ENERGY UTILIZATION IMPACTS IN DETECTING ABNORMALITY ON WIRELESS SENSOR NETWORKS

Zuhal CAN [1*], Elif DEĞİRMENCİ [2]

[1] Eskişehir Osmangazi University, Faculty of Engineering and Architecture, Department of Computer Engineering, Eskişehir, Turkey, ORCID No : http://orcid.org/0000-0002-6801-1334

[2] Eskişehir Osmangazi University, Faculty of Engineering and Architecture, Department of Computer Engineering, Eskişehir, Turkey, ORCID No : http://orcid.org/0000-0001-8772-4543

Keywords

Wireless sensor networks, Energy utilization

Abstract

With the novel developments in Wireless Sensor Network (WSN) technologies, environmental data collection and processing services are applied in diverse industrial and scientific areas. However, energy limitations and vulnerabilities of WSN nodes are still the main drawbacks of technological developments in the area. Understanding the energy utilization patterns of nodes helps to detect abnormal node behaviors and prevent malicious nodes. In this study, we observe the energy utilization behaviors of nodes and found that nodes have distinctive activity patterns based on their types. We also found that source, sink, and relay nodes on the data propagation path have higher energy consumption patterns compared to other nodes.

KABLOSUZ SENSÖR AĞLARINDA ANORMALİTE TESPİT ETMEDE ENERJİ KULLANIMININ ETKİLERİ

Anahtar Kelimeler

Kablosuz sensör ağları, Enerji kullanımı, Ns2

Öz

Kablosuz Sensör Ağları (KSA'lar) teknolojilerindeki yeni gelişmelerle birlikte, çevresel veri toplama ve işleme hizmetleri, çeşitli endüstriyel ve bilimsel alanlarda uygulanabilir durumdadır. Bununla birlikte, KSA düğümlerinin enerji kısıtlamaları ve güvenlik açıkları hâlâ bu alandaki teknolojik gelişmelerin ana dezavantajlarındandır. Düğümlerin enerji kullanım biçimlerini anlamak, anormal düğüm davranışlarını tespit etmeye ve kötü niyetli düğümleri önlemeye yardımcı olur. Bu çalışmada, düğümlerin enerji tüketimi davranışlarını gözlemleyerek, düğümlerin türlerine özgü aktivite biçimleri olduğu sunucuna vardık. Bunun yanında, veri kaynağı, veri sorgulayıcısı ve *veri yayılma yolundaki iletici düğümlerin, diğer düğümlere kıyasla, daha yüksek enerji tüketimi biçimine sahip olduğu sonucuna varmış bulunuyoruz.*

Araştırma Makalesi		Research Article	
Başvuru Tarihi	: 28.01.2021	Submission Date	: 28.01.2021
Kabul Tarihi	: 16.12.2021	Accepted Date	: 16.12.2021

1. Introduction

Wireless Sensor Networks (WSNs) have applications in diverse areas such as military, underwater, underground and unattended terrestrial environments, where maintenance of network units is not always convenient and practical (Bayrakdar, 2019a, 2019b). WSN nodes are prone to failure due to their energy-limited and vulnerable structure. Although WSN has a failure-prone structure, WSN applications are developed to extend network lifetime as long as possible.

Energy efficiency and security techniques help to determine the network lifetime. The main metric that determines a network's lifetime is the energy utilization of network units (Bayrakdar, 2019c, 2019d, 2020). While an expected energy utilization pattern of nodes helps to determine network lifetime, abnormal activities like node failures or security attacks (Hari and Singh, 2016) can shorten the network lifetime, unpredictably. Early detection of abnormal activities helps to ameliorate the failure-prone and malicious network units' negative effects on the network lifetime.

* Corresponding Author; e-mail : zcan@ogu.edu.tr

In this paper, we observe the typical energy utilization patterns of network units in a simulation environment for differentiating between normal and abnormal activity patterns. In section 2, we provide a literature review on WSN security attacks. In Section 3.1, we describe our WSN model. In Section 3.2, we define our simulation parameters and simulation details. Our simulation results are explained in Section 4, and we discuss and conclude the paper in Section 5.

2. Scientific Literature Review

Routing protocols are developed while strengthening their security mechanisms. As listed in Table 1, many researchers have proposed hierarchical and tree-based routing solutions for Wireless Sensor Networks while integrating novel security solutions.

ORLEACH protocol (Sahraoui and Bouam, 2013) is proposed based on RLEACH protocol (Zhang, Wang and Wang, 2008) for intrusion detection systems. ORLEACH has several phases: Shared key discovery phase, Cluster setup phase, isolation of previously detected attackers, data transmission, intrusion detection and alerting phases.

Secure Cluster-Based Multipath Routing Protocol (SCMRP) (Kumar and Jena, 2010) proposes secure clustering routing and multipath routing algorithms. This protocol has five phases: to find the neighbors and set up the network topology, pairwise key distribution, cluster evolution, transmission of data, re-clustering, and re-routing. Each node shares the neighbor list with the base station. Each link has pairwise keys that are generated by a basestation. In this protocol, security is provided using cryptography techniques.

The secure hybrid routing protocol (SHRP) (Muthusenthil and Kim, 2017) combines the geographical and hierarchical schemes. The protocol developed a cluster head selection method based on central weight, residual-energy, and mobility factors. Security is developed considering confidentiality, integrity, and authenticity using the symmetric and asymmetric cryptosystem techniques.

In the Hierarchical Multipath Routing Protocol (HMR-WSN) (Jadidoleslamy, 2017), time division is ensured by the number of super-rounds. Each super-round has multiple time intervals. In all super-rounds, multiple Cluster-Heads (CHs) are selected at each time interval. Using different cluster-heads at different time intervals ensures security against selective forwarding and sinkhole attacks.

Secure and Low-energy Zone-based Routing Protocol (SeLeZoR) (Mehmood, Lloret and Sendra, 2016) is proposed for secure and energy-efficient hierarchical routing in WSN. In the proposed protocol, nodes are first separated into zones, and each zone is separated into clusters. Data is transmitted via nodes to cluster-heads, then each cluster head sends data to zone-head via a secret key. Each zone-head transmits data with a secure key management system to the base station. The zone technique increases the packet delivery ratio, ensures the data reliability, reduces the base station communication load, and controls the network communication.

In (Moulad, Belhadaoui and Rifi, 2017), a hierarchical hybrid intrusion detection mechanism is implemented utilizing cluster-based protocols in WSNs. In this study, the IDS system is combined with different techniques to overcome intrusion and malicious activities based on the classification of behaviors as normal and anomaly. With signature-based anomaly detection, attacks in previous malicious behavior patterns have been detected using a specification-based technique.

In (Brindha and Senthilkumar, 2019), security, network lifetime, and control overhead are improved using the Augmented Tree-Based Routing approach developed for multipath routing protocol problems. In this approach, the Lightweight encryption algorithm (LEA) and two-phase hybrid cryptography algorithm (THCA) are used for enhancing security.

Table 1

Literature review by network structure

Paper	Year	Network structure
ORLEACH	2013	Hierarchical
SCMRP	2010	Hierarchical
SHRP	2017	Hierarchical
HMR-WSN	2017	Hierarchical
SeLeZoR	2016	Hierarchical
Moulad et al.	2017	Hierarchical
Brindha et al.	2019	Tree-based

3. Method

3.1. System and Security Model

Research and publication ethics were followed in this study.

We use Gear protocol (Yu, Govindan and Estrin, 2001) as the data collection and routing protocol for our network analyzes. Gear protocol provides a data-centric and distributed routing mechanism. Using the Gear protocol, nodes communicate with their neighbor nodes for data transmission, and, do not resort to a central authority for having the network topology. At the beginning of the communication, nodes send and receive broadcast messages and built up their neighborhood information.

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	$freq$	$914 * 10^6$

Some of the network nodes are assigned as the source and sink nodes. Source nodes are responsible for event detection. Whenever they detect an event, they store and process event data. The source node can aggregate different types of event information. Sink nodes request data from the network by broadcasting a subscription message into the network. A source node that receives sink messages and has the related data, replies periodically to the sink node with the corresponding data information. Other nodes on the data propagation path, transmit messages between the source and sink nodes.

For our network models, to understand typical node activities, we assume that the network is failure-free. Network nodes are deployed in a flat network topology and do not have distinctive properties from each other. Nodes are static and preserve their initial position. They are initially and deterministically deployed on the deployment area.

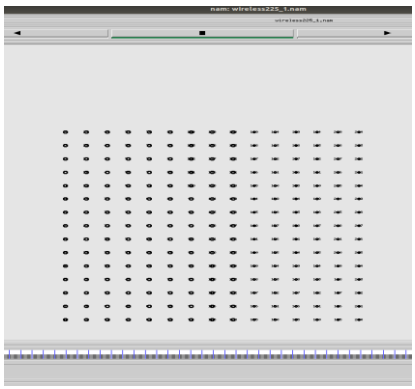

Figure 1. The network structure visualized by NAM tool

Table 2

Simulation Parameters

Parameter	Value
Number of nodes	25, 50, 100, 150, 200, 250
Network dimensions	4, 6, 9, 11, 13, 14
Number of sinks	1-5
Basic Routing Protocol	Gear
Deployment	Grid
Grid cell size	150 * 150
Interest packet length	36 bytes
Event packet length	50 bytes
Interest and event interval	5s and 50s
Channel bit rate	1.6 Mb/s

3.2. Simulation Environment

We run our simulations in the ns2 simulator. Figure 1 depicts the network structure of our simulations in ns2 environment regardless of the network size; network size changes in each simulation. This figure is captured by NAM which is a visualization tool for ns simulations.

In our simulations, any node in the network can be a sink or a source node. We selected sink and source nodes from the vertices of the network. Our energy consumption parameters are shown in Table 1. Our simulation parameters are listed in Table 2.

4. Results

We explain some of our findings regarding the network dimension. Network dimension is the total number of

hops between the furthest away nodes on a network. For example, on a network of 25 nodes, the network dimension is 4 hops.

In our simulations, source and sink nodes are selected from the diagonal vertices of the network. By the underlying routing protocol, data is transmitted through the nodes on the shortest path between source and sink nodes. We call nodes on the transmission path as data relay nodes.

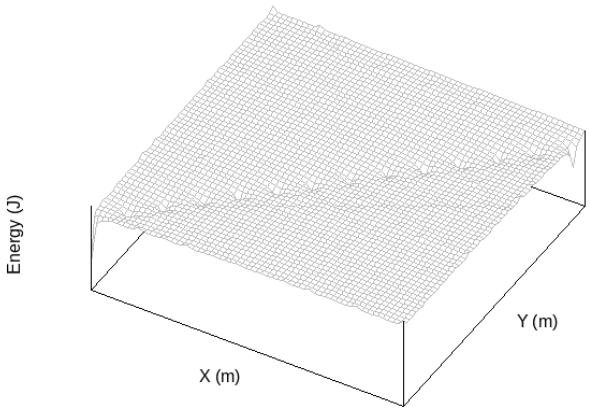

Figure 2. Remaining energy of network nodes in a network of 200 nodes

Figure 2 demonstrates the remaining energy of nodes. In this figure, as shown with the holes on the diagonal path, source, sink and relay nodes on the transmission path consume more energy comparing the rest of the network. We call these high energy-consuming nodes, source, sink, and data relay nodes on the transmission path between them, as active nodes. Active nodes' energies deplete faster than the rest of the network.

Figure 3 demonstrates the node activity frequency by time. For this simulation data is collected whenever nodes consume energy more than a threshold. In this simulation, a sink periodically receives data packets from the source node. As shown in this figure, the source node, the sink node, and the nodes on the transmission path between them are frequently active and continuously consume energy. We found that the sink node consumes more energy than the source node.

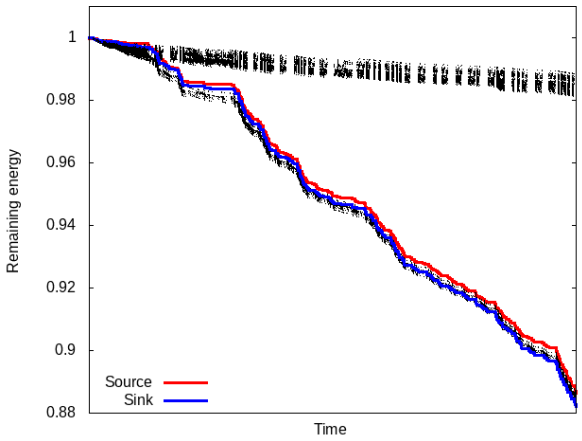

Figure 3. Remaining energy on various type of nodes in a network of 150 nodes. Black data points represent data of network nodes which are other than source and sink nodes

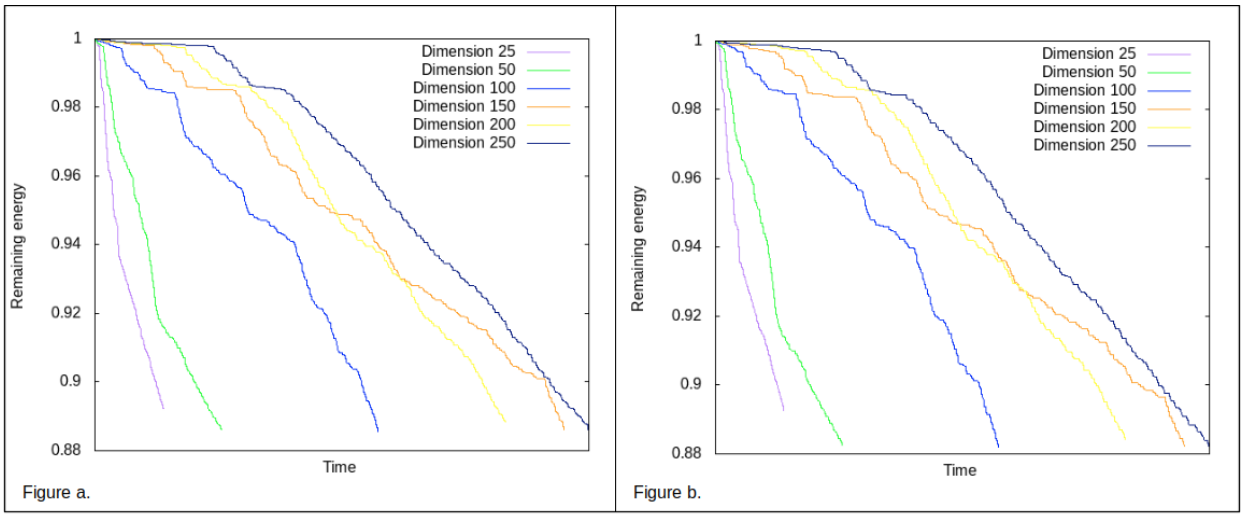

Figure 5. Number of received and sent packets by a source and sink node concerning network dimensions. a. Number of received packets by a source node. b. The number of sent packets from a sink node

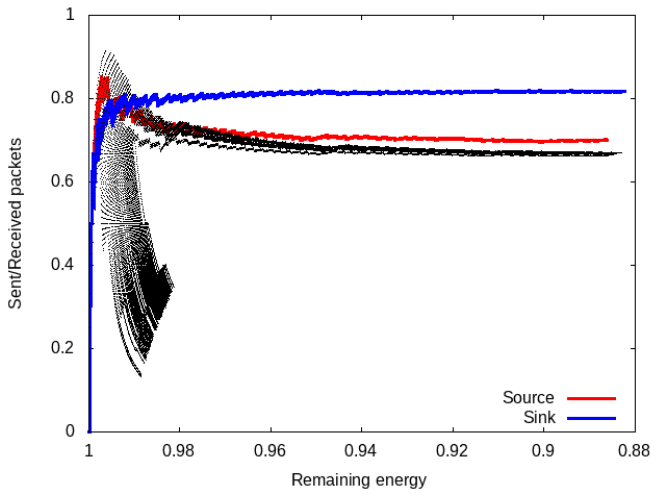

Figure 4. Ratio of sent packets to received packets by remaining energy on various type of nodes in a network of 150 nodes. Black data points represent data of network nodes which are other than source and sink nodes

Figure 4 represents the activity patterns of nodes by energy consumption. In this figure, the black line just below the source and sink data lines represent the energy consumption of data relay nodes on the data transmission path between source and sink nodes. As shown in this figure, inactive nodes consume a small portion of their energy, while active nodes consume a high amount of energy.

We evaluate the energy depletion behavior of source and sink nodes in a network in which a single source node and a single sink node exist. Figure 5.a and Figure 5.b represent the energy depletion behavior of the source node and sink node for various network sizes in terms of network dimensions. We found that the size of a network does not affect the amount of consumed energy at the source and the sink node. However, as the network dimension increases the source node and the sink node accomplish their tasks in a longer duration.

Figure 6 demonstrates the energy utilization of the source node as the number of sink nodes in a network increases. A single source node replies to all requests from all sink nodes. As the number of sink nodes increases, network load on a single source node increases, and consequently, causes a higher energy consumption at the source node.

5. Discussion and Conclusion

Energy utilization is an important parameter for understanding typical node behavior. Any abnormal energy utilization behavior in contrast to the typical energy utilization behaviors helps to detect abnormal nodes in a WSN. We found that different types of nodes have different activities, and, different behavior of energy utilization, in correspondence. Sink, source, and data relay nodes on the data transmission path have a high energy utilization behavior comparing to other nodes. A source node's energy consumption gets higher as the number of sink nodes in a network increases.

In this study, we only observe the energy utilization behaviors of the typical nodes, not of the abnormal nodes. We expect that a faulty or malicious node would give a warped result compared to typical node behavior results. The energy utilization behavior of abnormal nodes and their detections are left as future works.

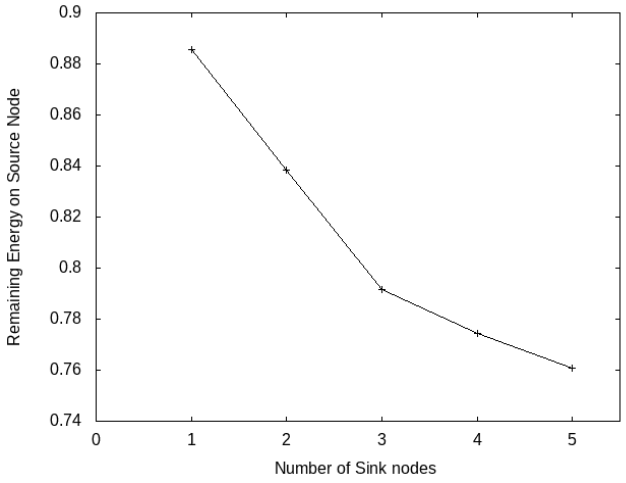

Figure 6. Remaining energy on source node by number of sink nodes in a network of 100 nodes

Conflict of Interest

No conflict of interest was declared by the authors.

References

Bayrakdar, M. E. (2019a). Kablosuz Yeraltı Algılayıcı Ağlar için Düğüm İletişiminde Derinlik Faktörünün Analizi, *Eskişehir Osmangazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 27 (2), 93-9.* https://doi.org/10.31796/ogummf.545943

Bayrakdar, M. E. (2019b). Kablosuz Algılayıcı Ağlarda En Az Sayıda Düğüm Kullanımı için Maliyet Etkin Algılayıcı Düğüm Yerleştirme Yaklaşımı, *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi, 6, 59-73.* https://doi.org/10.35193/bseufbd.566951

Bayrakdar, M. E. (2019c). Karasal algılayıcı ağlarda gözlemleme için enerji etkin TDMA erişim tekniği, *Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Dergisi,*

21 (2), 756-765. https://doi.org/10.25092/baunfbed.643924

Bayrakdar, M. E. (2019d). Yeraltı Algılayıcı Ağlarda Kayıpsız Veri İletimi için Sezme tabanlı Ortam Erişim Tekniğinin Başarım Analizi, *Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 12 (2), 1028-1035.* https://doi.org/10.18185/erzifbed.545497

Bayrakdar, M. E. (2020). Kablosuz Algılayıcı Ağlar için Gecikme Duyarlı CSMA Ortam Erişim Tekniğinin Performans Değerlendirmesi, *Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi, 12 (1), 227-235.* https://doi.org/10.29137/umagd.599000

Brindha, P., & Senthilkumar, A. (2019). Data dependability based bimodal encryption scheme for distributed routing in wireless sensor networks. *Peer-to-Peer Networking and Applications*, 1-10. https://doi.org/10.1007/s12083-019-00813-4

Hari, P. B., & Singh, S. N. (2016, April). Security issues in Wireless Sensor Networks: Current research and challenges. In 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring) (pp. 1-6). IEEE. https://doi.org/10.1109/ICACCA.2016.7578876

Jadidoleslamy, H. (2017). A hierarchical multipath routing protocol in clustered wireless sensor networks. *Wireless Personal Communications*, *96*(3), 4217-4236. https://doi.org/10.1007/s11277-017-4382-1

Kumar, S., & Jena, S. (2010, December). SCMRP: Secure cluster based multipath routing protocol for wireless sensor networks. In *2010 Sixth International conference on Wireless Communication and Sensor Networks* (pp. 1-6). IEEE. https://doi.org/10.1109/WCSN.2010.5712294

Mehmood, A., Lloret, J., & Sendra, S. (2016). A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring. *Wireless Communications and Mobile Computing*, *16*(17), 2869-2883. https://doi.org/10.1002/wcm.273

Moulad, L., Belhadaoui, H., & Rifi, M. (2017). Implementation of a hierarchical hybrid intrusion detection mechanism in wireless sensors network. *Int. J. Adv. Comput. Sci. Appl.*, *8*(10), 270-278. https://doi.org/10.14569/IJACSA.2017.081035

Muthusenthil, B., & Kim, H. (2017). SHRP-Secure Hybrid Routing Protocol over Hierarchical Wireless Sensor Networks. *International Journal of Computers Communications & Control*, *12*(6), 854-870. https://doi.org/10.15837/ijccc.2017.6.2909

Sahraoui, S., & Bouam, S. (2013). Secure routing optimization in hierarchical cluster-based wireless sensor networks. *International Journal of Communication Networks and Information Security*, *5*(3), 178. https://www.proquest.com/docview/1511428760

Yu, Y., Govindan, R., & Estrin, D. (2001). Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. *Technical report ucla/csd-tr-01-0023, UCLA Computer Science Department. http://www.ics.uci.edu/~dsm/ics280sensor/readings/networks/Estrin_geo-routing01.pdf*

Zhang, K., Wang, C., & Wang, C. (2008, October). A secure routing protocol for cluster-based wireless sensor networks using group key management*. In 2008 4th international conference on wireless communications, networking and mobile computing (pp. 1-5). IEEE. https://doi.org/10.1109/WiCom.2008.889*