	-	-	-	-	-	-	-	-	-	1
S8	-	-	-	-	-	-	-	-	1/3	2/3
S7	-	-	-	-	-	-	-	1/4	0	3/4
S6	-	-	-	-	-	-	1/2	0	0	1/2
S5	-	-	-	-	-	0	1/5	1/5	1/5	2/5
S4	-	-	-	-	1/4	0	0	0	1/4	1/2
S3	-	-	-	1/2	0	0	0	0	0	1/2
S2	-	-	0	0	0	1/3	1/3	0	0	1/3
S1	-	1/4	1/4	1/4	1/4	0	0	0	0	0

3. Kết luận

Bằng cách tận dụng tối đa sơ đồ quản lý khóa được đề xuất trong nghiên cứu này, giao thức định tuyến phân cấp có thể được sử dụng để đạt được sự phân phối khóa trong cụm một cách hợp lý hơn. Và dựa trên sự phân chia hợp lý số lượng khóa trong mỗi cụm, khả năng kết nối an toàn của phân phối khóa tổng thể có thể đạt đến mức phân phối khóa ngẫu nhiên cơ bản. Dựa trên cấp độ mạng cảm biến tổng thể, do các điểm nối khác nhau nên các điểm nối tổng thể của mạng sẽ được tối ưu hóa hơn để tránh ảnh hưởng đến các nút của cụm khác trong thời gian ngắn, đảm bảo tính bảo mật cho mạng cảm biến không dây.

Tài liệu tham khảo

[1]. Li Lanying, Yi Chunhuan, Sun Jianda, et al. *Wireless sensor network key management scheme based on unit element [J]*. Computer Engineering and Applications ,2013(1):88-88.

[2]. Zhang Ji, Du Xiaoni, Li Xu, et al. *Secure wireless sensor network key pre-distribution scheme [J]. Computer application,* 2013,33(7):1851-1853.

[3]. ZhouD, WeiG, ZhangH, et al. *Key-management Scheme Based on Public-key Institution to Clustered Wireless SensorNetworks[J].* Journal of Beijing University of Technology,2016.

[4]. Huang Tinghui, Yang Min, Cui Gengshen, et al. *Wireless sensor network key management routing scheme based on LEACH protocol [J]. Journal of Sensing Technology*, 2014 (8):1143-1146.

[5]. Chen Hao, Huang Haiping. *Wireless sensor network key management scheme based on inter-node trust evaluation algorithm[J]*. Computer Science,2015,42(s1):395-398.

[6]. Syed K U R R, Lee H, Lee S, et al. MUQAMI+: *a scalableand locally distributed key management scheme for clustered sensor networks[J]*. annals of telecommunications - annales des télécommunications, 2010, 65(1-2):101-116.

[7]. Wang Xiaokang, Li Peiyue, Sui Yongxin, et al. *Hexagon-based wireless sensor network key management scheme [J]*. Computer Engineering and Design,2014,35(2):425-429.

[8]. Wei Rong, Zhao Dezheng. *Identity-based clustered key management scheme for wireless sensor network [J].* Journal of Wuhan University (Engineering Edition), 2015,48(4):580-583.