International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 36 • 2017

Secure Clustering and Trustworthy Routing Protocol in WSN

Uma Maheswari P[a] and Ganeshbabu TR[b]

[a]*Research Scholar, Faculty of Information and Communication, Anna University, Chennai, India. Email: umapmaheswari@gmail.com*
[b]*Professor, Department of Electronics and Communication Engineering, Muthayammal Engineering College, Rasipuram, India*

Abstract: The rapidly developing sensor network technology has a broad range of applications, such as wireless sensor networks (WSNs), and emergency and military communications. Due to the characteristics such as openness and dynamic topology, ad-hoc networks suffer from various attacks in the data plane. Even worse, some attacks can subvert or bypass the frequently used identity-based security mechanisms. In this paper, we introduce Secure Clustering and trustworthy Routing Protocol in WSN (SCTRP), which is used to estimate the node trust and reliable routing in WSNs. In this scheme, the Cluster Head (CH) elected based on the Node Trust. The Node Trust calculated by energy. The signature verification algorithm and one-way hash chain function are used to provide the authentication and secure communication in the network. The simulation result shows that the SCTRP improve the network performance and increase the network lifetime in the network.

Keywords: Trust, Signature Verification, One-way hash chain, Clustering, Wireless Sensor Network.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are rising as a hopeful tech due to a large collection of applications such as environmental monitoring, industrial, military and civilian domains because of economic considerations, straightforward and cheap cost. However, it suffers from different types of attacks. The opponent compromises a node and loss all data packets that are routed through this node, consequential in sensitive data being unused or not capable of being transmitted to the sink. Since the network makes decisions depending on the nodes sensed data. As a result, the system will utterly fail and construct wrong decisions. Hence, detect and avoid the attack is great significance for security in WSNs.

The current trust-based route strategies face some challenging issues. However, getting the trust of a node is complex. In WSNs, the node energy is very limited. The trust gaining and transmission have high-energy utilization; that affects the lifetime of the network. In WSNs, the security route is a challenging issue. Because difficult to identify the malicious nodes. Hence overcome these problems, we propose Secure Clustering and trustworthy Routing Protocol in WSN (SCTRP). Security and trust routing provides reliable routing in WSNs. Here, the CH elected based on the node trust and trust computation based on the node energy. Thus, it provides

better energy efficiency. The signature verification method checks the sensor node send the data through an authenticated node in the networks.

The rest of this paper is structured as follows. In Section 2, describes the related works. In Section 3, Secure Clustering and trustworthy Routing Protocol in WSN (SCTRP) had presented. Performance and analysis are evaluated in Section 4. Section 5 presents the conclusion.

2. RELATED WORKS

In [2], first, technical challenges and design principles are introduced concerning hardware development, system architectures and protocols, and software development. Specifically, radio technologies, energy harvesting techniques, and cross-layer design for IWSNs have been discussed. In addition, IWSN standards are presented for the system owners, who plan to utilize new IWSN technologies for industrial automation applications.

In wireless sensor and actuator networks (WSANs), the sensor nodes are involved in gathering information about the physical phenomenon, while the actuator nodes take decisions and then perform appropriate actions upon the environment. The collaborative operation of sensor and actuator nodes brings significant advantages over WSNs, including improved accuracy and timely actions upon the sensed phenomena. However, unreliable wireless communication and finding a proper control strategy cause challenges in designing such network control system. In [3], the coordination and communication problems in WSANs are studied. First, the authors formulate the mathematical models for the WSANs system. Then, a predictor-controller algorithm based on distributed estimation is adopted to mitigate the effects of network-induced delay. Finally, the authors apply a collaborative processing mechanism to meet the desired system requirements and improve the overall control performance. This approach will group the sensor and actuator nodes to work in parallel to reduce the computation complexity and enhance the system reacting time.

In [4] proposed a decentralized algorithm to calculate the control signals for lights in wireless sensor networks. This algorithm uses an appropriate step size in the iterative process used for quickly computing the control signals. The authors demonstrate the accuracy and efficiency of this approach compared with the penalty method by using Mote-based mesh sensor networks. The estimation error of the new approach is one-eighth as large as that of the penalty method with one-fifth of its computation time. In addition, the authors describe a sensor/actuator node for distributed lighting control based on the decentralized algorithm and demonstrate its practical efficacy.

Fusion Prediction-Based Interacting Multiple Models (FPB-IMM) algorithms [5] utilizes multiple position measurements produced by trilateration and a self-tuning algorithm; it takes advantage of these various measures to minimize the effect of noisy measurements and the low data rates by modifying a cycle of IMM with fusion prediction. Virtual Certificate Authority [6] proposed key management technique used to overcome the difficulties in securing the networks. The sink collects sensor information securely, and it sends collect the information to the BS. This scheme improves the energy performance, communication overhead, and packet loss in WSNs. An energy-efficient data privacy protection system (EDPPS) [7] used to achieve security and confidentiality for transmitted sensed data within an energy-efficient network. It ensures secure transmission of data from the source sensors to the BS in a way that it can consume the available amount of energy. One-way hash function and shared secret keys for ensuring security service on the sensed data. It increases the network lifetime. It provides security data transmission from the source node to BS through three security services such as Confidentiality, Authenticity and integrity of the real Sensed Data. EDPPS provides a right level for energy consumption as well as maximizing the network lifetime.

An enhanced secure sensor association and key management protocol [8] introduced based on elliptic curve cryptography and hash chains. The authentication procedure and group key generation are very straightforward

and efficient. This protocol reduces the computation and communication cost for the authentication and key derivation. Public Key Infrastructure [9] used to solve the problem of security and ensuring the authenticity of the BS in WSN. This algorithm composed two phases, the first step using the handshake; it is protected and authenticated using the public key of the base station. The second step is the use of this session key for data encryption to ensure confidentiality and ensuring the integrity of the exchanged data.

Secure Communication for Cluster-Based WSNs [9] an intensive hashing and symmetric key cryptography based approach is proposed to secure data communication in WSN to achieve preservation of data integrity and confidentiality. This approach there is little energy consumption in WSN. Secure and Distributed Reprogramming for Wireless Sensor Networks [10] was proposed for industrial monitoring applications. The technique consisted of distribution of authorization to the privileged list of users in an already programmed group of sensor nodes in a WSN while performing the reprogramming operation. However, this scheme lack of Identity Based-Signature, lack of connected databases and data services of integrity on real data sets and lack of energy conservation analysis in the network.

Secure and Trustable Routing (STR) in WSNs [11] improves the data route security. This scheme keeps away from black holes through the node trust to quickly detect and provide security in WSN. Active Trust project can entirely use the energy in non-violence to produce as many discovery routes as essential to achieving the required safety and energy efficiency. Active Trust can importantly improve the packet transmission route and optimize network lifetime. Trust management [12] system introduced fuzzy logic is used to evaluate the path trust value. This trust path value is used to find the trusted route in the network. It is simple but efficient trustworthiness routing decision is to provide in WSNs.

3. PROPOSED METHOD

This paper proposes Secure Clustering and trustworthy Routing Protocol in WSN (SCTRP) investigate secure communication and transmit the data through the reliable route in a WSN. In this scheme, the CH elected by node Trust. The trust calculation based on the remaining energy of node. The signature verification and one-way hash chain provide secure communication in the network. The SCTRP scheme consists of 3 phase such as Network formation phase, CH selection phase, Data transmission phase. Figure 1 shows the architecture of SCTRP scheme.

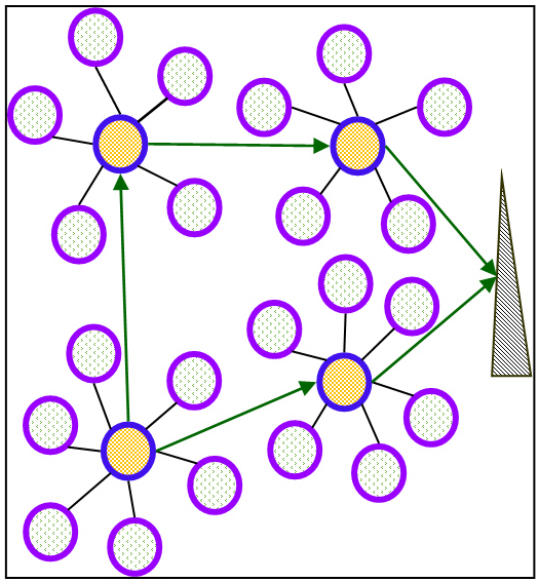

Figure 1: Sample Architecture of Proposed scheme

Network Formation Phase

In Network formation phase, the sensor nodes are grouped into clusters, and the clusters are formed depend on sensor node coverage. In every cluster, all cluster members are choosing the one head that is known as Cluster Head (CH).

CH Selection Phase

In SCTRP, the CH elected based on the node trust. Every round, the CH chooses the boundary based on the threshold i.e. computed by recommended percentage of CHs for the entire network. The Node trust value is above the threshold that node is selected as the CH.

The average energy of cluster computation is defined as

$$\text{AvgEn}(C) = \sum_{cm=1}^{n} \frac{\text{RE}_{cm}}{n} \tag{1}$$

The probability of CH calculation is given below.

$$\text{P}_{\text{CH}} = \text{G} \frac{\text{RE}_{\text{CM}}}{\text{AvgEn}(C)} \tag{2}$$

$\text{G} \rightarrow$ Required percentage of CH

The node P_{CH} measurement based on the node remaining energy and an average energy of all cluster members in each cluster.

The threshold measurement is given below.

$$\text{TH}(n) = \frac{\text{P}_{\text{CH}}}{1 - \text{P}_{\text{CH}} \times \left(r \bmod \frac{1}{\text{P}_{\text{CH}}} \right)} \tag{3}$$

$r \rightarrow$ Present round no

Data Transmission Phase

The source node S, wants to send the message to destination D via CHs. The node S computes the signature is given below.

$$\{\text{S}_{id}, \text{D}_{id}, \text{CH}_{id}\text{H}(\text{H}(m_i)), ts, \text{R}, i, \text{PK}_s\} \tag{4}$$

where,

$ts \rightarrow$ Time stamp

$i \rightarrow$ Message

$\text{H}(m_i) \rightarrow$ Produce the receipt

$\text{sig}(i) \rightarrow$ Signature of the message

$\text{PK}_s \rightarrow$ Private Key of signature

$\text{S}_{id}, \text{D}_{id}, \text{CH}_{id} \rightarrow$ Node ID of a Source, Destination, and CH

The source generates the signature provide the authenticity of the network. The destination node creates a one-way hash chain. Each CH verifies the hash element and send to the source. Finally, the source sends the

data to the destination via authenticated route in the WSN. This scheme provides authentication and integrity of the network also improve the lifetime and network performance.

4. PERFORMANCE EVALUATION

This section reports an execution estimation of the SCTRP protocol implemented by Network Simulator 2 (NS2). The system parameters used in our simulations mentioned in Table.

In this section, Figure 2, Figure 3, Figure 4, Figure 5 is a comparison between the proposed method Secure Clustering and trustworthy Routing Protocol in WSN (SCTRP) and existing method Secure and Trustable Routing (STR) in WSNs.

The performance of the proposed method SCTRP regarding data received rate against the simulation time is compared with the existing method STR as revealed in Figure 2. The SCTRP outperforms better data received when compared to the existing method due to the SCTRP transmit the data via trusted route in the network.

Table 1
Simulation parameters of SCTRP

Parameter	*Value*
Channel Type	Wireless Channel
Simulation Time	50 s
Number of nodes	50
MAC type	802.11
Traffic model	CBR
Simulation Area	1000×1000
Transmission range	250m
Network interface Type	WirelessPhy
Mobility Model	Random Way Point

1. Packet Delivery Rate

Packet Delivery Rate (PDR) is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node. The PDR is calculated by the equation 5.

$$\text{PDR} = \frac{\text{Total Packets Received}}{\text{Total Packets Send}} \tag{5}$$

The Figure 3 demonstrates that the data loss rate of STR and SCTRP. The SCTRP scheme used the signature verification method, therefore; unauthenticated node does not loss the packets. Thus the loss rate is very low when compared to the existing method STR.

2. Packet Loss Rate

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent. The formula used to calculate the PLR given in equation 6.

$$\text{PLR} = \frac{\text{Total Packets Dropped}}{\text{Total Packets Send}} \tag{6}$$

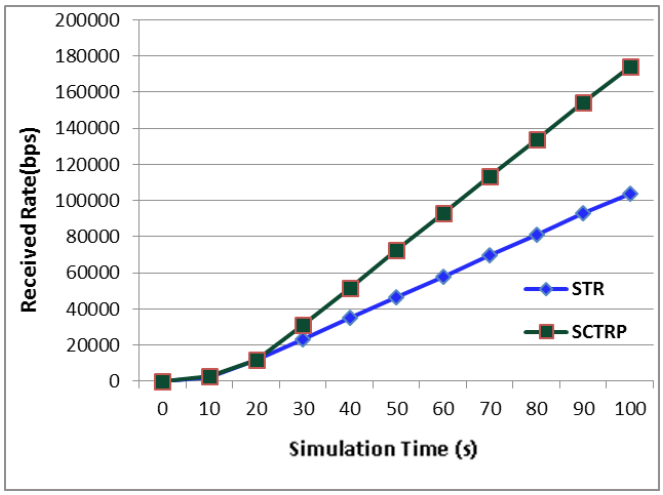

Figure 2: Packet Delivery Rate

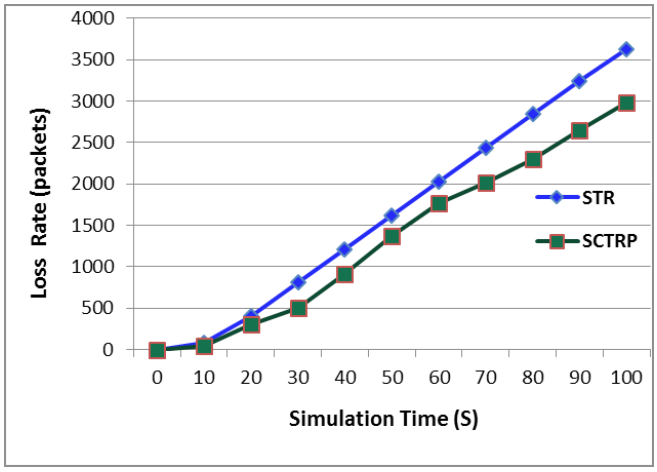

Figure 3: Packet Loss Rate

Figure 3 indicates the delay rate of proposed method SCTRP and existing method STR. The authenticated node transmits the data to the destination immediately. Therefore, the proposed scheme SCTRP delay time is very less when compared to the existing method STR.

3. Average Delay

The average delay is defined as the difference between the current packets received time and the previous packet received time. The delay in the network degrades the performance of the network. The average delay is measured by equation 7.

$$\text{Delay} = \frac{\sum_{0}^{n} \text{Pkt Send Time} - \text{Pkt Recvd Time}}{\text{Time}} \tag{7}$$

Figure 5 indicates the delay rate of proposed method SCTRP and existing method STR. The authenticated node transmits the data to the destination immediately. Therefore, the proposed scheme SCTRP delay time is very less when compared to the existing method STR.

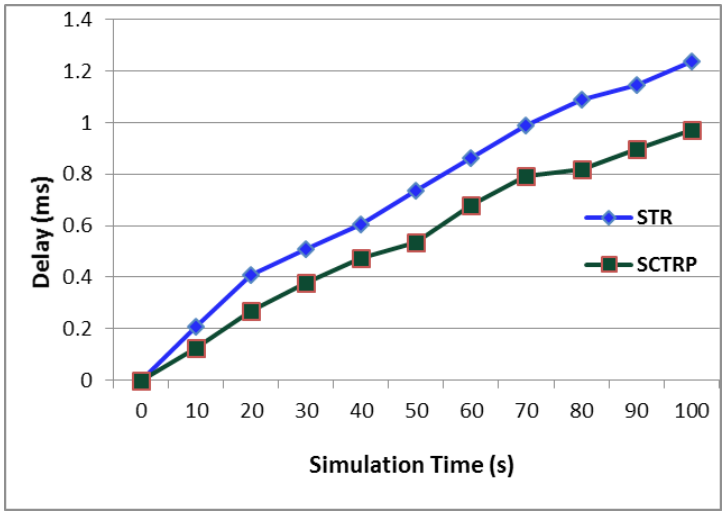

Figure 5: Average delay

4. Throughput

Throughput is the average of successful messages delivered to the destination. The average throughput is estimated using equation 8.

$$\text{Throughput} = \frac{\sum_0^n \text{Pkts Received}(n) \times \text{Pkt Size}}{1000} \tag{8}$$

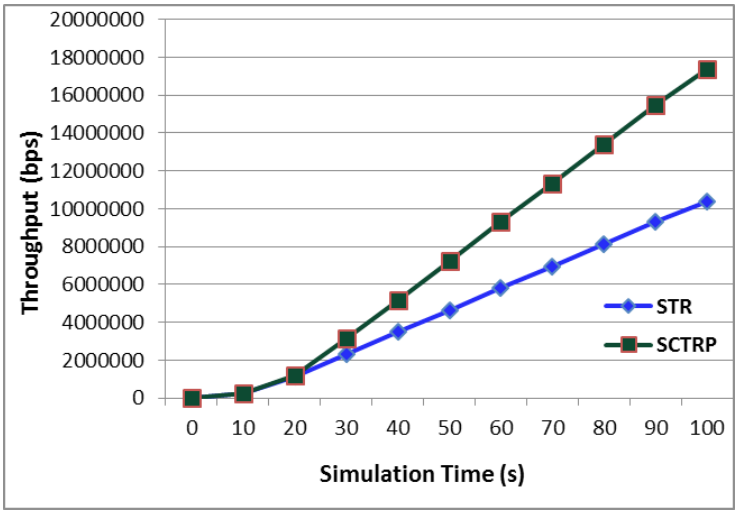

Figure 6: Throughput

Figure 6 reports performance analysis of proposed method SCTRP and existing method STR. Here the SCTRP increases the throughput when compared to the existing method STR because of the proposed method transmit the data through the reliable route in the network.

Residual Energy

The amount of energy remaining in a node at the current instance of time is called as residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operations.

Figure 7 represents the Residual energy of proposed method SCTRP and existing method STR. The SCTRP scheme used the power is restricted because of it transmits the data to the trusted node. The trust node calculation based on the node energy. Thus, increase the network lifetime.

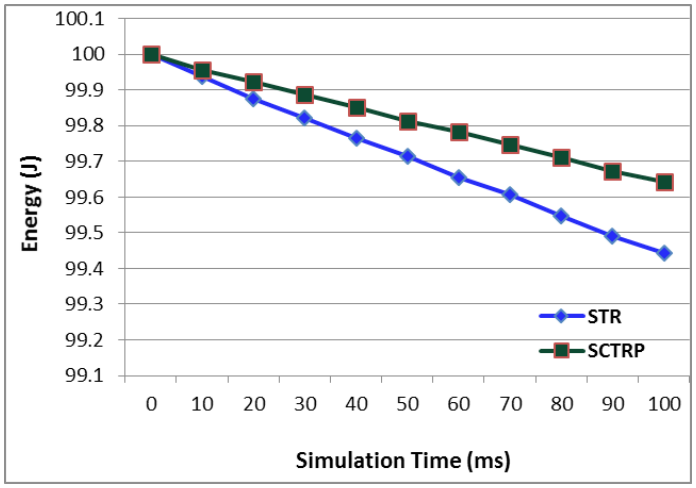

Figure 7: Residual Energy

5. CONCLUSION

A WSN is a combination of wireless communication and sensor nodes. The network must be energy efficient and stable and have a long life. In this scheme, the CH elected based on the Node Trust. This route improves the network reliability in WSNs. The one-way hash chain and signature verification provide authenticated way in the WSNs. The SCTRP improves the CH election process, and it achieved high security while data communication in the network. The simulation result proves that enhances the throughput and reduces the delay in the network. SCTRP increase both the network lifetime and performance in the network.

REFERENCES

[1] He, D., Chen, C., Chan, S. C., Bu, J., & Yang, L. T. (2013). Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks. *IEEE Transactions on Industrial Electronics,* Vol. 60, No. 11, pp. 5348-5354, 2013.

[2] V. C. Gungor and G. P. Hancke, "Industrial Wireless Sensor networks Challenges, design principles, and technical approaches," IEEE Trans. Ind. Electron., Vol. 56, No. 10, pp. 4258–4265, Oct. 2009.

[3] J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, "Distributed collaborative control for industrial automation with wireless sensor and actuator networks," IEEE Trans. Ind. Electron., Vol. 57, No. 12, pp. 4219–4230, Dec. 2010.

[4] X. Cao, J. Chen, Y. Xiao, and Y. Sun, "Building-environment control with wireless sensor and actuator networks: Centralized versus distributed," IEEE Trans. Ind. Electron., Vol. 57, No. 11, pp. 3596–3604, Nov. 2010.

[5] H. Song, V. Shin, and M. Jeon, "Mobile Node localization using fusion prediction-based interacting multiple models in cricket sensor network," IEEE Trans. Ind. Electron., Vol. 59, No. 11, pp. 4349–4359, Nov. 2010.

[6] Ramannavar, M. M., & Jagtap, M. M. "Authentication in wireless sensor networks using virtual certificate authorities," *International Journal of Emerging Technology and Advanced Engineering*, Vol. 2, No. 11, pp. 81-85, 2012.

[7] de Dieu, I. J., Wang, J., Asturias, D. J., Lee, S., & Lee, Y. K. "EDPPS: An Energy-efficient Data Privacy Protection Scheme for wireless sensor networks," IEEE *International Conference on* Computer *Sciences and Convergence Information Technology (ICCIT),* pp. 451-456, 2010.

[8] Shen, J., Tan, H., Moh, S., Chung, I., Liu, Q., & Sun, X. "Enhanced secure sensor association and key management in wireless body area networks," *Journal of Communications and Networks*, Vol. 17, No. 5, pp. 453-462, 2015.

[9] Yu, Z. "The scheme of public key infrastructure for improving wireless sensor networks security," In *2012 IEEE International Conference on Computer Science and Automation Engineering,* pp. 527-530, 2012.

[10] Liu, Y., Dong, M., Ota, K., & Liu, A. "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," IEEE Transactions on Information Forensics and Security, pp. 1556-6013, 2016.

[11] Banerjee, K., Sharma, H., & Chaurasia, B. K. "Secure communication for cluster-based wireless sensor network," IEEE *International Conference on Computational Intelligence and Communication Networks (CICN), 2014,* pp. 867-871, 2014.

[12] Tan, S., Li, X., & Dong, Q. "A Trust Management System for Securing Data Plane of Ad Hoc Networks," IEEE Transactions on Vehicular Technology, Vol. 65, No. 9, September 2016.