DISTRIBUTED AND SECURE STUFFED CLUSTERING ALGORITHM FOR WSNs

[1]JayaVidhyaSri.S, [2]Sabitha.S, [3]Saranya.S, [4]Sasikala.S, [5]Gayathri.D ,[6]M.Hemalatha
[1,2,3,4]UG Scholars, [5]AssistantProfessor, [6] Software Engineer
[1,2,3,4,5]Department of Electronics and Communication Engineering
Knowledge Institute of Technology, Kakapalayam, Salem-637504, Tamil Nadu, India.
[6]Robert Bosch Engineering andBusiness Solutions Pvt Ltd, Coimbatore

[1]jayavidhyasri@gmail.com,
2sabithakayathiri@gmail.com,[3]saransrti@gmail.com,[4]sasikalaecekoit@gmail.com,[5]dgece@kiot.ac.in

ABSTRACT

The main concern of clustering approaches for mobile wireless sensor networks is to extend the battery life of the individual sensors and the network lifetime. This paper proposes a distributed and a safe weighted clustering algorithm which is a figurative version of the previous algorithm (ES-WCA) for mobile WSNs using a combination of 5 metrics. Among these metrics lie the behavioral level metrics which promotes a safe choice of cluster head where it'll never be a malicious node. The goals of the proposed algorithm are: detecting common routing problems and attacks in clustered WSNs, based on behavioral level and solving those problems and fixing it. The highlight of our work is summarized in the comprehensive strategy for monitoring the networks, in order to detect and remove the malicious nodes. Generating the reduced number of balanced and homogeneous clustered in order to minimize the energy consumption of the entire network and prolong sensors lifetime. We have implemented and tested a simulation proposed algorithm to demonstrate its performance.

Keywords: WSNs, clustering, security attacks,malicious node, simulation.

I INTRODUCTION

The main idea of our algorithm to ensure the choice of a legitimate Cluster Head (CH) is to never elect a node that moves frequently even if it has the best performance metrics. So, in this paper, the ES-WCA algorithm detects the internal misbehavior nodes during distributed monitoring process in WSNs by the follow-up of the messages exchanged between thenodes. This paper proposes a distributed and secure stuffed clustering algorithm for mobile WSNs using a combination of the existing metrics to which the behavioral level metric is added. The latter metric is decisive and allows to the proposed clustering algorithm to avoid any malicious node in the neighbourhood to become a CH, even if the remaining metrics are in its favour. The election of CHs is carrying out using weights neighbouring nods which are computed based on selected metrics. So this strategy ensures the election of legitimate CHs with high weights.

II LITERATURE REVIEW

Etuk, Enobong E., S. Magesh proposed a "Secure Clustering Algorithm for Wireless Sensor Networks in the Perspective of Authentication". Authentication happens to be a fundamental security service in cluster based wireless sensor networks. This project will focus on designing a lightweight authentication scheme that will aim at achieving authentication of cluster members with cloud enabled cluster heads. This model also presents a hierarchical and on-demand cluster maintaining method in the clustered wireless sensor networks, ensuring that the network can identify and get rid of malicious nodes, achieve cluster-formation, self-management and self-sustenance based on the random/parallel cluster header selection algorithm and a pre-distributed key scheme. It will address

secure mechanism on nodes joining in or quitting from network and a secure clustering algorithm based on the ant colony approach is proposed to make sure that mobile nodes joining in and quitting from network safely is based onauthentication and secret telecommunications. An information security for wireless sensor network, simulation results will show that the proposed model is promising in terms of networking security, efficiency and adaptability. RosanaLachowski , Marcelo E. Pellenz , Manoel C. Penna , EdgardJamhour and Richard D. Souza describes Monitoring and data collection are the two main functions in wireless sensor networks (WSNs). Collected data are generally transmitted via multi hop communication to a special node, called the sink. While in a typical WSN, nodes have a sink node as the final Destination for the data traffic, in an ad hoc network, nodes need to communicate with each other. For this reason, routing protocols for ad hoc networks are inefficient for WSNs. Trees, on the other hand, are classic routing structures explicitly or implicitly used in WSNs. In this work, we implement and evaluate distributed algorithms for constructing routing trees in WSNs described in the literature. After identifying the drawbacks and advantages of these algorithms, we propose a new algorithm for constructing spanning trees in WSNs.The performance of the proposed algorithm and the quality of the constructed tree were evaluated in different network scenarios. The results showed that the proposed algorithm is a more efficient solution. Furthermore, the algorithm provides multiple routes to the sensor nodes to be used as mechanisms for fault tolerance and load balancing.NadeemJavaidEmail author, Muhammad Babar Rasheed, Muhammad Imran, Mohsen Guizani, Zahoor Ali Khan, Turki Ali Alghamdi and ManzoorIlahi proposed "An energy-efficient distributed clustering algorithm for heterogeneous WSNs". Wireless sensor networks (WSNs) were envisaged to become the fabric of our environment and society. However, they are yet unable to surmount many operational challenges such as limited network lifetime, which strangle their widespread deployment. To prolong WSN lifetime, most of the existing clustering schemes are geared towards homogeneous WSN. This paper presents enhanced developed distributed energy-efficient clustering (EDDEEC) scheme for heterogeneous WSN. EDDEEC mainly consists of three constituents i.e., heterogeneous network model, energy consumption model, and clustering-based routing mechanism. Our heterogeneous network model is based on three energy levels of nodes. Unlike most works, our energy consumption modeltakes into account the impact of radio environment. Finally, the proposed clustering mechanism of EDDEEC changes the cluster head selection probability in an efficient and dynamic manner. Simulation results validate and confirm the performance supremacy of EDDEEC compared to existing schemes in terms of various metrics such as network life.

III METRICS FOR CHs SELECTION

Cluster head (CH) can be selected by computing quality of nodes are depend on several metrics such as connectivity degree, residual energy and distance of a node from its neighbors. [1] This part introduces the different metrics for CH selection by focusing on behavioural level metric .Mobility(M_i),connectivity(C_i) ,residual energy(Er_i), and distance of node n_i(D_i) to its neighbours. Significant improvement in performance of this quality can be achieved by combining these metrics.

Fig-1: The behavioural level of node n_i(BL_i):

The term metrics means the set of properties of a communication path in the field of networking. Metrics are commonly used for navigation of nodes. [2] Metrics selection is based on generation of homogeneous clusters whose size lies between two threshold :$Thresh_{upper}$ and $Thresh_{lower.}$ These threshold are arbitrarily selected or they depend on the topology of the network .Behavioural level also termed as physical behaviour which describes locomotion, looking around, time and error classification. The representation of behavioural level of a node is described in the fig-1.

IV STUFFED CLUSTERING ALGORITHM

Clustering means grouping nodes that are close to each other. In WSNs it is used to reduce useful energy consumption and routing overhead. [3] There are two kinds of nodes can be found inside the cluster, one node is called Cluster Head (CH) that is responsible to coordinate the cluster activities, and several ordinary nodes are called Cluster Members (CM) that have direct access only to one cluster head.

An ordinary node that is able to hear two or more cluster head and it acts a gateway. [4] For each communication initiated by a cluster member to a destination inside the cluster must pass by cluster head. If the destination is outside the cluster, the communication must be forwarded by a gateway and consequently consume more energy compared with cluster members. This algorithm combines these system parameters with certain weighting factors according to the system needs. The algorithm runs in three phases: the Set up phase, Re-affiliation phase and Monitoring phase. [5] The phase used in this paper is Monitoring phase whose architecture is shown in the fig-2. It involves various steps to get the determined output with efficiency whose flow is determined in the fig-3. WSNs simulator "NS2" reveals the internal misbehaviour in the course of the disseminated monitoring process in WSNs by the follow- up of the messages exchanged between the nodes .We estimate that the network has prev0iously a mechanism of avoidance to prevent the external

attacks. All the received messages are analyzed by using a set of rules. [6]

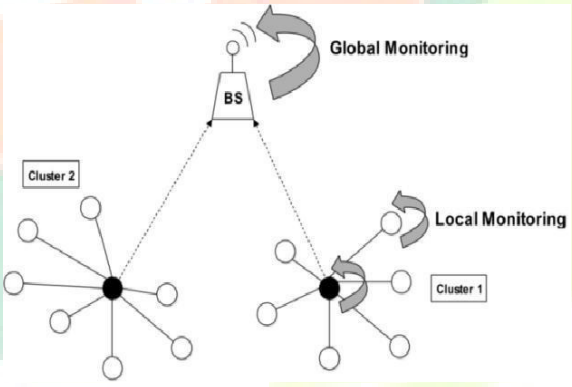

Fig-2: Monitoring phase architecture

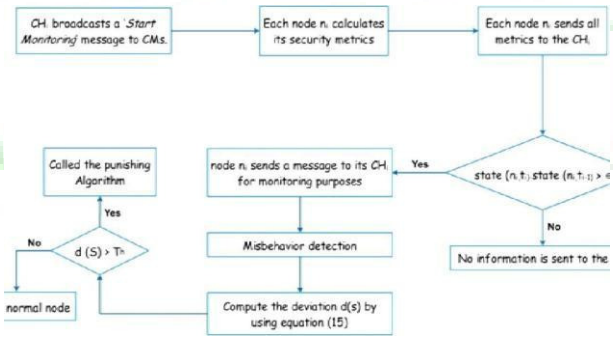

Fig-3: Flowchart of monitoring phase

V SIMULATION & RESULTS

To evaluate the proposed algorithm NS2 simulator is used and the procedure has been carried out to ensure the determined output. The output is Graphical Visualization which can be determined in XGRAPH which is highlighted in the fig-4. The algorithm demonstration is carried out with 200 nodes with the varying CH and CM.

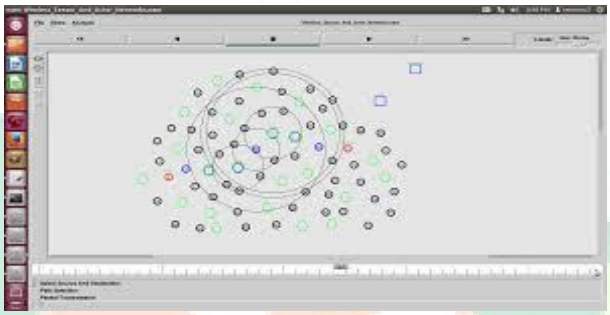

Fig-4: Simulation Output for clustering algorithm

VI CONCLUSION

This paper highlights the simulation output of our objectives to detect misbehaving nodes and the nature of attacks. To do this, we involved stable metrics to select CHs. Among these metrics, there is the behavioral level parameter which guarantees safe selection of CHs. The proposed algorithm chooses the most robust and safe CHs with the responsibility of monitoring the nodes in their clusters and maintaining clusters locally. Monitoring the phase analyses and detects specific misbehavior in the WSNs by the follow-up of the messages exchanged between the nodes. In addition the cluster-based architecture to examine passive attacks and to provide stable and reliable surveillance environment is also examined and the results are graphed.

REFERENCES

[1] T. Predrag and G. Agha. Maximal clique based distributed group formation for autonomous agent coalitions. In Coalitions and Teams Workshop (W10), 3rd Int'l Joint Conf. on Agents and Multi Agent Systems, 2014.

[2] A. Amis, R. Prakash, T. Vuong, and D. Huynh. Max-Min D-cluster formation in wireless ad hoc networks. In INFOCOM, 2012.

[3] D. Baker, A. Ephremides, and J. Flynn. The design and simulation of a mobile radio network with distributed control.IEEE Journal on Selected Areas in Communications, SAC-2(1):226–237, 2006.

[4] S. Bandyopadhyay and E. Coyle. An energy efficient hierarchical clustering algorithm for wireless sensor networks. In INFOCOM, 2009.

[5] S. Basagni. Distributed clustering for ad hoc networks. In In-ternational Symposium on Parallel Architectures, Algorithms and Networks (ISPAN '99), 2008.

[6] H. Chan and A. Perrig. ACE: An emergent algorithm for highly uniform cluster formation. In European Workshop on Wireless Sensor Networks (EWSN 2004), Jan 2004.

[7] M. Chatterjee, S. Das, and D. Turgut. WCA: A weighted clustering algorithm for mobile ad hoc networks. Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks),5(2):193–204, 2002.

[8] J. R. Douceur. The Sybil attack. In First International Work-shop on Peer-to-Peer Systems , Mar 2012.

[9] M. Garey and D. Johnson. Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman And Company, 2013.

[10] M. Gerla and J. T. Tsai. Multicluster, mobile, multimedia radio network. Wireless Networks , 2014