European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 01, 2020

Energy Efficient and Secure Design for Wireless Sensor Networks Using Network Simulator

G Ahmed Zeeshan[1], Dr. R Sundaraguru[2], Dr.P.Vijayakarthick[3]

[1] Department of Electronics and Communication Engineering, Global Institute of Engineering and Technology, Hyderabad
ahmedzeeshan_eng87@yahoo.com.
[2]Department of Electronics and Communication Engineering, Sir M Visvesvaraya Institute of Technology, Bengaluru
sugursg@gmail.com
[3]Professor and Head, Department of Information Science and Engineering, Sir M Visvesvaraya Institute of Technology, Bangalore
vijaykarthik_is@sirmvit.edu

Abstract

The scope of Wireless Sensor Networks (WSN) is fields tremendously improved in science, engineering, military, and health. Wireless Sensor Networks (WSN) equips the portable clients having large bandwidths through dynamic range with accessing different methods along with wireless various architecture. In This Proposed article is focus on optimize energy system with high security. Security became very challenging task now days to provide WSN systems. We proposed energy and security of WSN implement using cluster based grid adversarial method. The sensor nodes have a huge range of data to destination. Then the routing method is employed to analyze the shortest course of travel from source to destination. The proposed system will provide energy efficiency and security to the network with comparison with existing routing algorithm. The proposed method is using Network Simulator 2 for design.

Keywords: *Energy-Efficiency, Security, Wireless Sensor Networks*

1. INTRODUCTION

The bits are located on the programming boards which are associated with the computer and hence the application of WSN and the operating system can be cleansed into the bit memory. They can be programmed with the identification number. They can also be programmed without a physical linking to the computer which is termed as Over the Air (OTA) programming.The method is incredibly challenging in preserving the level of energy for a longer phase. They are stocked with restricted computing and radio communication features. This is mainly due to constrained energy level and size of the sensor nodes. These constraints make it difficult to utilize the standard security features in WSNs. The restrictions of sensor nodes must be known to augment the traditional security methods in WSN. The method is impressive with less infrastructure networking resources even though the unit is filled low cost sensing and storage abilities. The assimilation is provided in the diverse atmosphere for both sensing and administering the information. The critical data is transmitted to sink node in WSN by a multi hop ad hoc network. The sink node always acts as a data accumulator to the base station and doorway to the static infrastructure According to the existing state of affairs for security algorithm, Asymmetric cryptography is used. Asymmetric algorithm is more robust and secure to attack when compared with symmetric algorithm. But at the same time Cryptographic causes lot of CPU and communication overhead. This paper presented an Enhanced Energy Aware and Secure AODV (EEES-AODV) Routing Protocol for an efficient data communication network. The proposed offers the security algorithm called as grid based adversarial clustering. The intersecting segments, normal regions among the clusters are discovered by this algorithm. The intersection and outlier segments are not categorized by this method. The shape and size of the protective walls are identified by game theory. In the protective walls, there will be normal as well as attack

objects. The error occurs when the normal regions gets mixed with the attacking objects. Hence the adversarial clustering method gives correlation to security.

2. LITERATURE SURVEY

To advance the security, the information is extended at considerable cost. When the level of security is high the consumption of energy is also high because of the cryptographic primitives. The level of security can be classified into different levels based on the cost of the energy [1]. Bidoki et al (2018) proposed the approach called as "Energy Aware Sleep Scheduling Technique" [7]. The information is sent from the sensor node to aggregator node through wireless sensor networks. The difficulty is discovering the route of the sensed node and the data that is conveyed to the sink node would be higher and thus the consumption of energy becomes low. The sleep scheduling mechanism is utilized in MAC layer to remove the excessive communication among the sensor and aggregator. Ben Arbi et al (2017) introduced a new technique called "Self-Exiting Threshold Auto-regressive Technique". This method helps to minimize the amount od packets that are sent from sensor to sink node and the energy employed can be minimized [8]. The data minimization is also evolved to emphasize this trouble by forecasting at the sink and the source node for attaining the calculated value. The broadcasting value is required only when the sensed parameter value is different from the projected value. The projected value is dependent on the sensed value. In particular, the high-end entropy systems such as electric engine are challenging to construct and estimate the values in the system. Panda M (2015) implemented a "Data Security in Wireless Sensor Networks vis AES algorithm". This method is to offer data confidentiality. It is based on AES symmetric key encryption [9]. The method uses the same key for encipherment and decipherment. The algorithm is executed, and it is comprised of 10 rounds which help to provide more security.
Sekhar et al (2012) initiated a method called "Security on wireless sensor networks with public key techniques". The approach involves the feature of public key cryptography". The user communicates with the base station by encryption algorithm [10]. The user communication with the sensor nodes can be performed only with the help of private key. Since the method uses asymmetric encryption, it offers security to the network.

3. EXISTING SYSTEM

The energy consumption is a major problem in wireless sensor networks. The sensor nodes have a huge range of data to destination. Then the routing method is employed to analyze the shortest course of travel from source to destination. But the protocol must ensure accuracy, solidity, easiness, and optimality. The method is Dijkstra's algorithm [2]. The focus of this approach is to obtain the shortest path to reach its destination which minimizes the energy consumption in the network. The routing algorithm is Dijkstra's algorithm. The method tries to find the shortest path from source to destination. The source node is termed as's' and destination is 'd'. This is given on the directed graph said to be G. Here,

|G| →total nodes in the graph

D (d) →entire weight from source to destination

Cost (u, d) →routing cost from u to d

N →vertices in G

But the implementation of this algorithm seems to be complex. Because the protocol needs global state data. Each node's cost and protocol are visible to others which end in extending the routing table. The small change will cause a major error in the routing table. Hence the consumption of energy is more, and energy efficiency is reduced. The proposed system will provide energy efficiency and security to the network.

4. PROPOSED SYSTEM

GRID BASED ADVERSARIAL CLUSTERING

The security can be upgraded by clustering method called as "grid based adversarial clustering". The algorithm employs a Gaussian kernel classifier to find the probability values for unlabeled instances. There are two types of instances: a) labeled instance and b) unlabeled instances. But this method holds only for unlabeled instances [5]. The nodes will be assigned with pre-specified weights. Again, the density of the data points is re-computed using the pre-specified weights. In the first step, the method will group this data points into 4 categories like normal sub clusters, abnormal sub clusters, unlabeled sub clusters and unlabeled outliers. Here, the weight's choice may influence the normal and abnormal segments. Here, the labeled instances are not utilized here. The nodes are simply arranged into unlabeled clusters and outliers. In the third step, the method will connect the unlabeled, abnormal, and normal clusters obtained from the second step which has only the nodes that are unlabeled. From this point, the normal as well as abnormal segments that belong to one cluster are identified.
In the initialization phase, the weight w is chosen for re-assigning the weight to the unlabeled nodes. The value of w may have more influence on the normal segments. The algorithm is as follows:
Step 1: Cell Creation – For each point Pi the range is split into minimum and maximum. It is divided into did sections. I = 1, r. The 'r' is q dimensional cell with its neighborhood radius 1 as its neighbor nodes.
Step 2: Threshold: The distance threshold is calculated, and the density is calculated as:

$$RT = \frac{mean(d(c))}{q \times coef RT}.$$

The distance of 'c' neighbor nodes is calculated here. The distance threshold is represented as RT. The density threshold is computes as follows:

$$DT = \frac{mean(n(c))}{\ln(N)} \times coef DT,$$

Step 3: Weight Calculation: The data points are labeled here. The normal clusters are termed as 0's and abnormal are given as 1's. Then perform the function called as "merge".

Step 4: Merge 1: First step is to create the labeled instances of normal and abnormal clusters. The nodes which have been re-weighted and if the density is greater than density threshold then that node is taken as centric. The lesser densities are merged and if the distance of the point is less than RT then the remaining points are merged into another big cluster. The unmerged points are referred to as unlabeled instance.

Step 5: Merge 2: Cluster the rest of the unlabeled data points. Here the normal as well as abnormal clusters are removed. For the rest of the data points, source density is utilized. Then the unlabeled instances are merged.

Step 6; Merge 3: Consider the parameters RT, DT, and k of the source density. The unlabeled clusters and outliers are determined.

Step 7: Match: The above said unlabeled clusters are associated with the normal and abnormal clusters. Here, the normal and abnormal segments can be identified. The points in the normal segments are not labeled. If the segments are not labeled, then they are said to be distant.

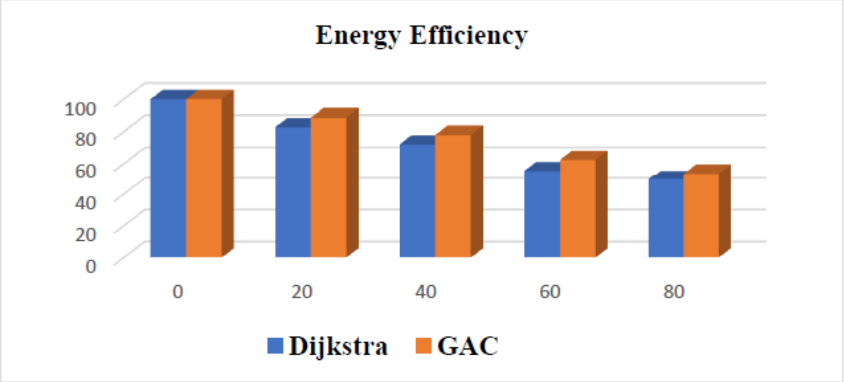
Step 8: Defensive walls construction: This wall is drawn to ensure protection from attacks. It is drawn in the normal regions to stop the abnormal regions. The strategy is followed to safeguard the core segments of the normal clusters. The merge sections mentioned above are called as defensive walls. The wall construction plays a major role in this clustering part. If the defensive wall is small, the normal segments may be blocked along with the attack objects. Hence the large defensive wall must be constructed avoid choosing the attacking objects with the normal segments

5. RESULTS AND DISCUSSION

The work contains two sections. The first section deals with the security and the second part deals with the energy efficiency. The security is enhanced by Grid based Adversarial Clustering (GAC). The projected work is the combination of Grid based Adversarial Clustering.

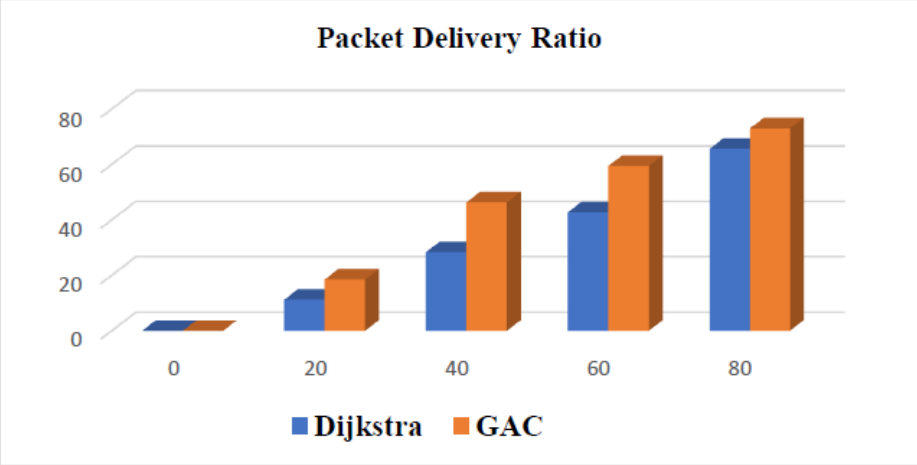
Simulation Time (ms)	Energy Efficiency (nJ)	
	Dijkstra	GAC
0	100	100
20	82.76	88.61
40	72.10	77.98
60	55.43	62.43
80	49.67	53.60

The unlabeled instances are taken, and they are merged into clusters for identifying the threat objects. Once the attacking objects are discovered, the pheromone updating by ants makes the process easier to attain the optimal path from source and destination. This helps to minimize the energy conservation and maximize the energy efficiency



Simulation Time (ms)	Packet Delivery Ratio (%)	
	Dijkstra	GAC
0	0	0
20	11.12	18.46
40	28.32	46.31
60	42.71	59.41
80	65.62	72.93

Next thing is packet delivery ratio. This is computed by considering the total amount of users passed from source to destination. Since the defensive wall construction is large, the attacking objects can be identified easily and the attacker less regions is determined.



6. CONCLUSION

The proposed work provides the platform for energy efficiency framework for WSN architecture using Network Simulator (NS2). The framework is focused on energy management model and security. The security is implemented by grid based adversarial clustering. This security algorithm must be comprised of large number of labeled instances. This clustering concept can discover the region to protect the normal objects from the attacking segments. Three types of merge operations are employed in this method. And the defensive wall is constructed to provide more security. Once the attacking objects are identified, ants can pass from source to destination to obtain the food. This is done by ant colony optimization. The shortest route of travel can be obtained by allowing the ants to flow in the normal objects' direction. Once the food is found, the ant deposits the pheromone in the path while returning. This serves the map directing path for rest of the ants. This methodology will reduce the energy consumption and improve the security as well as energy efficiency of the network

REFERENCES

[1]Selman (2019), "An adaptive intelligent alarm system for wireless sensor network", Indonesian Journal of Electrical Engineering and Computer Science, Volume: 15, Pages: 138 – 143.

[2] Ajar Magray, Mudasir Younis, Chitaranjansharma (2019), "Wireless Sensor Networks Based on Shortest Path Algorithms", International Journal of Advanced Scientific Research and Management, Volume 4 Issue 1, Jan 2019. International Journal of Advanced Science and Technology Vol. 29, No. 3, (2020), pp. 11750 - 11759

[3] Zou, Z., Qian, Y (2019), "Wireless sensor network routing method based on improved ant colony algorithm", Journal of Ambient Intelligence and Human Computing **10,** 991–998 (2019). https://doi.org/10.1007/s12652-018-0751-1.

[4] Mohamed Elhoseny, Ahmed Farouk, Nanrun Zhou, Ming-Ming Wang, Soliman Abdalla, and JosepBatle (2017),"Dynamic multi-hop clustering in a wireless sensor network: Performance improvement", Wireless Personal Communications, pages 1–21.

[5] Wutao Wei, Bowei Xi, Murat Kantarcioglu (2018), "AdversarialClustering: AGridBasedClusteringAlgorithmAgainstActiveAdversaries", arXiv:1804.04780v1 [stat.ML] 13 Apr 2018.

[6] Liu, A., Ren, J., Li, X., Chen, Z. & Shen, X (2012),"Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks" Computer Networks, 56, 1951-1967.

[7] Bidoki, N. H., Baghdadabad, M. B., Sukthankar, G., & Turgut, D. (2018),"Joint value of information and energy aware sleep scheduling in wireless sensor networks: A linear programming approach", IEEE International Conference on Communications, 2018May, 1–6. doi: 10.1109/ICC.2018.8422392.

[8] Ben Arbi, I., Derbel, F., &Strakosch, F. (2017),"Forecasting methods to reduce energy consumption in WSN", I2MTC 2017 – 2017, IEEE International Instrumentation and Measurement Technology Conference, Proceedings, 0–5. doi: 10.1109/I2MTC .2017.7969960.

[9] Panda, M. Data security in wireless sensor networks via AES algorithm (2015), "Intelligent Systems and Control (ISCO)", 2015 IEEE 9th International Conference on. 2015. IEEE.

[10] Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key techniques (2012), "Computer Communication and Informatics (ICCCI)", 2012 International Conference on. 2012. IEEE.
[11] 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), pp. 11750 - 11759