ECP 2024 Conference

The 3rd International Electronic Conference on Processes

29–31 May 2024 | Online

Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks

Author 1:- Purushothaman Ramaiah , Author 2 :- Ramakrishnan Narmadha
Affiliation 1:- Research Scholar , Sathyabama Institute of Science and Technology, Chennai.
Affiliation 2:- Associate Professor, Sathyabama Institute of Science and Technology, Chennai.

INTRODUCTION & AIM

In the realm of wireless sensor networks (WSNs), preserving data integrity, privacy, and security against cyberthreats is paramount. Proxy re-encryption (PRE) plays a pivotal role in ensuring secure intra-network communication. However, existing PRE solutions encounter persistent challenges, including processing delays due to the transfer of substantial data to the proxy for re-encryption and the computational intensity of asymmetric cryptography. This study introduces an innovative PRE scheme that is meticulously customized for WSNs to enhance the secure communication between nodes within the network and external data server. The proposed PRE scheme optimizes efficiency by integrating lightweight symmetric and asymmetric cryptographic techniques, thereby minimizing computational costs during PRE operations and conserving energy for resource-constrained nodes. In addition, the scheme incorporates sophisticated key management and digital certificates to ensure secure key generation and distribution, which in turn, facilitates seamless authentication and scalable data sharing among the entities in WSN. This scheme maintains sensor-node data encryption and delegates secure re-encryption tasks exclusively to cluster heads, thereby reinforcing data privacy and integrity. Comprehensive evaluations of security, performance, and energy consumption validated the robustness of the scheme. The results confirm that the proposed PRE scheme significantly enhances the security, efficiency, and overall network lifetime of WSNs

METHOD

Preliminaries

A. WSN Architecture Overview

Wireless sensor networks (WSNs) comprise sensor nodes (SNs), cluster heads (CHs), and data aggregation, governed by communication protocols. SNs, equipped with specialized sensors, form a distributed data-collection network. Cluster formation organizes SNs based on physical proximity, with each cluster led by a CH. CHs collect data from SNs and transmit to a central base station, minimizing redundant transmissions. Hierarchical structures and redundancy bolster WSN resilience. Periodic updates of CHs ensure efficient operation and facilitate intercluster communication. Various wireless protocols and routing algorithms optimize data transmission and network lifetime, customized for specific applications. Security measures like encryption and authentication are crucial due to inherent vulnerabilities.

B. Integrated Lightweight Encryption Methods

1.Lightweight Symmetric Encryption
Speck, a lightweight symmetric encryption algorithm, excels in resource-constrained environments. Its design prioritizes simplicity and efficiency, minimizing computational overhead and memory usage. Speck encrypts data without complex modes of operation, enhancing security and reducing vulnerability risks. Empirical studies demonstrate Speck's superiority over resource-intensive encryption algorithms, making it suitable for secure communication in WSNs.
2.Lightweight Public Key Encryption
Utilizing elliptic curve cryptography (ECC), inspired by ElGamal's work, involves concealing messages through α raised to the power of k and β raised to the power of k. The sender computes the message using a secret parameter a, ensuring secure message retrieval.

PROPOSED PRE ARCHITECTURE FOR WSNs

The architectural design of the proposed PRE-based WSN is presented, whereby we delve into the intricacies of the cryptographic algorithms employed and elaborate on the construction of the security model within the network.

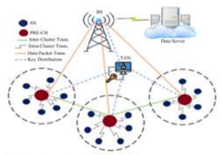
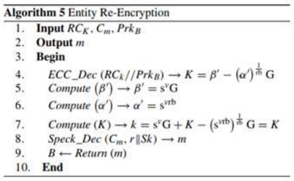


FIGURE 1. Architectural design of the proposed PRE-based WSN.



```
Algorithm 5 Entity Re-Encryption
Input $RC_K, C_m, Prk_B$
Output $m$
Begin
    $ECC\_Dec\ (RC_k//Prk_B) \rightarrow K = \beta' - (\alpha')^{\frac{1}{rb}} G$
    $Compute\ (\beta') \rightarrow \beta' = s^{v}G$
    $Compute\ (\alpha') \rightarrow \alpha' = s^{vrb}$
    $Compute\ (K) \rightarrow k = s^{v}G + K - (s^{vrb})^{\frac{1}{rb}} G = K$
    $Speck\_Dec\ (C_m, r\|Sk) \rightarrow m$
    $B \leftarrow Return\ (m)$
End
```

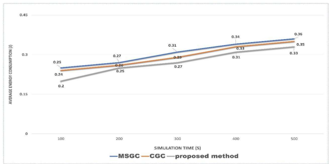
RESULTS & DISCUSSION

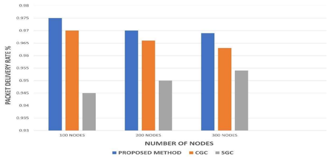
Our proposed protocol consists of three stages: i) gathering node positions and forming clusters, ii) selecting cluster heads, and iii) aggregating and transmitting data, ensuring efficient network communication through node clustering, energy optimization, and data aggregation

Nodes are organized into concentric layers around the base station, forming clusters based on angular values. An algorithm ensures all nodes are assigned to a cluster and localization level. Intermediate nodes gather coordinates from surrounding sensors and transmit them to the base station.

Nodes select cluster heads based on power and position, employing a weight-based algorithm. Data transmission utilizes time division multiple access (TDMA), with CHs aggregating and transmitting data either to the base station or intermediate CHs. Inter-cluster communication optimizes energy use.

Simulation compares proposed approach with CGC and MSGR methods, demonstrating reduced resource consumption and improved packet delivery rate. Proposed method's structured data transfer and predetermined paths enhance delivery rate and reduce collision risks.





CONCLUSION

Proposed protocol employs concentric cluster layers to optimize energy-efficient communication and dynamic node adaptation. Expansion is facilitated by adding concentric cluster layers, ensuring robustness and redundancy in network operation. Further research will determine optimal cluster size for resource management and transmission efficiency in large WSNs.

FUTURE WORK / REFERENCES

[1] Y. Rahayu and F. N. Mustapa, "A secure parking reservation system using GSM technology," *International Journal of Computer and Communication Engineering*, pp. 518–520, 2013, doi: 10.7763/ijcce.2013.v2.239. [1] M. Chen and T. Chang, "A parking guidance and information system based on wireless sensor network," in *2011 IEEE International Conference on Information and Automation, ICIA 2011*, Jun. 2011, pp. 601–605, doi: 10.1109/ICINFA.2011.5949065.
[2] H. C. Yee and Y. Rahayu, "Monitoring parking space availability via Zigbee technology," *International Journal of Future Computer and Communication*, vol. 3, no. 6, pp. 377–380, Dec. 2014, doi: 10.7763/ijfcc.2014.v3.331.

[3] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the Hawaii International Conference on System Sciences*, 2000, vol. vol.1, p. 223, doi: 10.1109/hicss.2000.926982.
[4] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, Oct. 2004, doi: 10.1109/TMC.2004.41.

https://ecp2024.sciforum.net/