Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.2, August : 2024

TRUSTPATHX: ENHANCING SECURE ROUTING IN WIRELESS SENSOR NETWORKS WITH SECURE PATH FINDING

E. Abirami, Research Scholar, Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamil Nadu, India
Dr. Sreejith Vignesh B P Assistant Professor, Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamilnadu, India.

Abstract
In modern communication world the importance of Wireless Sensor Network(WSN) is unavoidable. Security of WSN need more supervision and secured protocols to maintain better security and integrity. It is a basic and prominent way in data transfer among various applications and industries. Due to digitization everything transfer via wireless networks and it need efficient maintenance for interconnected devices. To prevent cyber threats in WSN, it needs the help of path security protocols and algorithms. The utilization of proper security mechanisms is varies for different types of data. Traditional algorithms and protocols not able to fulfill the requirement of current scenario. This study analyse the reliability of network nodes and experimented Secure Path Algorithm to identify the secure data transfer nodes in WSN with help of TrustPathX algorithm and Machine Learning(ML) algorithms Random forest and Neural Networks Algorithm.

Keywords:
secure path algorithm, data security, secure nodes, WSN

Introduction

Wireless Sensor Networks (WSN) is a rising field in the family of modern communication systems. It offers secure data transfer among varies applications such as medical devices, remote monitoring and diagnosis, research and education, transport industry, social media, environment monitoring, smart cities etc. WSN has a position to check most authentication and suitable encryption algorithm for passing secure data. Hence this research utilized the Secure Path Algorithm (SPA) to ensure the secure data communication path to avoid the security breaches and unauthorized access. Machine learning algorithm Random Forest utilized, Neural Networks utilized to identify the trustworthiness of the node with various features. This research experiment and simulate the SPA in different network scenarios to check its performance to prevent security threats and integrity of data transfer. This study address the advanced security solution through Secure Path Algorithm. This algorithm is a improved version of Dijikstra's and its named as TrustPathX. The rest of paper organized as follows: Section 2 summarizes the related work, Section 3 experiment the proposed algorithm TrustPathXfor secure path finding, Section 4 presents result and discussion of the study, Section 5 presents the conclusion and future enhancement.

Literature Review

Network threat and data security is emergency challenge to handle by Wireless Sensor Networks. Secure routing and secure data transfer algorithms helps to overcome cyber threat issue. This literature examines performance of secure algorithms in data transfer and security.Ullah et al.(2009) investigated the Security Protocol for Sensor Networks (SPIN) which contains Secure Network Encryption Protocol(SNEP) and the micro version of the Timed Efficient Stream Loss-tolerant Authentication (μTESLA). These protocols support the data confidentially and two party data authentication.It reduce the memory overhead and maintain limited time [1].
Karlof et al.(2003), proposed energy efficient routing protocol to secure routing in sensor networks and also suggest factors consider for designing the protocols [2].

He et al.(2020), summarized the security mechanism in tryst based routing algorithm and types of attacks , then analyzed the best routing algorithm [3].Reddy et al.(2023), used Master Auditor Node (MAN) from trusted nodes and monitor the each node behaviour. To select trusted route selection author introduce the Energy Efficient Master Auditor Node with Trust based Secure Routing (EE-MAN-TbSR)[4].

Hu et al.(2022), proposed Trust Based Secure and Energy Efficient Routing Protocol (TBSEER) for WSN. It calculates the trust value from energy trust value, indiretc trust value, and adaptive direct trust value.This mechanism increases the speed, reduces the energy consumption and works against the common attacks [5].

Di et al.(2007), analyzed usability of machine learning algorithms for solving networking and application problems and future transformation of machine learning [6].Jean et al. (2012), proposed energy efficient path algorithm to overcome the issues created by symmetric key cryptography algorithms and balance the network energy and improve the network lifetime [7].Shi et al.(2020), used improved version Dijkstra algorithm to find secure path and it results low ratio of packet loss, avoid malicious node [8] .

Methodology

Dijikstra algorithm with machine learning algorithms Random Forest, Neural Networks effectively used to identify the trust score, based on this score improved version of Dijikstra algorithm named TrustPathX find the reliable and secure path for data transmission.

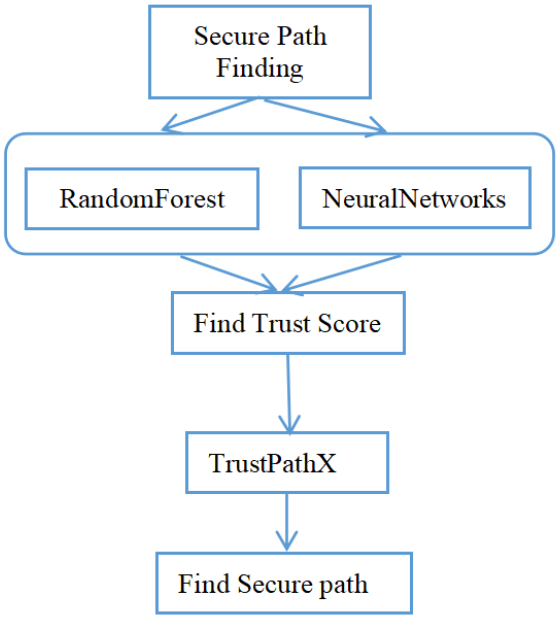


Figure 1. Schematic Workflow

Dijikstra's algorithm

Dijikstra's algorithm is a model used in graph theory and finds the shortest path between nodes. It solves the network routing and optimization problems in WSN. This algorithm works from start node to destination node to find each node distance and each iteration it explores the short route and update it. It used the greedy strategy to find shortest path and find the optimal path. Weight in the each node or edge denotes the cost or distance between nodes. Hence this algorithm find the shortest path from single source node to remaining nodes in the graph. In this study same algorithm improved with machine learning algorithms random forest and neural networks to obtain trust score and found the secure route for data transfer.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.2, August : 2024

In this digital era support of machine learning algorithms needed in every field. In WSN the ML algorithms works to check trustworthiness of the node. Role of ML in WSN as follows

1. It helps to find unusual patterns and anomalies detection.
2. It optimize the energy consumption
3. It helps to calculate the trust score thereby finding secure path
4. It evaluates the trustworthiness of nodes
5. It finds the node failure.

Algorithm steps

Step 1. Data fetched for Packet Delivery ratio, energy, cooperation, transmission success rate, packet loss rate, trust labels (Synthetic data was created).
Step 2. Relevant features were extracted from given data.
Step 3. Trust scores were predicted by machine learning algorithms Random Forest and Naive Bayes separately from extracted features .
Step 4. Integrate trust score with TrustPathX algorithm to find secure path.
Step 5. Evaluate the accuracy of secure node by data delivery ratio and latency.

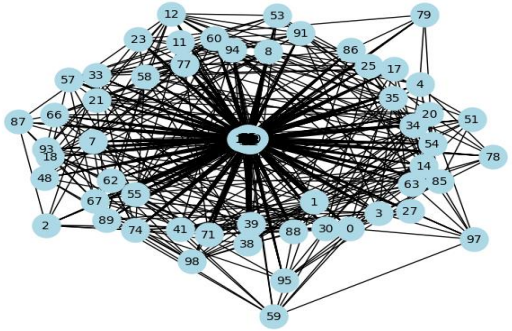
Following figure shows the features and description of synthetic dataset

	node_id	pdr	energy	cooperation	trust_label	\
0	0	0.352529	0.703280	0.782924	0	
1	1	0.722684	0.402526	0.442655	1	
2	2	0.319225	0.920040	0.485267	0	
3	3	0.905912	0.650255	0.777909	1	
4	4	0.126637	0.090419	0.382363	0	

	transmission_success_rate	packet_loss_rate
0	0.841096	0.334105
1	0.996849	0.521831
2	0.430343	0.585654
3	0.320299	0.008496
4	0.906653	0.761006

Figure 2. Network data

Where PDR - packet delivery ratio
Energy - residual energy of the node
Cooperation - cooperation level of the node
Transmission Success Rate - proportion of successful data transmissions
Packet Loss Rate - percentage of packet lost during transmission
Trust Label - trustworthiness label assigned for each node
Following graph shows the 1 to 100 nodes in the experimented data.



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.2, August : 2024

Figure 3. Graph with Nodes

Result and Discussion

This section discuss experiment results in detailed manner as follows.Random forest (RF) and neural network (NN) found the trust score for following nodes.

Table 1. Trust Score

Trust Score	RF	NN
Node 0	0.96	0.98
Node 85	0.74	0.78
Node 96	0.79	0.81
Node 99	0.99	1

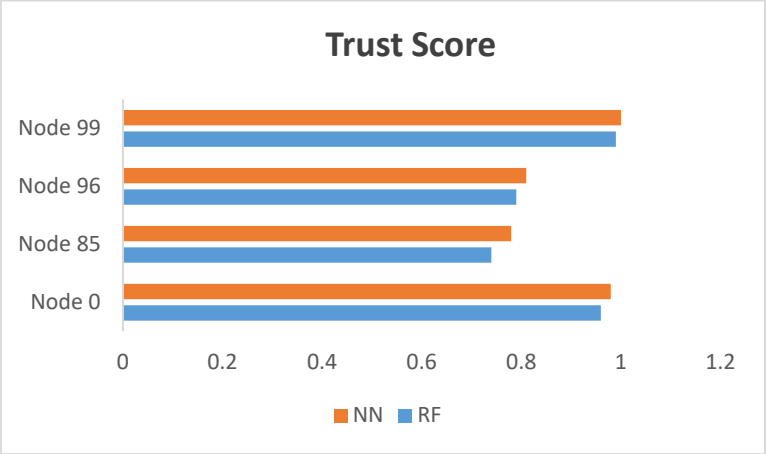


Figure 4. Trust Score from RF & NN

From the table and figure its observed that both algorithm detect the trustworthiness of the node. Higher score indicate the reliable node and denote the trustworthiness. While lower trust score represents the less reliable. In the table Node 0, Node 85, Node 96, Node 99 trustworthy scores were different for RF and NN. At the same time both algorithm found same nodes as trustworthy nodes. From the experiment result its confirmed that Neural Networks predict the trustworthy score higher rate than than Random Forest. So this study used NN trust scores for next phase. Those nodes differ in few values, so that Machine learning algorithm successfully detect the trust worthy nodes and further these nodes were experimented by TrustPathX algorithm.

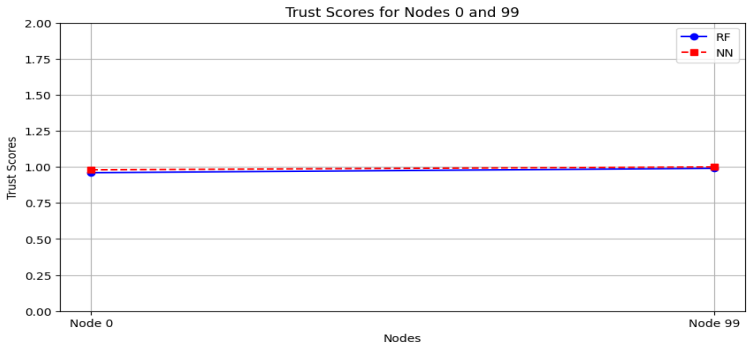


Figure 5. Secure Path Node 0 to 99

Based on the trust score TrustPathX find the secure path is Node 0 to 99. The initial node is 0 and destination node is 99. From this result , proposed algorithm found Node 0 to 99 is safest and simplest path for secure data transfer. The following figure shows the secure path from node 0 to 99.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.2, August : 2024

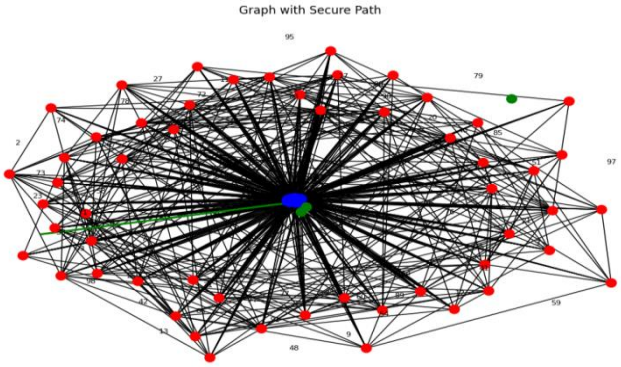


Figure 6. Secure path in graph

In this fig 6 green colour line shows the secure path from Node 0 to Node 99. Red colour shows the trustworthy nodes and blue colour shows untrustworthy nodes.

The Node 0 to 99 was checked by finding the performance metrics Data Delivery Ratio and Latency. From the secure path 0 to 99 the data transfer carried out to check the reliability of the route.

Data Delivery Ratio	1.0
Latency	50ms

Table 2 : Performance Metrics

Data Delivery Ratio represents the ratioof successfully delivered data and total number of packets transferred.

DDR - 1.0 denoted successful delivery of data without any loss

Latency 50 milliseconds indicates the data packets were transfer with less latency

These results confirmed that the proposed algorithm TrustPathX provide the secure path to prevent data loss and controls the data breach.

Findings:

Machine learning algorithms efficiently detect the trust worthy nodes by eliminating bias in the network.

Proposed algorithm TrustPathX successfully predict the proper safe node for secure data transfer.

The secure path node is 0 to 99.

Conclusion

Now a days data is everything hence threat free data can empower the industries development. Data security and secured data transfer is challenging task for WSN which also need to provide optimized network performance and resource utilization. Hence this research utilized machine learning algorithms Random Forest and Neural Networks in phase 1 and these algorithms found node 0, node 85, node 96 and node 99 as trust worthy nodes. In that nodes NN produced higher trustworthy score than RF. Hence phase2 used trust node from NN with TrustPathX algorithm to identified the secure node. Finally this research identified secure path node 0 to 99 for data transfer.

References

1. Ullah, Fasee & Mehmood, Tahir & Habib, Masood & Ibrahim, Muhammad. (2009). SPINS: Security Protocols for Sensor Networks.

2. Karlof, Chris & Wagner, David. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Ad Hoc Networks. 1. 293-315. 10.1016/S1570-8705(03)00008-8.

3. He, Junyao & Xu, Feng. (2020). Research on Trust-Based Secure Routing in Wireless Sensor Networks. Journal of Physics: Conference Series. 1486. 022052. 10.1088/1742-6596/1486/2/022052.

4. Reddy, D. M. K. ., Sathya, R. ., & Lakshmi, V. V. A. S. . (2023). An Energy Efficient Master Auditor Node with Trust Based Secure Routing in Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(3), 519–529.
5. Hu, Y. Han, M. Yao and X. Song, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," in IEEE Access, vol. 10, pp. 10585-10596, 2022, doi: 10.1109/ACCESS.2021.3075959.
6. Di, Ma & Er, Joo. (2008). A survey of machine learning in Wireless Sensor netoworks From networking and application perspectives. 1 - 5. 10.1109/ICICS.2007.4449882.
7. Jean de Dieu I, Assouma N, Muhamad M, Jin W, Lee S. Energy-Efficient Secure Path Algorithm for Wireless Sensor Networks. International Journal of Distributed Sensor Networks. 2012;8(4). doi:10.1155/2012/751784
8. Shi Q, Qin L, Ding Y, Xie B, Zheng J, Song L. Information-Aware Secure Routing in Wireless Sensor Networks. Sensors. 2020; 20(1):165. https://doi.org/10.3390/s20010165