Brief Report
Volume 11:4, 2022

International Journal of Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

A Report on Distributed Schemes in Wireless Sensor Networks

Xiangyang Luo*

Department of Decision and Control Systems, Zhengzhou Institute of Information Science and Technology, Zhengzhou 450001, P.R China

Introduction

A wireless sensor network (WSN) is made up of numerous sensor nodes that are distributed throughout a planned area with no fixed structures and have limited power, computation, and communication capabilities. Applications involving wireless sensor networks high security measures, including military target tracking, border security, and scientific research are in a hazardous setting. Six issues with WSN security exist. In order to conduct wireless communication (ii) Without a stable infrastructure, Sensor Nodes have Limited Resources, and WSN can the network architecture before to deployment is unknown, (v) be enormous and dense, (vi) Risk of Unattended sensors are frequently physically attacked. Security is thus of the utmost importance. Especially when the surroundings is harsh, like in military zones. For illustration, a foe may nodes of sensors. We suggest a group key distribution strategy for WSNs in the IoT scenario in this study. The sensor nodes in WSNs are grouped according to a hierarchical structure in our suggested scheme. In the top wired layer, group keys for the subgroups are distributed to trusted head nodes via an end-to-end secure communication protocol. To reduce the energy consumption of the sensor nodes, the head nodes in the lower wireless layer distribute the group keys using wireless multicast and the underlying tree-based topology [1].

Description

The rest of this essay is structured as follows. The TKH scheme, with which we will compare our scheme in the analysis, group key distribution, group key negotiation, the self-healing theory, and other relevant studies are all reviewed in Section 2 of this article. In Section 3, we outline our suggested group key distribution method, which comprises initialization, assumptions, group key distribution, and rekeying in the lower wireless layer as well as group key distribution in the upper wired layer. In Section 4, we examine the security and effectiveness of our suggested strategy and contrast it with TKH. In Section 5, where we also outline some future work, we finally draw a conclusion to this essay. To provide secure communication between sensor nodes, the sensor network must select the most suitable encryption method from a variety of options. Keys must be used in order for encrypted communications to function properly. They must therefore be created and delivered. The current key management approach has a considerable computational overhead because it requires a lot of resources and takes a while to complete. The network is ineffective as a result of the sensor nodes' constrained bandwidth capacity. IoT controllers are in charge of managing a collection of networks, and this paper outlines a dynamic, scalable technique for key management. When compared to a traditional one-hop, packet loss has been significantly decreased [2].

Conclusion

We will primarily concentrate on key management strategies, although we emphasise that the issue of the unpredictability of the key sequences employed is a crucial one furthermore the query of effective matrix calculations. Additionally, there are those. The issue of security is relevant in particular applications like health care networks Attack detection anomaly. Multiple dangers exist for WSNs, including the following: Attacks on communication, denial of service, node compromise, and impersonation attack that is particular to a protocol. Key management in WSNs is a challenge because nodes only have a finite amount of resources. In the Key management protocols described in literature are either symmetric or asymmetric. Due to resource constraints, (asymmetric functions) are inappropriate [3].

The goal of security, or cyber security, is to protect transmitted data from unauthorised access. Unauthorized data access results from poor security measures. Inappropriate access to sensitive data will cost a corporation employing IoT more than just money. To prevent unwanted access, several strategies can be used, including robust authentication, data encryption, monitoring tools, etc. One of the best methods for ensuring end-to-end security is data encryption. Traditional encryption algorithms cannot be used due to the IoT network's nodes' technical limitations, such as low processing power and limited memory. As a result, various encryption methods like stream cyphers or light-weight block cyphers are appropriate answers for these settings. To provide a compromise between various security requirements for hardware and software environments and performance, security mechanisms must be used [4,5].

Conflict of Interest

None.

References

1. Lan, Hualin. "Acoustical observation with multiple wave gliders for internet of underwater things." IEEE *Internet Things J* 8 (2020): 2814-2825.
2. Feng, Liangbing. "Pheromone based alternative route planning." *Digital Commun Networks* 2 (2016): 151-158.
3. Gbadamosi, Omoniyi Ajoke and Dayo Reuben Aremu. "Design of a Modified Dijkstra's Algorithm for finding alternate routes for shortest-path problems with huge costs." *Inter Conf Math Comp Eng Comp Sci* (ICMCECS) IEEE (2020): 1-6.
4. Li, Xin, Bin He, Yanmin Zhou and Gang Li. "Multisource model-driven digital twin system of robotic assembly." *IEEE Systems J* 15 (2020): 114-123.
5. Zhang, Chao. "A self-heuristic ant-based method for path planning of unmanned aerial vehicle in complex 3-D space with dense U-type obstacles." *IEEE Access* 7 (2019): 150775-150791.

***Address for Correspondence:** Xiangyang Luo, Department of Decision and Control Systems, Zhengzhou Institute of Information Science and Technology, Zhengzhou 450001, P.R China; E-mail: luoxy_ieu25@sina.com*

Received: 05 April, 2022, Manuscript No. sndc-22-68690; **Editor Assigned:** 07 April, 2022, PreQC No. P-68690; **Reviewed:** 15 April, 2022, QC No. Q-68690; **Revised:** 20 April, 2022, Manuscript No. R-68690; **Published:** 25 April, 2022. DOI: 10.37421/2090-4886.2022.11.155

How to cite this article: Luo, Xingkang. "A Report on Distributed Schemes in Wireless Sensor Networks." *J Sens Netw Data Commun* 11 (2022): 155.