International Journal of Multidisciplinary Research And Studies

Available online at https://ijmras.com/

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND STUDIES
ISSN: 2640 7272
Volume:04; Issue:05 (2021)

SECURE CLUSTERING AND TRUSTWORTHY ROUTING PROTOCOL IN WIRELESS SENSOR NETWORKS

Mukesh Kumar Singh

M.Phil., Roll No. :140425: Session: 2015-16

University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur

E-mail-: singh.mukesh96@gmail.com

ABSTRACT

Wireless Sensor Networks, also known as WSNs, are gaining in popularity as a potentially useful technology owing to the diverse array of applications that may be carried out using them. This is one of the reasons why they are called "WSNs." The monitoring of the environment is only one of many applications; others include those in the industrial, military, and civilian domains respectively. On the other hand, it is vulnerable to a wide variety of attacks of different sorts. The adversary was successful in compromising a node, which led to the loss of all data packets that were routed through that node. The data packets were lost as a consequence of the node being compromised. The amount of energy that can be pulled from batteries places severe limitations on the performance of sensor nodes, which in turn decreases the network's durability and overall quality. Because of this, it is very necessary for wireless sensor networks (WSNs) to make the most of the lifetime of its nodes and minimize the amount of bandwidth they require by coordinating locally among sensor nodes.

KEYWORDS: Clustering, Trustworthy, Wireless, Wireless Sensor, Compromising A Node.

INTRODUCTION

Wireless Sensor Networks, also known as WSNs, are gaining in popularity as a potentially useful technology owing to the diverse array of applications that may be carried out using them. This is one of the reasons why they are called "WSNs." The monitoring of the environment is only one of many applications; others include those in the industrial, military, and civilian domains respectively. On the other hand, it is vulnerable to a wide variety of attacks of different sorts. The adversary was successful in compromising a node, which led to the loss of all data packets that were routed through that node. The data packets were lost as a consequence of the node being compromised. As a direct consequence of this, sensitive data was either made completely unusable or was unable to be sent to the sink. Because the data that is seen by the nodes in the network is the basis for the decisions that are made by the network. As a consequence of this, the system will carry out its operations in an improper way and arrive at wrong results. Because of this, it is crucial for the safety of wireless sensor networks (WSNs) to recognize the assault and take precautions to prevent it. The currently available trust-based route options are being put to the test by a variety of challenging obstacles. Nevertheless, winning the trust of a node might be a difficult task at times. In WSNs, the amount of energy that is accessible at each node is severely limited. It takes a large amount of energy to complete both the process of gaining trust and the process of transferring data, which in turn shortens the total lifetime of the network. When it comes to WSNs, the issue of the security route is a challenging one to deal with. mostly due to the fact that it is difficult to determine which nodes on the network are malicious. In order to find solutions to these problems, we provide a trustworthy routing protocol and a safe clustering in WSN (SCTRP).

The use of security and trust routing in WSNs makes it possible to achieve high levels of routing dependability. In this particular instance, the CH was picked based on the node's trust, and the node's trust was calculated based on the energy that the node had. Because of this, it has a greater potential for reducing its overall energy use. The signature verification method is used in order to confirm the sensor node's capability of communicating the data across the networks by means of an authorized node. The remaining components of this work are structured as outlined in the following paragraphs. In Section 2 of this document, please provide a description of the connected works. A presentation on the trustworthy Routing Protocol in Wireless Sensor Networks (WSN) was given in Section 3, as was the Secure Clustering Protocol (SCTRP). A wireless sensor network, more often referred to as a WSN, is

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

a network system that monitors physical or environmental parameters, such as sound, temperature, and movement. Examples of these factors include: sound, temperature, and mobility. It makes use of wireless sensor nodes and is composed of distributed devices that are dispersed throughout the network geographically. A WSN is comprised of individual nodes that are able to detect the environment in which they are situated, perform local processing of the information that has been acquired, and wirelessly transfer the information that has been processed to one or more collecting points .

The amount of energy that can be pulled from batteries places severe limitations on the performance of sensor nodes, which in turn decreases the network's durability and overall quality. Because of this, it is very necessary for wireless sensor networks (WSNs) to make the most of the lifetime of its nodes and minimize the amount of bandwidth they require by coordinating locally among sensor nodes. A huge number of sensor systems are used in physically hazardous and often hazardous settings, such as battlegrounds and military domains with untrustworthy surroundings.

Because of this, the vast majority of practical WSNs have a considerable need for increased levels of security. Clustering sensor nodes together has been the subject of a considerable amount of investigation by researchers who are interested in determining whether or not it is possible to meet the scalability and administration requirements of the network system. Every cluster would be equipped with a leader sensor node, often referred to as the cluster-head (CH), which, depending on the specifics of the situation, may either be fixed in place or mobile. CHs combine the data obtained by the sensor nodes that are a member of their cluster. As a consequence of this combination, the number of packets that need to be sent is decreased. Clustering has a number of benefits, one of which is that it helps to preserve transmission bandwidth and minimizes the exchange of duplicate messages among sensor nodes. Clustering also offers a number of other advantages. This is accomplished by putting limits on the interactions that may take place between clusters. Clustering, as a direct consequence, results in an extension of the lifetime of wireless sensor networks.

The digital signature is one of the many distinct types of security services that can be obtained via cryptography. It is also one of the most significant. Establishing a digital certificate is the tried-and-true way for obtaining the binding between a signer's public key and their identity.

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

In the context of key management systems, this strategy is used. If there was no need for this binding, then the identity of the user would be the same as their public identity. This would be more time and resource efficient, as Shamir pointed out. The conclusion is discussed in the fifth part of the article. important In addition to this, if the user's identity is known, it is feasible to simply derive the public key with the assistance of specific methods that have been revealed in public.

An identity based (ID-based) signature system is provided by Hess and the question of whether or not an efficient ID-based encryption method might be devised remained an open question as of the publication of this article. The complexity of factoring integers is directly related to the level of protection provided by the ID-based signature system. In this study, we focus on the efficacy of secure communications and provide a secure routing protocol for cluster-based wireless sensor networks (WSNs) that makes use of ID-based digital signatures. The purpose of this protocol is to restrict access to areas that are not authorized. According to the design that we have shown, the cluster heads will choose themselves and will communicate directly with the base station (BS), while the leaf sensor nodes will decide whether or not to join a cluster according to how strong the transmission signal is. The cryptography that is based on IDs is used as the basis for the safe routing protocol. Users' public keys act as personal identification information in this kind of encryption, and users are able to get their corresponding private keys without the need for the transmission of any auxiliary data.

ROUTING ATTACK AND KEY MANAGEMENT

Sinkhole in which an attacker attempts to direct the traffic from a specific region through its node; wormhole attack, in which tunnel packets to other locations; and false neighbour relationship, in which a person pretends to be their neighbour. These are just some of the attacks that can be launched against the traditional routing protocol used in wireless sensor networks. An adversary who is conducting a Sybil attack may appear to have a large number of identities or locations, after which they will provide inaccurate information for routing in order to start phoney routing attacks In addition, eavesdropping, denial of service, and man-in-the-middle attacks are some of the most common dangers that may arise in wireless sensor networks This is because wireless sensor networks are prone to making errors and participate in open broadcasting of their data. In

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

order to guarantee the integrity of our routing protocol, we offer a technique for key management and combine it with methods for the selection of cluster heads and the establishment of routing routes. In this manner, we create a secure environment for the protocol.

Wireless Sensor Networks, sometimes referred to as WSN for short, are a kind of self-organizing, multi-hop wireless network that are made up of a large number of sensor nodes that may either be stationary or mobile. This type of network is commonly abbreviated with the acronym WSN. Because it is capable of carrying out a wide variety of tasks, wireless sensor networks (WSN) have garnered an increased amount of attention in recent years. The sensor nodes that come together to form a WSN have the capacity to carry out a variety of tasks, including data collection, event detection and identification, node control, position monitoring, and continuous position monitoring. These characteristics and wireless connection methods of sensor nodes increase the application possibility of WSN, which includes a variety of domains such as the military, ecological environment monitoring, intelligent transportation, and so on .

RESEARCH MYTHOLOGY

In WSNs, one strategy for topology control that is effective is to arrange sensor nodes together into clusters. The selection of Cluster Heads (CHs), who are responsible for generating clusters and regulating member nodes, has a significant impact on the efficiency with which clustering is carried out. The purpose of the clustering process is to go through a collection of sensor nodes in order to identify a group of nodes that have the potential to serve as CHs. It might be challenging to identify the best combination of CH nodes for a particular network design. There are N K various combinations of solutions available when there are N sensor nodes and K CHs. Enumerating each and every conceivable combination is a step in the brute-force approach of finding the best answer, which is a basic and simple process. However, due to the vastness of the solution space, the brute-force technique is not the best choice for addressing issues involving sophisticated spatial searches. When utilizing a strategy based on brute force, the level of computing complexity that is required to determine the best set of CHs for a big WSN is quite high . In addition, determining the best possible CHs is an iterative process that takes place online and necessitates speedy computation. If the search space is large, using brute force as a strategy might take many days or even several months. Illustration 5.1: If we consider a network that has 500 sensor nodes and 25 CHs, we can estimate that there are around 2,980 1067 unique alternative

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

solutions for only one cycle of operation. The process of enumerating all of the potential solutions might take many days or perhaps several months. This is not acceptable in a process that must be repeated, such as clustering, which is carried out in rounds, and each round may take minutes or even seconds to complete. It has been shown that the clustering issue in WSN is a Non-deterministic Polynomial (NP)-hard optimization problem [Clustering Problem in Wireless Sensor Networks] Finding answers to NP-hard issues requires conducting exhaustive searches over enormous catalogues of potential responses. Approaches from the field of evolutionary computing have shown to be effective when applied to a range of issues of this nature. In this chapter, the issue of CHs selection in WSN is described as a single-objective optimization problem. This is done in order to better understand the topic. In order to determine the best combination of CHs, a centralized weighted-sum multi-objective optimization strategy has been modified. The method that is being suggested locates a certain number of CHs in a way that causes them to cluster together after just one hop.

The suggested method's objective is to improve the network in terms of its capacity to scale, as well as its energy efficiency and dependability in terms of data transmission. Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Differential Evolution (DE) were the three evolutionary methodologies that were used to successfully answer the defined challenge (PSO). The effectiveness of each of the three strategies is evaluated according to the level of fitness that is attained. The best evolutionary algorithm technique is used to evaluate and compare the performance of the proposed protocol to that of other well-known clustering protocols. This evaluation and comparison is based on the findings of the performance assessment. In addition, in order to investigate the impact that reducing the total number of CHs has on the energy efficiency of the network, a hierarchical clustering strategy that creates two-hop clusters has been suggested as a methodology. The goal of the strategy that has been presented is to improve the energy efficiency of the network.

DATA ANALYSIS

The research literature has a number of different clustering procedures' suggestions. On the other hand, the majority of these protocols make assumptions that aren't practical about how the CHs will provide the aggregated data to the BS. They work on the assumption that each CH may use a "one-hop" strategy to transfer the aggregated data it has collected straight to the BS. However,

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

sensor nodes in WSN have a restricted communication range, and the base station (BS) is often situated at a considerable distance from the region being sensed, making it difficult for many nodes to reach the BS directly. A multi-hop strategy would be a more practical way to go about things since it would enable the CHs to collaborate with one another to establish a network that would direct the data towards the BS . It is a well-known fact that it is an NP-hard task to locate a reliable and energy-efficient routing tree that links the CHs to the BS . As a result, solutions based on evolutionary principles may be used to address this issue. PSO has been shown to have superior performance than that of GA and DE, as shown in the previous chapter. GA, which has extremely high processing needs . PSO's benefits include the simplicity with which it may be implemented on hardware or software, the provision of high-quality solutions as a result of its capacity to break free from local optimums, and the speed with which it can converge. In this chapter, the NPhard issue that has to be solved necessitated the use of PSO because of how successful it is in tackling such problems. The goal was to determine the best inter-cluster routing tree. Clustering and routing are both iterative processes; hence, an optimization approach that is easier to understand would yield more effective networks. PSO is a popular solution for resolving the issues associated with clustering and routing in WSNs for this reason, among many others. A centralized weighted-sum PSO-based protocol is suggested for use in this chapter as a means of finding the best possible inter-cluster routing tree.

When the CHs have already been decided upon in advance, it is acceptable to use this process. The protocol that has been suggested makes use of a particle encoding technique and specifies an objective function in order to locate the best routing tree. The aim function is used to develop the trade-off between the energy-efficiency of the generated tree and the dependability of the data transmission. It is anticipated, for the sake of this proposed protocol, that the CHs will be predetermined in advance by using the PSO-OC protocol. PSO-OC was chosen because it has been shown to have a greater PDR at the CHs while simultaneously maintaining a fair energy consumption level. This was an important factor in the decision-making process. TPSO-CR is an abbreviation that stands for "Two-tier Particle Swarm Optimization for Clustering and Routing protocol," which is the full name of the protocol that has been suggested. In the next sections, a comprehensive explanation of TPSO-CR is provided.

PARTICLE ENCODING PROCESS

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

There are exactly the same number of sensor nodes in the network as there are dimensions of the particle (i.e., N). Let Pi = [Xi,1, Xi,2, Xi,3,..., Xi,N] signify the ith particle of the population, where each component, Xi,d, 1 d N reflects the node's relative importance for being chosen as a relay node. On the basis of a uniform distribution, each component is given an initial value that is the result of a random number generation within the range.

PARTICLE DECODING PROCESS

During the branch growth process, a routing tree is constructed using the encoded particle as its basis. Every branch is a different path that leads from a CH to the BS. For instance, if there are two CHs in the network, the decoding procedure will provide two routes, one for each CH. This occurs because each CH has its own unique identifier. The construction of each route begins at the CH and continues with the addition of relay nodes. At each stage of the development of the route, the next node to be constructed is selected based on which of those that have direct linkages with the present node has the greatest priority. It is very improbable that a node that is previously part of a growing route would be chosen again since that node will be given a very low priority value and a significant negative priority value**.**

In the worst-case situation, if a node is picked again, the route in question may be regarded as illegitimate and may be given a large penalty value. This would be the case if the worst-case scenario occurred. The procedure will continue until all of the CHs are linked to the BS, at which point it will be complete. If a routing tree includes one or more invalid branches—that is, branches that do not finish on the destination node or that have loops—then the tree is deemed invalid, and it will be given a very high fitness rating as a punishment. The particle that includes priorities that direct the decoding operation to pick nodes that form the optimum routing tree is the best particle after a run of the algorithm. This particle is the best candidate for the optimal routing tree. Illustration 6.1: Consider a WSN with twenty sensor nodes and two cluster heads, denoted as N1 and N8 in This network would have a total of eighty nodes. Therefore, the size of the particles is equal to the number of sensor nodes, which brings us to the conclusion that N = 20. Let's have a look at the graph labelled G(V, E) that is shown in The fact that u may transmit to v but not necessarily vice versa is shown by the edge that reads "u v."

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

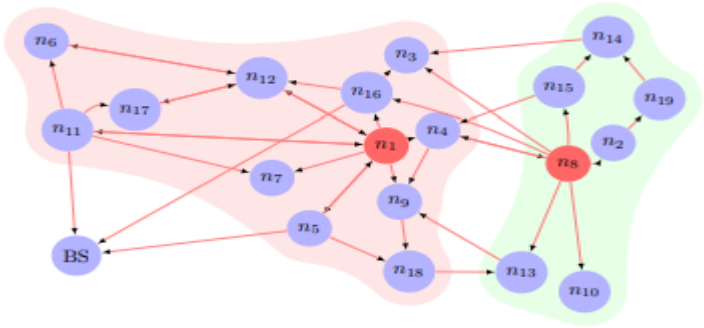

Figure 1 A Wireless Sensor Network With 20 Sensor Nodes And 2 Chs (N1 And N8)

Assume for the moment that a particle with the symbol Pi was produced at random, as shown in figure 1 (a). The protocol will first establish a route from N1 to the BS, and then it will build another route from N8 to the BS in order to find a routing tree that connects N1 and N8 to the BS. A node that is linked to N1 must be found first before a branch can be found that leads from N1 to the BS. The nodes are the ones that need to be taken into consideration, as can be seen in Figure 1. Their order of importance is in that particular order. Because Node 11 has the greatest priority, it is the one that is selected to serve as the subsequent relay node for N1.

However, its priority is changed to a high negative number N in order to prevent it from being chosen once again along the path. The potential nodes from node 11 are nodes . The corresponding priority of these nodes are as follows: In order to create the route, node 0 (BS) is used as the next relay node. This is due to the fact that it has the greatest priority. Due to the fact that the BS has been reached, the building of the route from N1 to BS has come to an end, which results in the route (8, 1, 0). The same process is carried out many times for the branch that leads from N8 to the BS in order to produce a whole route that consists of 8, 16, and 0. The steps involved in this procedure are shown in (b-d).

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

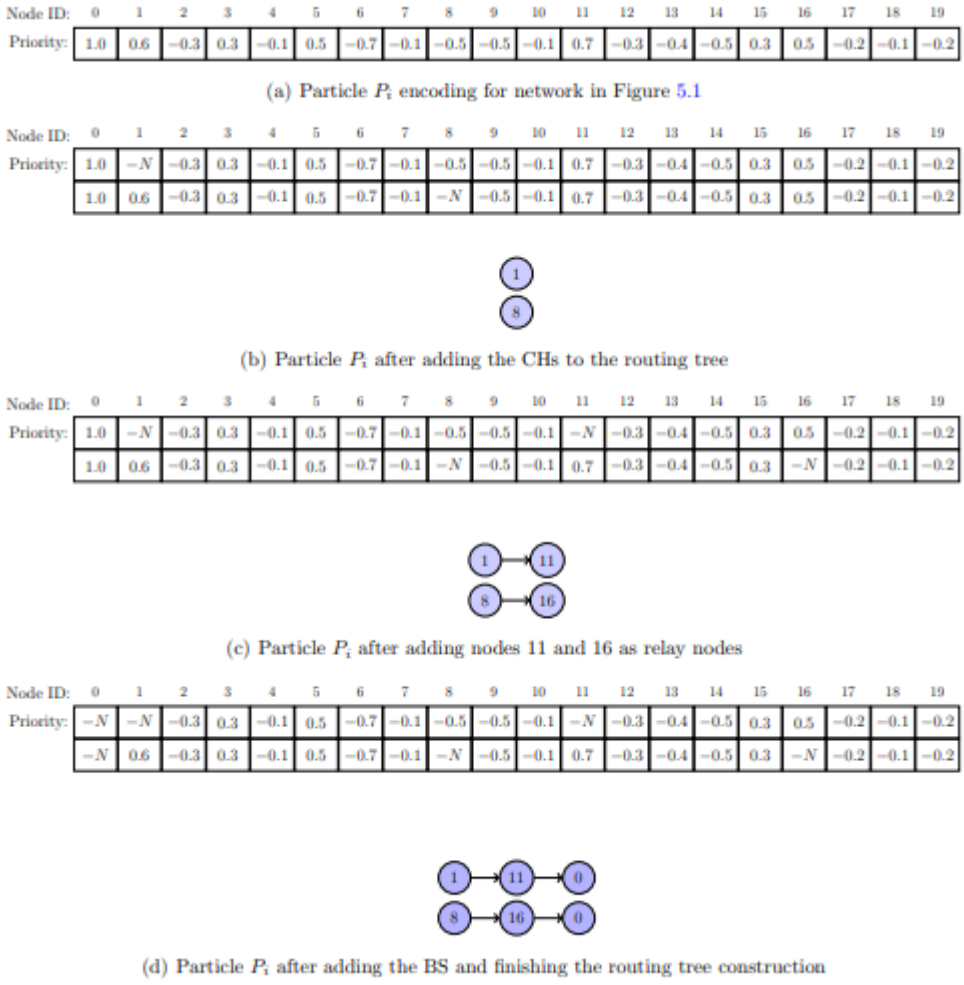

Figure 1 Example Of Priority-Based Encoding And Decoding Process For An Arbitrary Particle Pi

CONCLUSIONS

In recent years, the attention of the scientific community has been drawn to wireless sensor networks because to the potential uses that these networks might have in a variety of different fields. According to what we have seen, having a flat sensor network design might cause significant problems for the overall performance of the network. In this particular design, the unattended low-powered sensor nodes have the potential to rapidly drain their energy reserves, which will ultimately result in a shorter network lifespan. These issues may be remedied by implementing routing protocols that are based on the concept of clustering. Cluster-based routing offers an effective method for cutting down on the energy consumption of sensor nodes, which in turn helps to enhance the lifespan and scalability of wireless sensor networks (WSNs). In

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

WSNs, it is vital to adopt a routing protocol that is not only scalable but also dependable in terms of the delivery of packets. This protocol should also be energy efficient. There have been many different proposals made for clustering and routing protocols for WSNs. Problems that arise while trying to determine an appropriate radio model for the sensor nodes that make up the network do, however, put a damper on the performance of the protocols in question. For an estimate of the power consumption that is both more exact and more realistic, the use of a discrete radio model is recommended. Key needs for wireless sensor networks (WSNs) are energy efficiency, the ability to reliably relay data, and scalability. In the course of working on this thesis, our team came up with a collection of clustering and routing protocols that satisfy these objectives. Both clustering and routing in WSNs are well-known optimization issues, and both are recognised to be notoriously difficult non-deterministic polynomial (NP) problems. The findings of this study indicate that evolutionary strategies are capable of being effectively applied to the solutions of various difficulties. In addition, the results of several experiments have shown that in terms of the overall fitness value, the PSO algorithm is superior to both the GA and the DE algorithms.

REFERENCES

[1] S. H. Yang, "Introduction," in *Wireless Sensor Networks*, Signals and Communication Technology, pp. 1–6, Springer London, 2014.

[2] Y. Yu, V. K. Prasanna, and B. Krishnamachari, *Information Processing and Routingin Wireless Sensor Networks*. World Scientific Pub., 2006.

[3] M. Zungeru, L. M. Ang, and K. P. Seng, "Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1508–1536, 2012.

[4] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.

[5] K. Dwivedi and O. P. Vyas, "Network layer protocols for wireless sensor networks: Existing classifications and design challenges," *International Journal of Computer Applications*, vol. 8, no. 12, pp. 30–34, 2010.

[6] Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[7] L. M. Arboleda and N. Nasser, "Comparison of clustering algorithms and proto-

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*

cols for wireless sensor networks," in *IEEE Canadian Conference on Electrical and Computer Engineering*, pp. 1787–1792, 2006. A. Dabirmoghaddam, M. Ghaderi, and C. Williamson, "On the optimal randomized clustering in distributed sensor networks," *Computer Networks*, vol. 59, no. 0, pp. 17

[8] E. A. Khalil and B. A. Attea, "Energy-aware evolutionary routing protocol for dynamic clustering of wireless sensor networks," *Swarm and Evolutionary Computation*, vol. 1, no. 4, pp. 195–203, 2011.

[9] P. Kuila and P. K. Jana, "A novel differential evolution based clustering algorithm for wireless sensor networks," *Applied Soft Computing*, vol. 25, no. 0, pp. 414 – 425, 2014.

[10] P. Kuila and P. Jana, "Approximation schemes for load balanced clustering in wireless sensor networks," *The Journal of Supercomputing*, vol. 68, no. 1, pp. 87–105, 2014.

[11] P. Kuila, S. K. Gupta, and P. K. Jana, "A novel evolutionary approach for load balanced clustering problem for wireless sensor networks," *Swarm and Evolutionary Computation*, vol. 12, no. 0, pp. 48 – 56, 2013.

[12] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

Mukesh Kumar Singh*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: singh.mukesh96@gmail.com*