A Secure Ant Colony based Trust Computation Model in Wireless Sensor Networks

Y.AdlineJancy¹, B.Gomathy², A.BenuelSathishRaj³

¹Sri Ramakrishna Engineering College, Tamilnadu, India.
²KPR Institute of Engineering and Technology, TamilNadu, India.
³ Sri Venkateswara College of Computer Application and Management, Tamil Nadu, India. e-mail:adlinjan@gmail.com

Abstract: We have always observed that the wirelessly connected sensors have difficulties in maintaining the charge and transmitting data safely from the sender to the receiver end. Due to this the longevity of the nodes doesn’t last longer and the efficiency is found to be very less. The chances of data being lost during the transmission are also very high. This paper deals with the methods employed to cut short the energy used by the nodes, transmit data safely from sender to receiver and also increase the efficiency. This paper associates algorithms like LEACH, ACO, ECC which in integration performs operations that selects the cluster head, reduces energy consumption. In the proposed technique transmission of data happens from the cluster member to cluster head and from the cluster head to the base station. The results show that the LEACH-ACO algorithm significantly reduces the average energy consumption. The threshold value of each and every task has to be defined manually keeping in mind the risk that the task is able to handle. The threshold value differs with different systems. By cross checking the trust value that was obtained by computing and the threshold trust value, it is straightforward to conclude if the particular node is a safe node or an unsafe node. The proposed protocol reduces overall energy consumption by reducing the number of dead nodes, and providing an optimal path with increased packets delivery ratio.

1. INTRODUCTION

Wireless sensor network finds its applications in almost all fields like military, health air pollution monitoring, environmental sensing, water quality, home and commercial applications etc. They are deployed with sensor nodes required for each system in account of the task the system is going to perform. For example, in case of environmental sensing, the count of nodes required is more than that required for home purpose. The sensor nodes are generally used to keep track of conditions like temperature, sound and pressure. The wireless sensor networks consists of nodes which on integration senses and transmit the needful data to the end user i.e., the receiver, which analyses the data received. If the data received is found not to be the expected data or no data is received then the receiver acts accordingly. The Wireless Sensor Architecture generally consists of a sender, receiver, battery and antennae.

Different types of WSN topologies are available which can be used for different types of applications depending on what type the system requires. These topologies vary from being simple to most complicated designs. The size and the price of sensor nodes vary proportionally to the complexity of the sensor nodes. It is found that the complex topologies consume more energy when compared to simple design. There are also possibilities that the packets sent from the sender to receiver end can either be lost or manipulated by some other sources. To avoid this, it must be taken into account that the data being transmitted is provided with security aspects. In this paper, the aspects which involve providing security to the data transmitted, less energy consumption by the sensor nodes and also identifying the shortest route to reach the destination are discussed.
Background Overview

A. Existing System
   The existing system involves the following practice,
   - It is the traditional method in which the agent ants travel to and fro from the sensor node to
     sink node.
   - It produces a backward ant that takes the same path as the forward ant in the opposite direction.

B. Drawbacks of Existing System
   The above mentioned method is time consuming, inefficient and consumes more power. In the
   case of sensor-driven ant routing, the network suffers from misleading due to the obstacle error in
   sensing thenode.

C. Overview of the proposed system
   Design of the efficient “A secure ant colony based trust computation model in wireless
   sensor networks” is mainly based on combining three algorithms namely LEACH, ACO and ECC to
   provide low energy consumption, to know the shortest route and to provide a secure transmission of
data respectively.

2. RELATED WORK
   In [2], based on the computational complexity, energy efficiency, network architecture and
   route establishment, the routing protocols are classified. The paper re-simulates different protocols
   using a Matlab-based simulator: Routing Modeling Application Simulation Environment (RMASE)
   and provides simulation results for standard simulation and performance metrics.
   In [3], the potential increase in performance obtained by balancing traffic throughout the WSN is
   investigated. Sending the traffic created by each sensor node through multiple paths, rather than a
   single path, is shown to allow significant energy conservation. The simulation complements are cent
   theoretical model for load-balanced systems to quantitatively analyse the benefits of the proposed
   load-balancing technique. In particular, it is possible to derive the set of paths to be used by each
   sensor node and the corresponding weights (i.e. the proportion of utilisation) that optimise the lifetime
   of thenetwork.
   In [4], a proposal uses an ant-colony-based scheduling algorithm to solve the EEC problem. (ACB-SA).
   This algorithm is a simplified version of the standard ant colony optimization algorithm,
   adapted to overcome the EEC problem. In the proposed algorithm, a heterogeneous sensor collection
   that reflects a more realistic approach to solving the EEC problem is added to the probability
   sensors detection model.
   In [5], the Bio-Inspired Routing Mechanism is a technique proposed. Network congestion and
   rapid energy consumption of individual nodes can be avoided. Then it will extend the entire network's
   lifecycle. This paper describes the implementation of WSN and compares its performance with the
   ant-algorithm-based AODV routing protocol in terms of packet delivery ratio, throughput and energy level.
   In [6], a new event data collection technique called reliability and multipath encounter
   routing(RMER) is suggested to meet the criteria of reliability and energy efficiency. Energy
   consumption can be significantly decreased, thereby allowing the life of the network to be further
   increased.

3. PROPOSED SYSTEM
   A. By using swarm intelligence, an approach is applied to select the cluster head. This method is
   based on a LEACH clustering algorithm.
   B. The LEACH algorithm selects the efficient cluster using an advanced ant colony optimization
   technique with residual energy as a parameter.
C. The proposed technique operates in three phases: The data stored in the cluster member is transmitted directly to the cluster heads, the heads of the cluster forward the data to the leader, and the leader sends the data to the base station.

D. LEACH-ACO algorithm effectively reduces the average energy consumption.

E. To make a decision on security with the computed trust value, risk level affordable for each ongoing task need to be estimated.

F. It is easy to see whether the trustee node meets the trust requirement or node by comparing the computed trust value and the threshold trust value.

4. METHODOLOGY

The main objective of the paper is to ensure that, in a given Wireless Sensor Network, communication between nodes take place in a much secured manner with less end to end transmission delay and in a trustable manner. In case there is a node which is found to be malicious in the given network, data should neither be received nor be sent from the node and the node is neglected considering it to be malicious i.e., unsuitable to send or receive data. In order to perform the above said objective, the principles used are the LEACH (Low Energy Adaptive Clustering Hierarchy) algorithm, ACO (Ant Colony Optimization) algorithm and the ECC (Elliptic Curve Cryptography) algorithm.

LEACH algorithm reduces the energy consumption in the wireless sensor network thus making it efficient. A network consists of several nodes and each node in a wireless sensor network is a cluster members. In case all these cluster members are ON for every specific point of time, the energy utilized by the cluster members is considerably high. To solve this, LEACH is applied where a cluster head is chosen among the several cluster members. The cluster head commands the cluster members, to send the data at some specific point of time, until then the cluster members are OFF. This reduces energy consumption. The head of the cluster now collects data from different nodes and transmits it to the base station or sink. The head commands all its members. Once a cluster member is chosen as head, the same cluster member cannot become head for the second time until all the members have become head for at least once. For example, let us consider that there are 50 nodes in a wireless sensor network. The energy consumed by the nodes is very high if all the nodes are made to transmit data directly to the base station.

Ant Colony Optimization is a best method to find the shortest route possible from the node to reach the base station. This is done similar to the way ants find its path by leaving pheromones in its way. Once a route is found by an agent to the destination, pheromones are dropped on its track. They are likely to follow with a certain probability when other ants come across the pheromones. If they do, when they return, they then populate the route with their own markers. As the ants travel often, shorter
Paths are more likely to be stronger. The path is no longer populated with pheromones and eventually decays once the food source is exhausted. Thus the shortest route is identified with dense pheromone level. The other main feature of the Ant Colony Optimization is the trust computation of a node. Any node is initially assigned a threshold value of 1. The calculation of each and every node's trust value is completed. If the node is deemed to be trustable, a value of 0.2 is applied to the node's threshold value. If the node is found to be not trustable i.e., a value of 0.2 is subtracted from the threshold value. This approach avoids the data being sent to malicious nodes and security is ensured.

ECC (Elliptical Curve Cryptography) guarantees that the sender's transmitted data is encrypted and the receiver's data is decrypted, so that the data sent is highly secured, and eliminates the chances of an attack. ECC produces keys using the properties of the elliptical curve equation with the very large prime numbers product.

ECC algorithm is used when compared to all other algorithms because it establishes an equivalent security with relatively lower computing power and reduced resource is used from the battery. Another point on the curve is generated by multiplying a point on the curve by a number, but it is very hard to find what number was used, even though you know the original point and the result. ECC algorithm uses smaller keys to get the same levels of security. A stronger trade-off between high security and quick and fast keys seems to be provided by the ECC.

5. SYSTEM MODEL

The following encloses the brief explanation of the working principle of various major blocks in the system. The Figure 2 shows that initially, there are several cluster members present in a wireless sensor network (WSN). A cluster head is chosen to avoid congestion of data being sent towards the base station and to reduce the energy consumed by the system. For example, instead of 50 cluster members sending data to the base station simultaneously, a cluster head is chosen in a random stochasticalgorithm method. So now data is sent from these cluster members to the cluster head and then sends it to the base station. This can reduce congestion and energy consumption. ECC (Elliptical Curve Cryptography) is applied over the leach to ensure the privacy of the data being sent. Apart from ensuring privacy, the trust computation algorithm and shortest path finding algorithm is employed over the leach. Ant Colony Optimization algorithm is used as the shortest path finding algorithm.

At the base station, it is ensured that no collision of data being received with the help of Collision Attack Detection. Once the data is received and performance analysis is done. Better efficiency and security are obtained in the result.

![Figure 2. Block Diagram of Trust Computation Model](image-url)
6. TRUST COMPUTATION BASED ATTACKER DETECTION MODEL

To make a security decision in the system, some parameters need to be considered. The value of trust, as considered by the parameter (α). The value of trust and the affordable risk level for each node of the on-going task needs to be calculated. In other words, a threshold of trust value needs to be defined for each task. By comparing the calculated trust value and the predefined threshold trust value, it is easy to check whether the route meets the trust requirement or not. For example, if the computed trust value is greater than or equal to the threshold value the route is trustable; the route is malicious if the calculated trust value is smaller than or equal to the threshold value.

\[
T^{ij} = \frac{\alpha_i}{\alpha + \beta_j}
\]

T - Trust value
i and j - Nodes
α - Positive value
β - Negative value

Attack prevention model
ECC algorithm is one of the best algorithms for the prevention of attack. The three steps in the model includes,
- Key generation
- Encryption
- Decryption

Key generation
Let us choose a number that does not exceed ‘n’. The public key can be generated with the following expression.

Q = dP

D is a random number selected within the range of (1 to n-1).
P - point on the elliptical curve.
Q - public key.
d - private key.

Encryption
Let us consider the message send to be ‘m’ and represent this message on the elliptic curve. This has detailed implementation information. Consider ‘m’ has the point ‘M’ on the elliptic curve ‘E’. Select ‘k’ randomly from[1 to(n-1)].

E is the Elliptic curve.

Two cipher texts will be generated let it be C1 and C2.

C1 = kP
C2 = M + kQ

C1 and C2 will be sent.
Decryption

The original message ‘m’ get backed from the received cipher texts ‘C₁’ and ‘C₂’.

\[ M = C₂ – dC₁ \]

M is the original message send.

M’ can be represented as ‘C₂–dC₁’

Substituting values of C₁ and C₂

\[ C₂–dC₁ = (M+kQ)–dkP \]

Substituting value of Q

\[ C₂–dC₁ = M + kdP – dkP = M \text{(Original Message)} \]

7. RESULT

The results of the simulation are obtained successfully. The results with attacker node and without the attacker node are shown below.

![Figure3. Result without attacker nodes](image)

The figure shows the results of the wireless sensor network without an attacker node in the system. Here the middle sensor node acts as the cluster head from which commands are send to the cluster members. The node in green is the base station node, while the cluster members and the cluster head are in different colors. Since no attacker node exists on this network, information is collected from all cluster nodes without excluding any nodes on the network.
The figure 4 clearly shows that the malicious nodes are found and represented in black color and the respective nodes are being marked as At (Attacker) and the cluster members are provided with their ID’s. Communication is made only to the nodes that are not malicious whereas the malicious nodes are left alone. There is a grid to know the positions of the sensor nodes, which can also be switched ON or OFF.

The Results from the simulation were obtained. The network parameters were analyzed through network simulator and plotted with gnu plot. The analysis of these parameters such as packet delivery ratio, throughput ratio and average delay from end to end shows that the performance of the proposed work is as expected.

8. CONCLUSION AND FUTURE WORK

An approach for transmitting data packets between each sensor node and the base station with higher efficiency, lower energy consumption, decreased average end-to-end delay, increased packet delivery ratio and higher through put ratio has been proposed. This approach has been developed by integrating the three main principles namely, Low Energy Adaptive Clustering Hierarchy, Modified Ant Colony Optimization with trust computation for each node and Elliptic Curve Cryptography. The trust computation based attacker detection model that has been included to detect the attack happening between two sensor nodes with the three main principles. That is, to check the trust factor of a route between two nodes. With these four principles and computation techniques, the objective of the proposed work has been made possible. The Results from the simulation were obtained. The network parameters were analyzed through network simulator and plotted with gnu plot. The analysis of these parameters shows that the network performance of the proposed work is as expected and marked the successful completion of the paper and thus producing an opportunity for the routing of packets in a secure and trustable way. The future scope of the proposed work can be to implement the work as a Real-Time project and to apply this wireless sensor network application in mission critical areas. Future work can aim to eliminate the problem of sufficient energy remaining to collect the data packets from the cluster members, cluster head and to forward the data packets to the base station successfully.

REFERENCES

[1] Sohail Jabber, Rabia Iram, Abid Ali Minhas, Imran Shafi, Shehzad Khalid, and Muqueet Ahamed “Intelligent Optimization of Wireless Sensor Networks through Bio-inspired Computing: Survey and Future Directions”, International Journal of Distributed Sensor Networks, 2013.
[2] Adamu Murtala Zungeru, Li-Minn Ang and Kah Phooi Seng, “Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison”, Journal of Network and Computer Applications, 2012.

[3] F. Boudabdallah, N. Boudabdallah, R. Boutaba, “On balancing Energy consumption in Wireless Sensor Networks”, IEEE Transactions on Vehicular Technology, vol. 58, Issue 6, 2009.

[4] J.W. Lee and J.J. Lee, "Ant-colony-based scheduling algorithm for energy-efficient coverage of WSN", IEEE Sensors Journal, vol. 12, no. 10, October 2012.

[5] K. Syed Ali Fathima and Mr. K. Sindhanaiselvan, “Ant Colony Optimization Based Routing in Wireless Sensor Networks”, International Journal of Advanced Networking and Applications, 2013.

[6] M. Dong, K. Ota, and A. Liu, “RMER: Reliable and energy-efficient data collection for large-scale wireless sensor networks”, IEEE Internet of Things Journal, vol. 3, August 2016.

[7] Prakash, B. and Gowri Durga, “An Efficient Energy Consuming Protocol For Wireless Sensor Networks”, Indian Journal of Applied Research, 2011.

[8] P. Visu, T. Suriya Praba, N. Sivakumar, R. Srinivasan & T. Sethukarasi “Bio-inspired Dual Cluster Heads Optimized Routing Algorithm for Wireless Sensor Networks” Springer Journal of Ambient Intelligence and Humanized Computing, January 2020.

[9] Zhong Luo, Liuzheng Lu, Jianqun Xie, and Jinrong He, "An ant colony optimization-based trustworthy routing algorithm for wireless sensor networks", 2015 4th International Conference on Computer Science and Network Technology, Harbin, 2015.

[10] Harsimran Kaur 1 and Mani Sahore 2, "A Survey on Wireless Sensor Network Security Using AI Methods", International Journal of Latest Trends in Engineering and Technology, Vol. (7) Issue (4), pp. 234-239, 2018.

[11] Heena Rathore, Venkataramana Badarla, Sushmita Jha, Anupam Gupta, “Novel Approach for Security in Wireless Sensor Network using Bio-Inspirations” Sixth International conference on Communication Systems and Networks, 2014

[12] Pooja Singh, R.K. Chauhan, "A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN", International Journal of Electrical and Computer Engineering (IJEC E), Vol. 7, No. 4, August 2017.

[13] Min Tian, Jibin Bai, "Resource Allocation Based on Chaotic Ant Colony Algorithm in Self-organizing Wireless Sensor Network", Journal of Physics: Conference Series, 2020.

[14] Anusha Sowbarnika V., Dr. Balasubramani M., Dr. Kavitha K., ‘Enhancing the Security and Energy Efficiency by Integrating Grid Based Adversarial Clustering and Ant Colony Optimization (ACO) in Wireless Sensor Networks’, International Journal of Advanced Science and Technology, Vol. 29, No. 3, 2020.

[15] Ziwen Sun, Min Wei, Zhiwei Zhang, Gang Qu ‘Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks’", Journal of Applied Soft Computing, Vol. 77, April 2019.