Denial of Service (DoS) Detection in Wireless Sensor Networks Applying Geometrically Varying Clusters

S. S. Nagamuthu Krishnan

Abstract Wireless Sensor Networks (WSN) have great benefits of reduced costs, lesser scalability factor, and can be employed upon complex and dangerous locations for the purpose of control/automation of tasks and for sensing, processing, sharing/forwarding data. Denials of service (DoS) attacks hinder the regular functioning of such networks leading to compromise of the objectives of them. In this paper a hierarchical clustering approach is proposed to detect the compromise of nodes in WSN due to DoS attacks. This approach outweighs other approaches in the aspect of elimination of outliers and faster response time in detecting the attacks.

Keywords Service denial · Clustering · Centroid · Heuristics · Partition Propagation

1 Introduction

In WSNs the network is embedded with the environment and the nodes that form the network can effectively perform sensing and actuation to have a measure or impart its influence on the environment [1]. The processed information in each node is communicated in wireless fashion. The communication happens through radio signals among the nodes. The target applications could be industry-oriented, Science related, transportation enhancing, maintaining civil infrastructure, security related, etc. The processor within the sensor nodes could be in one of the three modes of sleep, idle and active. The power source and memory capacity of the nodes are very limited.

The nodes in the network may be participating as sources that involves in measuring data, sink listening to receive data from the network and act as actuators for control of devices based on the transmitted data. The interaction patterns between the various sources and sinks will be for detection of events, periodical measurement

S. S. Nagamuthu Krishnan (✉)
Department of MCA, R V College of Engineering, Bengaluru 560060, India
e-mail: ssnkrishnan@gmail.com

S. Smys et al. (eds.), *International Conference on Computer Networks and Communication Technologies*, Lecture Notes on Data Engineering and Communications Technologies 15,
https://doi.org/10.1007/978-981-10-8681-6_93

and reporting besides some secondary needs. The primary characteristics of WSNs include good scalability, verifying number of nodes for a given area, reprogrammable capability, and conveniently maintainable. The most important limitation of such network is the limited energy, which has to be efficiently utilized for communication, sensing, computation and actuation [2, 3]. The nodes very importantly collaborate among themselves to achieve a common goal primarily through preprocessing.

The energy of sensor nodes could be wasted due to their exposure to Denial of service attacks. One common attack at the physical layer is node tampering that leads to destroy of keys related to encryption and decryption [2]. The link layer attacks could be continuous interrogation by sending RTS message for handshaking that makes the nodes completely busy with responding requests, denying the sensor nodes to move to the sleep mode, thus reducing the battery life of sensors [4]. Network layer attacks could be of IP spoofing effected by masking the source address as bogus address, or the address of a victim, homing attacks targeting key managers for blocking and neglecting, and greed attacks aiming on neglecting routing of some messages and greedy of sending own messages [5, 6]. The sole aim of the work presented here is to devise a new method to nominate control elements/nodes in WSN and find out the distance between other nodes of a subset of nodes. The beginning of the process is to employ a clustering algorithm termed as CURE clustering [7] and reapplying the clustering technique to every other cluster determined. The cluster heads are determined as control nodes to detect harmful traffic if any. The next section discusses on some related works, followed by usage of CURE clustering for control node selection, followed by discussion of simulation results. Here the main contribution is highlighted and future developments are also indicated.

2 Related Works

It is very common that dynamics exist in topology as well as traffic. In order to accommodate that, clustering technique among nodes is adopted. Clustering groups a set of nodes such that the nodes in a cluster have similar properties. The similarity among the nodes (points) is normally defined using distance measures of Euclidian, Cosine, Jaccard, etc. Here all the nodes compete to become head and increase the chance of detecting denial of service attack [8] through the entry points of the sensor network.

Several clustering algorithms following the principles of hierarchical, heuristics based and partition based exist. Hierarchy-based clustering works on the principle that each point is cluster by itself. The key operation here is to merge two nearest clusters into the merged cluster to elect the head upon the nodes that are accessible within the range of radio signals [3, 9].

One popular clustering algorithm is K-Means that assumes Euclidian space for distances. BFR clustering algorithm for handling very large data sets considers clusters to be normally distributed around the centroid of the cluster [10].

Partitioning-based clustering algorithms [11, 12] involve movement of instances from one cluster to another. The number of clusters to be arrived is preset by the users and all possible partitions are exhaustively enumerated. Error minimizing algorithm with the basic idea of finding a structure minimizing certain error criterion, say sum of squared error for giving an approximate solution for minimizing errors. This is also employed by K-means algorithm which is the simplest and most common algorithm that also comes under this category [13].

Heuristics-based clustering algorithm works on the basis of definite heuristic. MaxMin D clustering [14] is a technique where there cannot be any node more than D hops distance from the head of the cluster. In this algorithm the cluster head is selected by performing $2d$ flooding rounds. In the first "d" round the nodes propagate largest node ID and the second "d" round is used by the nodes to propagate smallest node IDs. The rules adopted here are, if any node has received its id, it declares itself as cluster head, nodes look for pairs and select minimum node pair to become cluster head [13]. Linked cluster algorithm [14] is another example for this category where the cluster head is elected by choosing the lowest ID among non cluster head nodes or nodes that are at one hop distance from the cluster heads.

Low Energy based Adaptive Clustering Hierarchy (LEACH) and energy efficient hybrid clustering are examples for this. LEACH is a time division multiple access based protocol. Four phases involved here are, advertisement by cluster head for nodes to become member, setting up phase where the nodes answer to the heads, creation of schedule by the cluster head based on time division multiplexing and sending to cluster member during the time of data transmission [15].

Here we consider a hierarchical clustering algorithm CURE [7] with special capabilities of recognizing arbitrarily shaped clusters, not affected by outliers and linearly increasing storage requirements detection of Denial of Service attacks in a large network. The steps that are adopted here aim for inserting the node information of all the nodes into a tree and treating each node in the tree as a cluster for computing closest for each cluster, to be inserted into a heap. The closest clusters collect information on varied behavior indicating DoS activities and report to the elements of the cluster through the cluster head. This reduces the distance through which the information has to traverse.

3 Proposed Method

The proposed method employs DoS detection in a sensor network among the scattered nodes applying a hierarchical clustering algorithm proposed by [7]. Here the number of sensor nodes to be chosen is determined as a constant "C". The number of scattered nodes decides on the shape and extent of the cluster. The totally scattered points are shrunk towards the centroid decided by a fraction Cr. These points act as representatives of the cluster. The clusters of sensor nodes with the closest pair of representative nodes are merged at each step of the clustering algorithm thus alleviating the disadvantage of all points and centroid based clustering algorithm.

Table 1 Simulation parameters

	No. of nodes	Shape of clusters	No. of cluster
Data set 1	900	Small circles and ellipsoids	4
Data set 2	900	Small rings	6
Data set 3	1200	Circles	10

This process enables to correctly identify the clusters, and the approach is relatively less sensitive to the outliers as the number of nodes scattered are shrunk towards their mean thus dampening the adverse effects due to outlier nodes. This method of multiple scattered points enable discovering elongated clusters where the space within the vicinity of clusters is obviously non-spherical.

The algorithm begins by drawing a random sample of nodes representing the geometry of clusters, reasonably accurate for correctly clustering the input set of clusters and effective DoS detection. The minimum size of the sample is chosen to be in exponentially decreasing form and contain a fraction of nodes for every cluster. Here partitioning of the sample is carried out, and further clustering is done with very partition. Elimination of non-considered values (outliers) that contribute least for denial of service detection is carried out next, and partitions finally clustered during the final pass. The merging of clusters is repeated until arbitrary number of clusters is arrived, such that transfer of attack information is done in minimum time.

The algorithm builds clusters and inserts into a heap. At any point in time the cluster at the top of the heap is the closest to the next immediate cluster. Every iteration in the algorithm deletes the top element "Q" and then merges closest clusters at the next level. The representative points of the merged cluster are the union of representative nodes of the clusters that are merged. After merging the distance between them is recomputed.

For larger number of nodes the combination of random sampling and partitioning could be effective in identifying the clusters. Outlier handing technique is combined with random sampling to eliminate outliers. The partitioning constant is set to three here and clustering of partitions is continued, until the no. of nodes remaining is one-third of the number of nodes initially. Clusters that contain one node are eliminated as outliers. Then as the total clusters reach a value k, here too the outliers are removed as clusters that contain as many as five nodes.

The testing experiment is carried out through simulation with three data sets having nodes on two dimensions (Table 1).

The algorithm was run with the data sets 1–3 mentioned above and it moderately shrunk to a mean factor of 0.4 enabling it to be less sensitive to outliers.

The simulation experiment also prove that for a node representative value of greater than 10 right number of clusters, for effective DoS detection information propagation were found. The splitting of clusters was also carried out fairly during the instances of large distance between the representative nodes, enabling speedier communication among them during anomalous traffic. The study also proved that

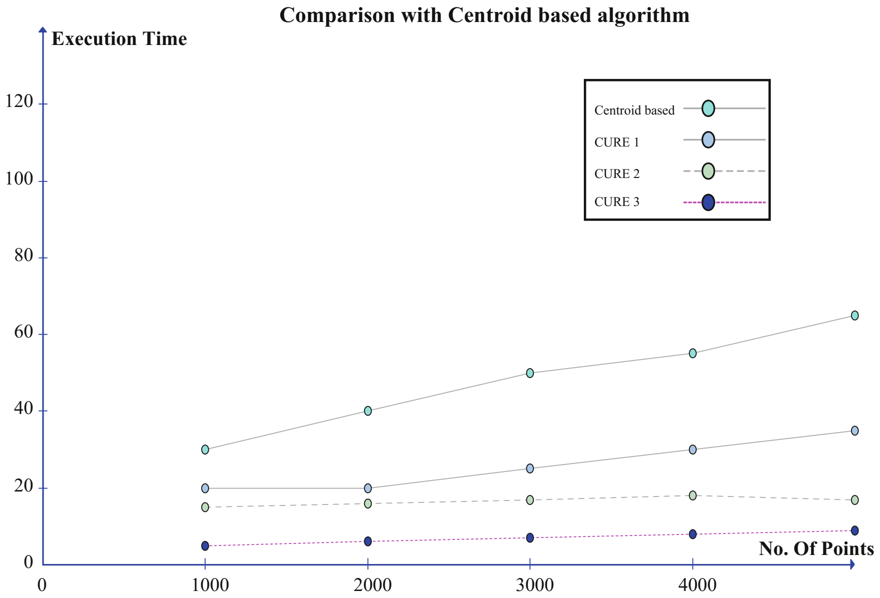

Fig. 1 Execution time comparison with centroid based algorithm

for a value close to 50 partitions the desired number of clusters was discovered for effective DoS detection and information propagation. When the number of partitions was successively increased the quality suffered due to reduction in number of representative points.

The execution time of the partitioning algorithm is also relatively lesser as compared to the other counterparts as it combines the techniques of random sampling and partitioning in a way to bring down the input size of the nodes. This is particularly seen as the number of nodes is increased. The execution time increases very little as the sample size remains the same (Fig. 1).

The graphical representation indicates the comparison of execution times of the clustering algorithm for three different shapes of clusters viz. small circles and ellipsoids, small rings, and circles. The execution times tend to improve in all the three cases when compared to that of Centroid based algorithm (Fig. 2).

The graphical representation given below shows the relationship between the no. of partitions taken for the sample run with the sample sizes of 1000, 2000 and 3000 nodes respectively. It clearly indicates the decrease in time of execution of the algorithm as the no. of partitions increase resulting in faster communication among the node representatives on DoS detection.

The third aspect analysis is on representative points versus execution time for the algorithm. It proves that the execution time tends to increase as the number of representative points increase for the three sample sets taken for the study. This recommends the choice of lesser representative points to achieve the execution time.

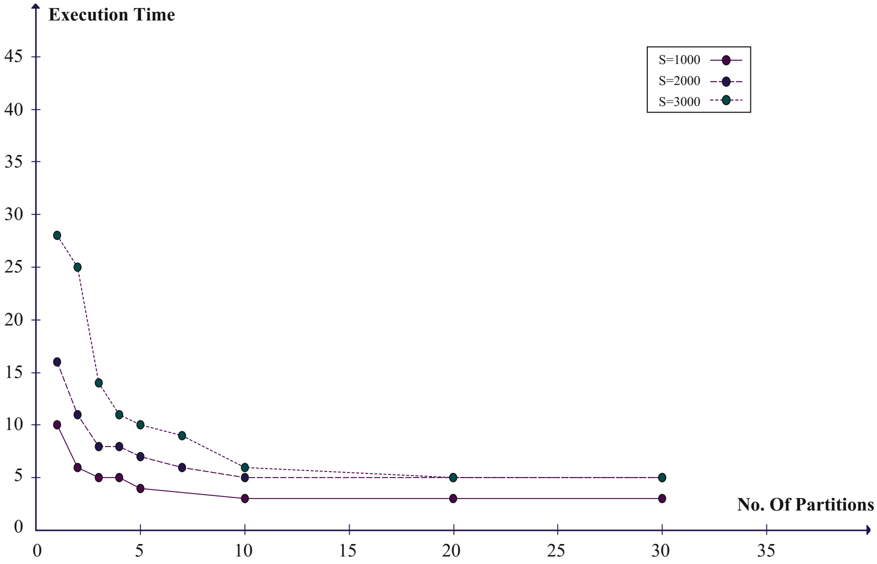

Fig. 2 No. of partitions versus execution time

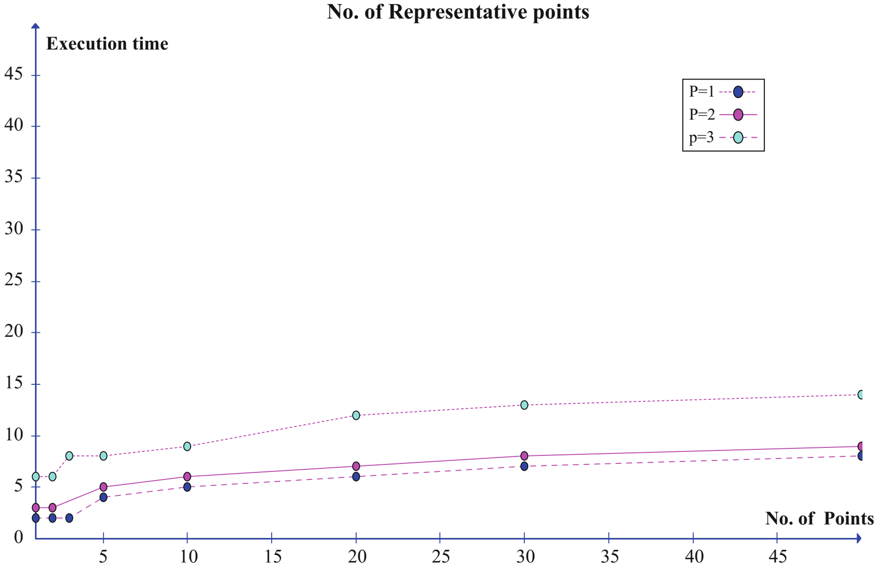

Fig. 3 Cluster representative points versus execution time

But, considering the speeder propagation of DoS attack information among the sensor nodes, a slight increase in execution time is inevitable to prevent further damage to the sensor network, on identification of anomalous behavior in a node (Fig. 3).

4 Conclusion

The algorithm uses multiple representative points (nodes) by selecting well-scattered nodes and then shrinking them to the center by a fractional number enabling effective identification and propagation of DoS attack information. This results in wide-varying geometrical shapes to the clusters. A Combination of random sampling with partitioning is used for larger number of nodes for faster identification of attacks. Filtering of outliers is also done effectively through random sampling. The time is estimated to the order of $O(S^2)$ for a sample of size S and space complexity varies linearly with “S”. The primary benefit of the identification procedure applying the clustering algorithm is scalability for large number of nodes without compromising cluster quality. The rate of identification of attacks and the time period could be further improved by considering an alternative clustering procedure that improvises the distribution/scattering of nodes in a network.

References

1. www.vonbi.ac.ke/conferences/WSN/day1/introduction.pdf
2. Lai, G.H., Chen, C.-M.: Detecting denial of service attacks in sensor networks. J. Comput. **18**(4) (2008)
3. Jain, A.K., Dubes, R.C.: Algorithms for Clustering Data. Prentice Hall, Englewood Cliffs, New Jersey (1988)
4. Heizelman, W.R.: Energy efficient communication protocol for wireless microsensor networks. In: Proceedings of IEEE Hawaii international Conference in System Sciences (2000)
5. Wood, A.D., Stanklovic, J.A.: Denial of service in sensor networks. IEEE/Computer 49–56 (2002)
6. Dhara, B., Devesh, J.: Denial of service attacks in wireless sensor networks. In: International Conference on Current trends in Technology (2010)
7. Guha, S., Rastogi, R., Shims, K.: CURE: an efficient clustering algorithm for large databases. Inf. Syst. **26**(1), 35–58 (2001)
8. Guechari, M., Mokdad, L., Tan, S.: Dynamic solution for detecting denial of service attacks in wireless sensor networks. In: Proceedings of IEEE ICC 2012—Ad-hoc and Sensor Networking Symposium, pp. 173–177 (2012)
9. Olson, C.F.: Parallel algorithms for hierarchical clustering. Technical report, University of California at Berkeley (1993)
10. Springer: https://link.springer.com/chapter/10.1007/978-1-4939-2468-4-1
11. www.csie.ntpu.edu.tw/~tschen/course/96-1/wn-ch10.pdf
12. Raymond, D.R., Midkiff, S.F.: Denial-of-service in wireless sensor networks: attacks and defenses. IEEE CS Pervasive Comput. 74–79 (2008)
13. Amis, A., Prakash, R., Vuong, T., Hymnh, D.: Max-min D-cluster formation in wireless Ad-Hoc networks
14. https://web.stanford.edu/class/cs345a/slides/12-clustering.pdf
15. Meng, T., Volkan, R.: Distributed network protocols for wireless communication. In: Proceedings of IEEE ISCAS (1998)

Dr. S. S. Nagamuthu Krishnan obtained his Bachelor's degree in Physics from Madurai Kamaraj University during 1995 and Masters Degree in Computer Applications from Bharathiar University during 1998. He has completed his Ph.D. in Computer Science in the Department of Computer Science and Engineering, Bharathiar University during 2015. He specialized on security in Networks. His research area includes detection and prevention of Distributed denial of service attacks in networks. He has presented many research papers in National, International conferences and Journals. He has totally 19 years experience in teaching. He is a life member of Computer Society of India. He has served in various premier educational institutions in Tamil Nadu, India and at present, he is working as Assistant Professor in the Department of Computer Applications of R V College of Engineering Bangalore.