ESTUDAM Bilişim Dergisi
Cilt 3, Sayı 1 , 6-10, 2022

Journal of ESTUDAM Information
Volume 3, Issue 1, 6-10, 2022

DOI: 10.53608/estudambilisim.1021409

(Geliş Tarihi / Received Date: 09.11.2021, Kabul Tarihi/ Accepted Date: 06.01.2022)

Network Load Effects on Wireless Sensor Network Node Activity

Zuhal CAN*[1], Elif DEĞİRMENCİ[2]

[1]Eskişehir Osmangazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, 26480, Eskişehir, ORCID No : http://orcid.org/0000-0002-6801-1334

[2] Eskişehir Osmangazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, 26480, Eskişehir, ORCID No : http://orcid.org/0000-0001-8772-4543

Keywords:
Wireless sensor network, Node activities, Network load

Abstract: Due to the failure-prone and vulnerable structure of WSN nodes, understanding the typical activity patterns of nodes helps identify the faulty and malicious node activities and differentiate normal node behaviors from abnormal node behaviors. In this study, for understanding the typical node activities, we observe the effects of the network load on energy consumption, packet throughput, and latency parameters. We run simulations of networks with a variable number of sinks up to 5 in a network of various sizes. We observed a growth in the network load as the source and sink node request activities increased. We found that increasing the number of sinks affects the overall network load and causes communication delays between the source and sink node.

Kablosuz Sensör Ağı Düğüm Aktivitesi Üzerinde Ağ Yükü Etkileri

Anahtar Kelimeler:
Kablosuz sensör ağları, Düğüm aktivitesi, Ağ yükü

Özet: WSN düğümlerinin savunmasız ve arızaya meyilli yapısı nedeniyle, düğüm aktivite biçimlerinin anlaşılması, arızalanmaya yatkın veya kötücül olan düğümleri tanımlamaya ve normal düğüm davranışları ile anormal düğüm davranışlarının ayrılmasına yardımcı olur. Bu çalışmada, düğüm aktivitelerini anlamak için; ağ yükünün düğümlerin enerji tüketimi, paket alma verimi ve gecikme parametrelerine etkilerini gözlemledik. Çeşitli sayıda düğümlü ağ simulasyonlarını en fazla 5 adet olacak şekilde farklı sayılarda veri sorgulayıcılarıyla çalıştırdık. Kaynak ve sorgulayıcı düğümlerinin istek etkinlikleri arttıkça ağ yükünde bir büyüme gözlemledik. Sorgulayıcı sayısındaki artışın ağ yükünü etkilediği ve kaynak düğüm ile sorgulayıcı düğüm arasındaki iletişim gecikmelerine sebep olduğu sonucuna vardık.

1. INTRODUCTION

Recent technological advances in Wireless Sensor Networks (WSNs) allow the development of diverse applications for environmental data collection and processing [1]. Since WSN applications are mainly developed for harsh environmental conditions, WSN devices are designed with disposable and inexpensive materials, which causes WSN nodes to be failure-prone and vulnerable to various network attacks. These deficiencies cause some network units or the overall network to fail, especially when the communication and processing overhead is heavy.

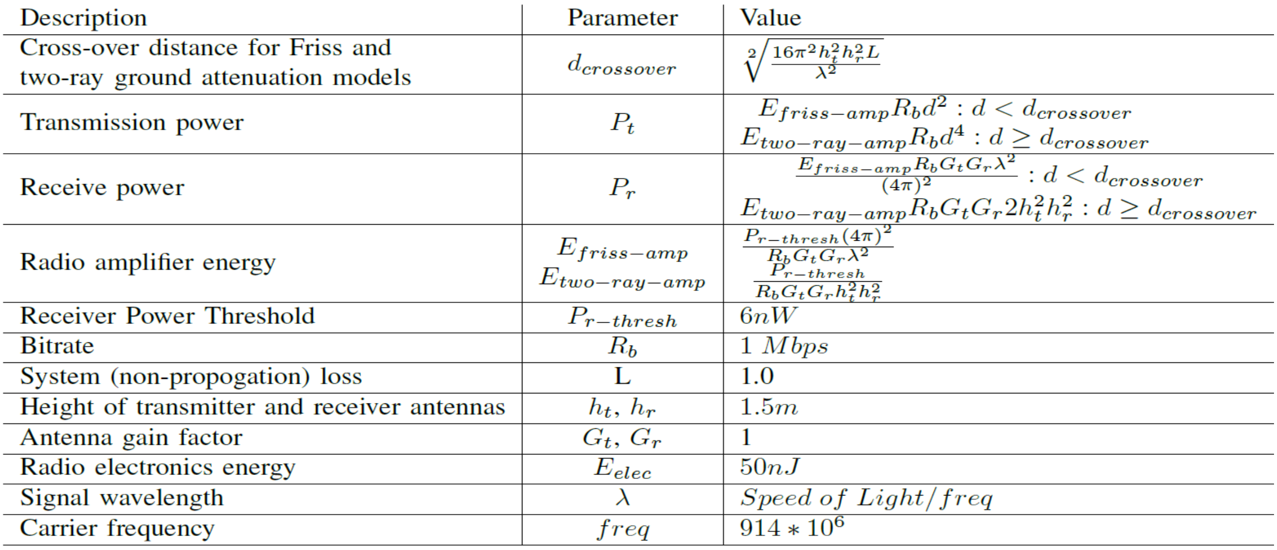
The energy-restricted and vulnerable structure of nodes is the constraint of WSNs. Energy utilization and security techniques help determine the network lifetime. Several strategies are developed based on Wireless Sensor Network (WSN) node activities to improve node security by balancing the network load [2]. Understanding the typical node behavior is essential to developing effective security mechanisms in WSNs.

In this study, we focus on the typical node behavior patterns by expanding the network load to help detect and prevent abnormal nodes. We define the network load as the total sent and received messages at a given time. Section 2.1 describes our WSN model and defines related parameters for analyzing node behavior. In Section 2.2, we express our simulation parameters and details. We explained our simulation results in Section 3. We discuss our findings in Section 4 and conclude

*İlgili yazar/Corresponding Author: zcan@ogu.edu.tr the paper.

Table 1

Energy Parameters



Description	Parameter	Value
Cross-over distance for Friss and two-ray ground attenuation models	$d_{crossover}$	$\sqrt[2]{\frac{16\pi^2 h_t^2 h_r^2 L}{\lambda^2}}$
Transmission power	P_t	$E_{friss-amp} R_b d^2 : d < d_{crossover}$ $E_{two-ray-amp} R_b d^4 : d \geq d_{crossover}$
Receive power	P_r	$\frac{E_{friss-amp} R_b G_t G_r \lambda^2}{(4\pi)^2} : d < d_{crossover}$ $E_{two-ray-amp} R_b G_t G_r 2 h_t^2 h_r^2 : d \geq d_{crossover}$
Radio amplifier energy	$E_{friss-amp}$ $E_{two-ray-amp}$	$\frac{P_{r-thresh}(4\pi)^2}{R_b G_t G_r \lambda^2}$ $\frac{P_{r-thresh}}{R_b G_t G_r h_t^2 h_r^2}$
Receiver Power Threshold	$P_{r-thresh}$	$6nW$
Bitrate	R_b	$1\ Mbps$
System (non-propogation) loss	L	1.0
Height of transmitter and receiver antennas	$h_t,\ h_r$	$1.5m$
Antenna gain factor	$G_t,\ G_r$	1
Radio electronics energy	E_{elec}	$50nJ$
Signal wavelength	λ	$Speed\ of\ Light/freq$
Carrier frequency	$freq$	$914 * 10^6$

2. METHODS

2.1. System Model

We analyze data on a flat wireless sensor network model in which there is no hierarchical clustering. The network is homogenous; all nodes are equipped similarly, and there is no central control unit on the network. Any node in the network can gather, store and process data, and initiate and relay network messages. Nodes store, forward, and aggregate data using in-network data collection and processing methods.

We use Gear protocol [3] as the routing protocol for our network communications. Gear protocol allows data-centric and geographical routing. Nodes, initially, gather neighbor information from received broadcast messages. After having neighbor information, nodes forward messages to the next neighbors on the destination path using routing mechanisms of the Gear protocol.

We define the network load as the total sent and received packets on a network. The network load depends on the number of sources and sinks. Some nodes are initially assigned as the source and sink nodes in our model. These pre-determined source and sink nodes are in charge of data acquisition. Source nodes detect, collect and store data. Sink nodes request data by sending subscription messages into the network. Whenever a source node receives a subscription message, it replies to the sink node with the related data. Relay nodes on the data propagation path transmit data packets between a source and a sink node. In our model, after data transmission starts between the sink and source node, the source node updates the sink node by data packets periodically, for some time, to guarantee data acquisition by the sink node.

In our model, WSN nodes are not mobile. Network nodes are initially deployed on the deployment area. Nodes can be deployed uniformly, for example, at the center of grid cells or randomly. Nodes move autonomously or passively due to environmental conditions, like wind or water flow. If nodes are static and not mobile, they preserve their initial position during the network lifetime. Network nodes can fail and stop operating. Our model neglects network failures to observe failure-free node activity patterns.

2.2. Simulation Environment

In our simulations, network nodes are static and uniformly deployed in pre-determined grid cells. We run our simulations in the ns2 simulator. The network load parameter depends on the number of sources and sinks. We run our simulations using a single source node and multiple sink nodes up to five. Our simulation and energy parameters are summarized in Table 1 and Table 2.

Table 1

Simulation Parameters

Parameter	Value
Number of nodes	100, 150
Number of sinks	1-5
Basic Routing Protocol	Gear
Deployment	Grid
Grid cell size	150 * 150
Channel bit rate	1.6 Mb/s

3. RESULTS

We run simulations on various sizes of networks using a single source node and multiple sink nodes up to five. Source, sink, and the nodes are actively communicating for data acquisition. Underlying routing protocols allow source and sink nodes to communicate through the shortest path between them.

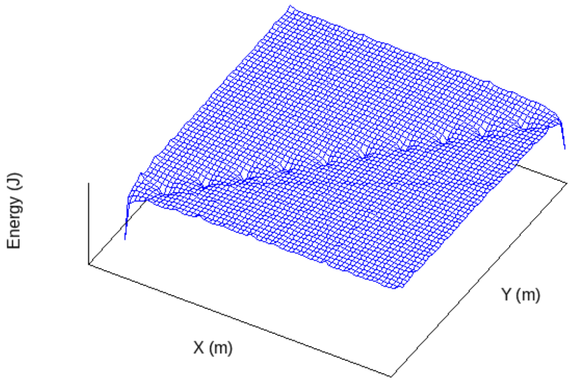


Figure 1. The remaining energy of network nodes in a network of 150 nodes

The source, sink, and relay nodes are called active nodes. An active node consumes more energy and has a high packet throughput than an inactive node. Energy consumption is one of the parameters of node activity. In these simulations, the sink node periodically receives data from the source node. After the sink node starts data requesting, active nodes continuously consume energy. In our simulations, we select the source and sink nodes from the diagonal vertices of the network. Figure 1 demonstrates the remaining energy of active nodes in a network of 150 nodes. In this figure, diagonal holes represent the location of active nodes. As shown in this figure, active nodes consume more energy than the rest of the network.

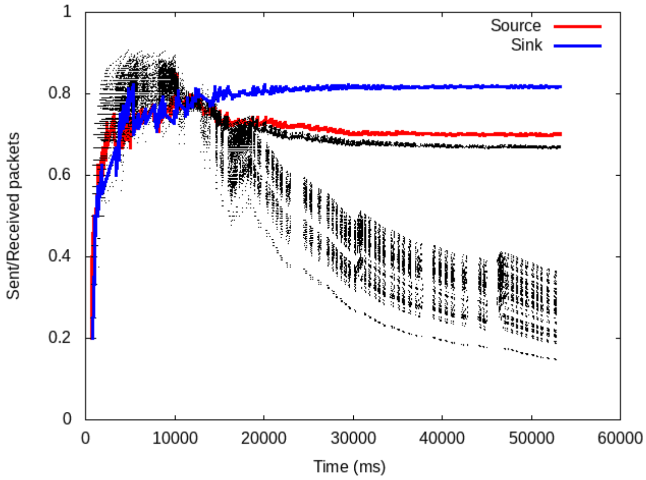


Figure 2. The ratio of sent packets to received packets by time on various types of nodes in a network of 100 nodes

The packet throughput parameter is another node activity parameter. Packet throughput is the ratio of the sent packets to the received packets on a node. An active node has a high packet throughput; it replies to the network and receives packets. Figure 2 represents the packet throughput of nodes by time in a network of a single sink node. Black data points represent network nodes other than the source and sink nodes. The black line under the source and sink node represents the packet throughput of the relay nodes on the data propagation path between the source and sink nodes. This figure shows that the source, sink, and relay nodes on the data propagation path are more frequently active than other nodes. And also, since the sink node has the highest packet throughput, the sink node is found to be more active than the source node and the rest of the network.

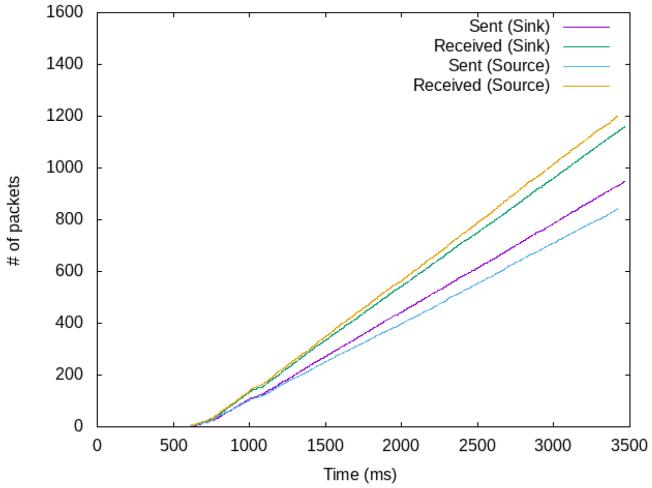


Figure 3. Number of sent and received packets by time on a source and sink node in a network of 100 nodes

Figure 3 represents the number of sent and received packets on the source and sink nodes. As the node activity increases, the angle between sent and received packet lines gets smaller. Since the sink is more active than the source, the angle between its lines is smaller.

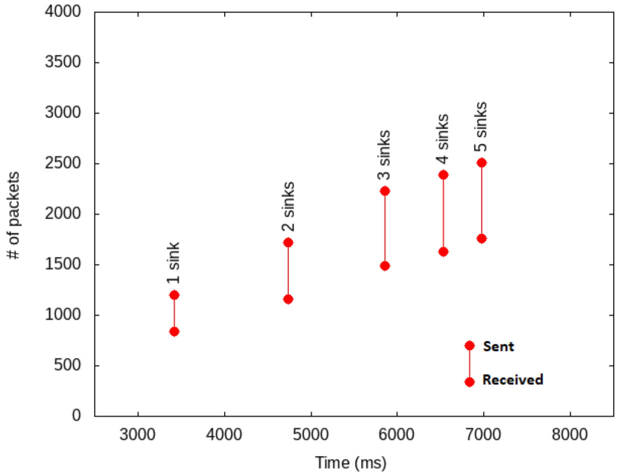


Figure 4. Total sent and received packets of the source node by number of sinks in a network of 100 nodes

We run simulation experiments with a single source node and various sinks. Since network load is the total sent and received packets on a node, sinks request more data from the source node as the number of sinks increases in the network. Figure 4 represents the total sent and received packets on the source node. As demonstrated in this figure, the total number of packets on the source node increases as the number of sinks increases in the network.

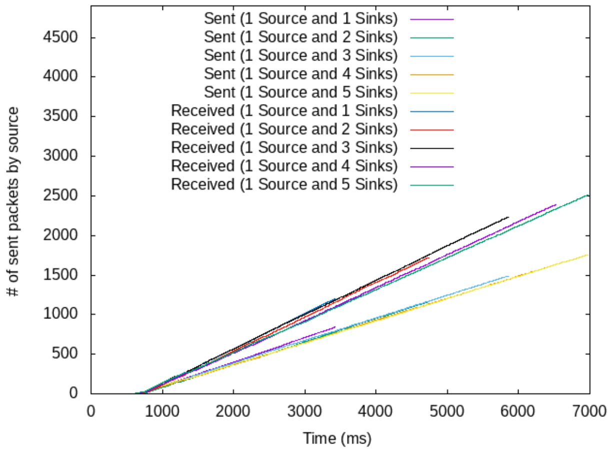


Figure 5. Number of sent and received packets by a source node in a network of 100 nodes and various numbers of sink nodes

Figure 5 demonstrates the number of received and sent packets on a source node by time. As shown in these figures, the source node accomplishes its task in a long time as the number of sinks increases in the network.

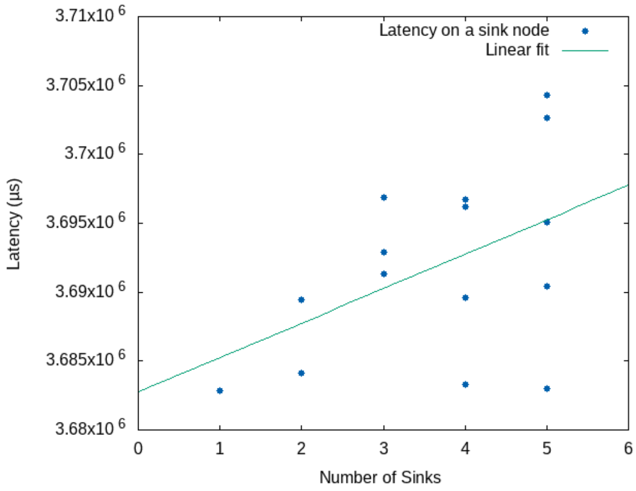


Figure 6. Latencies on sinks in a network of 100 nodes and a various number of sink nodes

Network latency on a sink node is the time difference between the first subscription and data reception. Figure 6 represents the network latencies on sink nodes as the number of sinks increases in the network. The linear fit line in this figure represents the behavior of network latency as the number of sinks increases. According to this line, the network latency on a sink node is prone to increase as the number of sinks in a network increases.

4. DISCUSSION AND CONCLUSION

In this paper, we observe the typical node activity behaviors according to the network load effects running simulations using a single source node and various sinks. Regarding energy consumption and packet throughput, we found that the sink, source, and relay nodes are more active than the rest of the network. We also found that the network latencies on the sink nodes are prone to increase as the number of sinks increases in a network.

Building a robust WSN system with fragile, failure-prone, and vulnerable sensor devices brings a new research area to detect damaged and malicious nodes. Observing node behaviors at heavy network loads is crucial to understanding typical node behavior. Having expected patterns of node behaviors under heavy network loads will help researchers understand the abnormal behaviors of damaged and malicious nodes and prevent them from operating in the network.

A significant amount of research on WSN addresses extending the network lifetime with energy-efficient and secure routing protocols. Most of these protocols detect malicious nodes by examining the abnormality on node behaviors. In this section, we briefly explain some these protocols and their security mechanisms.

The Secure Routing Protocol for Sensor Networks (SRPSN) protocol [4] is proposed for developing a secure and hierarchical routing structure. In this study, data transmission from the sensor node to the sink node is established with the group key management using a distributed group-key generating algorithm for secure communication. The proposed scheme also contains group communication policies for group membership requirements.

SS-LEACH protocol [5] addresses the shortcomings of the LEACH protocol. In SS-LEACH, selecting the dynamic stochastic cluster-heads helps increase the residual energy of nodes and network lifetime. Pre-distributed and self-localized keys establish security. This protocol presents techniques to prevent HELLO flood, Sybil, and selective forwarding attacks.

Energy-Efficient Cluster-Based Key Management (EECBKM) protocol [6] is proposed for secure cluster-based routing using a key management technique. There are pairwise keys for inter and intra-cluster communications. Packet delivery ratio rises by the key distribution through the cluster nodes. However, the complex environmental workload may increase the computational overhead and cause memory depletion.

Authentication key management (AKM) scheme [7] presents secure hierarchical routing in WSN. The proposed scheme uses two different keys; one is a pairwise shared key for cluster nodes, and the other is for network security. Periodical key distribution requires global and continuous authentication.

Aponte-Luis et al. [8] proposed a graphical user interface for remote power consumption configuration, data availability, authenticity, and confidentiality for real-time control and monitoring. The study enables the security configuration on both hardware and software layers.

Low-Energy Adaptive Clustering Hierarchy (LEACH) Protocol (SM-LEACH) [9] enhances Leach protocol with secure routing mechanisms. In this protocol, security is achieved by a hash algorithm, which helps to reduce the transmitted data over the network for conserving energy.

Abnormalities in the node activity patterns can signify the existence of faulty and malicious nodes in a WSN. Understanding the behaviors of faulty and malicious nodes relative to the typical node activities is left as a topic of future studies.

Conflict of Interest

The authors declared no conflict of interest.

Contribution of Researchers

Author1 coded simulation scenarios and plotted the collected data. Author2 browsed the literature and discussed the related studies.

References

1. Rashid, B. and M.H. Rehmani, *Applications of wireless sensor networks for urban areas: A survey*. Journal of network and computer applications, 2016. **60**: p. 192-219.
2. Zhang, X.L.a.P., *A Novel Load Balancing Strategy for Wireless Sensor Networks*. IEEE Communications Letters. **22**(1): p. 125-128.
3. Yu, Y., R. Govindan, and D. Estrin, *Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks*. 2001.
4. Tubaishat, M., et al., *A secure hierarchical model for sensor network*. ACM Sigmod Record, 2004. **33**(1): p. 7-13.
5. Wu, D., G. Hu, and G. Ni. *Research and improve on secure routing protocols in wireless sensor networks*. in *2008 4th IEEE International Conference on Circuits and Systems for Communications*. 2008. IEEE.
6. Lalitha, T. and R. Umarani, *Energy Efficient Cluster Based Key Management Technique For Wireless Sensor Networks*, in *India. InternationalJournal of Advances in Engineering & Technology*. 2012, Bharatiar University.
7. Gaber, T., et al., *Trust-based secure clustering in WSN-based intelligent transportation systems*. Computer Networks, 2018. **146**: p. 151-158.
8. Aponte-Luis, J., et al., *An efficient wireless sensor network for industrial monitoring and control*. Sensors, 2018. **18**(1): p. 182.
9. Priyadharshini, A.S. and C. Arvind. *Security-Based LEACH Protocol for Wireless Sensor Network*. in *International Conference on Innovative Computing and Communications*. 2021. Springer.