Data Communication through Reliable Sensor using Huffman Coding System

K Padmanaban*, A M Senthil Kumar, A K Velmurugan, and E S Madhan
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
Email: *padmanaban.k@kluniversity.in

Abstract. Wireless sensor networks (WSNs) contain a large number of sensor nodes that can forecast the atmosphere to transmit information in unfavourable situations. Though, restricted efficient also security problems in WSN. To solve these problems this paper Data Communication through Reliable Sensor using Huffman Coding system (DCRS) is introduced. In this strategy, the node with highest remaining energy will get division in the information transmit procedure. Security for each hop node is accessible through binary hop count (BHC) also verification is specified utilizing Huffman coding to avoid the malicious as well as other attacks in the network. The DCRS strategy is formalized through a network simulator.

Index Terms: Huffman Coding, network simulator, Wireless Sensor Network, route optimization, Binary hop count.

1. Introduction
Nowadays, WSN is motivating grassland of examining owing to their numerous applications as well as their incorporation toward extra difficult network systems. WSN is a type of self-governing network component of a huge amount of sensor nodes with inadequate calculation ability, bandwidth, energy also memory [1]. WSNs that can gather the entire varieties of data of supervised objects is mostly utilized in armed, ecological observing, intention chasing health care as well as other fields [2]. Sensor nodes produce real-time data as well as path data to the destination node through multi-hop transmitting. In a large WSN, the sensor observes the information is transmitting to the base station (BS) take longer time [3]. Thus, immediate information cannot reach in time. The BS node distributes a database, transmits control controls, and also examines data [4]. To notice some cases WSNs transmission delay happen to the major condition because sensor nodes that are regularly distributed in remote as well as neglected surroundings may be appropriated and its communication data also can be stopped [5].

Cryptography is a system to encode the usual information in this method which it should be decrypted to retrieve the real information. It can be prepared through the private key that offers the similar key for encryption as well as decryption also public key offers dissimilar keys for cryptography [6]. The authorized user is offered with the key toadmittance the realinformation also the illegal user can't entrance it. Thus security by encryptions might be difficult as the allocation of keys itself is a dispute in this self-configured networks [7].

In this approach, Data Communication through Reliable Sensor using Huffman Coding system is proposed. Here, the node with highest remaining energy will get division in the information transmit procedure. Security for each hop node is accessible through binary hop count (BHC) also verification is specified utilizing Huffman coding to avoid the malicious as well as other attacks in the network.
2. Related Works

An attack-resilient adversary node recognition approach is introduced which is capable to notice as well as manage with malevolent attacks. The effectiveness as well as efficiency of the Trust approach is corroborated via widespread experimentations [8]. Heterogeneous remote anonymous verification approach based on L-OOCLS for remote WBAN users to take pleasure in several healthcare services on IoT applications. In this approach, anybody can falsify certificate less verification on any information for any individuality from only publicly recognized information [9].

Lightweight, confidential, as well as denial-of-service-resistant to make sure the information items disperse not distorted or fiddled. Depend on several one-way hash chains, approach offers immediate verification as well as can accept node cooperation [10]. An executes in-depth security to illustrate that approach is demonstrably safe [11].

Provisioning of Efficient Authentication technique is using Elliptical Curve Cryptography for improving node authentication. This security technique is checking every intermediate hop before data communication in the network [12]. Delay-Efficient Data Scheduling (DEAS) approach creates the collision-free schedule, which diminishes the collection latency. This approach diminishes the sleep delay among nodes, also creating pipelined schedules. However, this approach can’t provide the node reliability [14]. Optimal Capacity-Delay Trade-off strategy significantly concentrates on the collision of the connection of node movement on the capability-delay trade-off in the networks [13]. This method inquired the character of related movement also figured out the primary association among the capability, delay as well as the connected scheme factors that afterwards offer immense assist to derive the capacity-delay trade-off [15].

3. Proposed Method

In this approach, Huffman Code (HC) is introduced for improving sensor reliability in WSN. It contains two steps such as Initially, source discovers the nodes with optimal route between hop then compute the binary hop count at every hop through preserves the routing table to offer the security at every hop. In addition, it provides reliable communication among source to destination using Huffman Coding system.

To create the transaction among the in-between nodes secure BHC security technique is used. During data communication the source checks the BHC value if it equates afderspecific node can admissionthe information from the prior node. This complete procedure should happen inside the particular time-to-live.

At initial hop the security code is 01 and next hop security code is 10. Likewise, for hop k, the half man code is corresponding to the binary value of k constituted as

\[ BCH = HC(k) \text{(binary equal)} \]

Here, \( HC \) represents the hop count at \( k \)th hop and \( BCH_{k=1}^{k} \) at \( k \)th hop as well as \( k = \{1, 2...\} \). A source transmits the packet to destination through neighboring nodes established on minimum distance, highest remaining energy, also BCHsecurity.

One time the optimal route is received from source to destination, a Huffman code since destination to the source is transmitting. If this code equalizes next the data is transmit from source to destination. Computing the Huffman procedure is given below.

\[ HC = C_{h}C_{h1}...C_{h} \quad (1) \]

Where, \( h \) denotes the length of the hop count and \( C_{h} \) denotes the Huffman code received at \( h \). Coding is used to develop the end-to-end authentication code.

The procedures of DCRS strategy is given below.

Step 1: Compute the minimum distance, remaining energy and BCH of neighboring nodes

Step 2: Choose the node with greater energy.

Step 3: if two nodes are exist with equivalent greater remaining energy next choose the one node among the two, having a smallest amount of distance for discovering efficient route.

Step 4: for reliable function BCH at every hop is enclosed. If it equals node inside the suitable TTL is told to be energetic otherwise unreliable sensor node.

Step 5: An end to end reliable to preserve the reliability of information through computing the HC of the remaining energy values.

Step 6: This procedure is continued till the destination node is accomplished.

Simulation Analysis:
4. Simulation Analysis
The DEAF through itself can be utilized as a proficient routing metric because it efficiently catches not only the delay of the queue; however, the retransmission delays. We employ NS2.35 simulation results for a WSN. Here, the 50 sensor nodes are arbitrarily distributed in a 600x500m² topology area with required modification to preserve the property. We as well run 4 flows over the arbitrary topology. The node communication range is 200m, the size of the packet is 512 bytes, and we utilized constant-bit-rate flow.

Figure 1. Packet Received Rate

Figure 1 depicts the Packet Received Rate of DEAS and DCRS Scheme. It explains that the proposed scheme DCRS has the highest received rate than the DEAS since DCRS form the route based on node reliability.

Figure 2. Packet Loss Rate

Figure 2 demonstrates the Packet loss of DEAS and DCRS scheme. The DCRS scheme diminishes the loss of data packet since it chooses to select the forwarder node by hop reliability in the network. But, DEAS utilizes more packet losses.
Figure 3 explains the delay rate explicitly around recognized with the time period essential to distribute the whole data. This figure proves the proposed scheme DCRS have minimum delay time than the existing scheme DEAS.

Figure 4 depicts the throughput of DEAS and DCRS. It explains which the introduced approach DEAF has the highest throughput than the DEAS since DCRS form the route based on Huffman coding system.

5. Conclusion
This paper presents Data Communication through Reliable Sensor using Huffman Coding system. In this strategy, the nodes with highest remaining energy will getdivision in the information transmit procedure. Security foreachhop node is accessible through binary hop countalso verification is specified utilizing Huffman coding to avoid the malicious as well as other attacks in the network. Simulation results illustrates that DCRS method provide better throughput and lesser delay in the WSN.

References:
1. Jan, Z., Azeem, N., &Zahoor, F. (2015, November). Digital watermarking using combination of Ranklets and wavelets. In 2015 First International Conference on Anti-Cybercrime (ICACC) (pp. 1-5). IEEE.

2. Rambabu, K., &Venkatram, N. (2018). Contemporary affirmation of security and intrusion handling strategies of internet of things in recent literature. Journal of Theoretical and Applied Information Technology, 96(9), 2729-2744.

3. Shaik, R., &Ahmad, S. S. (2018). Security attacks and challenges of wireless sensor network's a review. International Journal of Engineering and Technology(UAE), 7(2.32 Special Issue 32), 136-138.

4. Sri Lakshmi, M., & Srikanth, V. (2018). A study on light weight cryptography algorithms for data security in IOT. International Journal of Engineering and Technology(UAE), 7, 887-890.

5. Suma, P., & Hussain, M. A. (2018). Secure and effective random paths selection (SERPS) algorithm for security in MANETs. International Journal of Engineering and Technology(UAE), 7(2), 134-138.

6. Sabri, N. A. M., Basari, ASH., Hussin, B., Samah K.A.F., 2015, Dijkstra-Ant Colony Optimization Algorithm For Shortest And Safest Evacuation In High Rise Building, 79:3 (2017) 69–77

7. Arora, S. K., &Ayushree. (2016). Detection and performance analysis of wormhole attack in MANET using DELPHI technique. International Journal of Security and its Applications, 10(10), 321-330.

8. Kumar, MJ&Baskaran, R (2017), Analyzing a Personalized Network System through NetFlow’, Institute of Integrative Omics and Applied Biotechnology (IIOAB), 7(7), pp. 1-7.

9. Shim, K. A. (2019). Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things. IEEE Internet of Things Journal, 6(5), 9211-9212.

10. Kumar, MJ&Baskaran, R 2015, ‘Performance Analysis and Comparison of Congestion Control in Wired and Wireless Environment’, International Journal of Control Theory and Applications, vol. 8, no.5, pp. 1743-1757.

11. Hassan, J. (2018, April). Future of Applications in Mobile wireless Sensor Networks. In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

12. Lingeshwari S (2014), Provisioning of Efficient Authentication technique for implementing in large Scale Networks, International Journal of MC Square Scientific Research, 6(1), 34-42.

13. Santhakumar, R (2017) Resource Allocation in Wireless Networks By Channel Estimation And Relay Assignment Using Data-Aided Techniques. International Journal of MC Square Scientific Research, 9(3), 40-47.

14. Appala Raju, V., Sri Harsha, V., Bhanudeepthi, N., & Prasanth, N. (2018). Zonal stable election protocol for heterogeneous wireless sensor networks. International Journal of Engineering and Technology(UAE), 7, 725-728.

15. De Paulo, M. A., Nascimento, M. C., & Rosset, V. (2016, October). Improving the Connectivity of Community Detection-based Hierarchical Routing Protocols in Large-scale WSNs. In KES (pp. 521-530).