International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 2 December 2020

Wireless Sensor Networks Using Meta-Heuristic Algorithms for DoS Attacks

Muhammad Ropianto
Universitas Ibnu Sina, Indonesia
ropianto@uis.ac.id

Abstract: In the processing and transmitting of data via wireless networks, wireless sensor networks (WSNs) are being commonly used. Similar to its minimal cost and fast connectivity, this form of network is currently used in several systems for surveillance operations in various domains. In these networks, the nodes use a finite source of energy which, as it is sustainable, concludes the life of the network after its degradation. They are vulnerable to various threats referring to the vulnerabilities in the sensor network. Denial of Service (DoS) is another important attack threatening WSN. DoS attacks show the lack of energy in these sensors by stopping the nodes from entering into idle mode and conserving energy. The Abnormal Sensor Identification Accuracy technique is used in this paper to prevent DoS attacks to minimize the amount of energy consumed. A new and unique lift-set algorithm is based on the Imperialist Competitive Algorithm (ICA) is proposed in this article. The proposed algorithm that uses the ICA specifies the nodes of the sensor that must be chosen in various live sets. The live sets are developed to detect all applied goals as the algorithm efficiently wants to continue. Several evaluations have been performed to test the efficiency of the proposed algorithm and the results achieved show that the proposed methodology performs better than alternative algorithms to expand the lifespan of the network.

Keywords: Wireless Sensor Networks; Meta Heuristics - Imperialist Competitive Algorithm; Denial of Services (DoS); Sensor Detection

I. INTRODUCTION

Multi-sensor networks allow new functionalities spanning a broad variety of fields [1]. It is well defined, therefore, that networks built from a variety of sensors are vulnerable to the influences which affect their security [2]. In wireless sensor networks (WSNs), security is a major research area. The extensive use of WSNs in security-sensitive settings, like the military climate, has made safety concerns a fundamental necessity. As nodes in the network are the routing process, the network is eliminated by attacking the nodes. Because routing is a trust-based function between the nodes, there is a fair possibility for attackers to interrupt the routing protocol. Some tasks including Wireless Sensor Networks (WSNs) [3]. A sensor network is made up of several smaller nodes, and in multiple protocols, energy efficiency has some of the most important problems. The key disadvantage of these sensor nodes is their battery life, where it restricts the lifespan of the network. Thus, in developing network protocols, energy conservation is such a method to expand the life of the network.

For WSNs included in environmental control and security uses, the scope issue is a basic one. According to the multitude of sensors and implementations, the scope definition is open to a broad variety of viewpoints. Criteria were considered to have a significant impact on the efficiency of the network and could be regarded as a metric of service quality in WSNs [4]. This network is commonly established without planning and design and is used for a limited period; thus, security principles are set out independently on these networks. As such, security measures to defend the WSN from security breaches ought to be introduced. In-network sensors, Denial of Service (DoS) attack [5] are the most common modes of attack. To exhaust its battery, DoS prevents the radio from going into idle mode. The energy efficiency ratio of monitors consumes their batteries in decades under usual system parameters, while denial of service attack consumes them within a few days by maintaining the radio signal unit on the sensor network [6].

Users concentrate on measuring goals with a WSN in this article. The scheduling of sensor nodes into subgroups becomes one of the most effective methods for minimizing energy usage in sensor networks and that

much lifespan so each one reaches all targets in the network implemented. Then, to track dispersed goals, each subset should be involved in various periods. As such, all other subsections may turn to modes of low energy consumption to conserve their energy for their periods.

There are generally two strategies for separating sensor nodes into subsets called the disconnected set cover and the maximum set layer. Each node in the subsystem could only be enabled for that round in the disjointed decision reached, which absorbs the entire energy during the activated period. But, in a full set loses its capacity, each node may be activated more than once in separate subsets. For various implementations, the requirements to take are wide. Based on the problem's expectations and goals, there could be several other limitations. For instance, it would be important for the sensor nodes in each sensor support to just be able to establish a network linked to the sink.

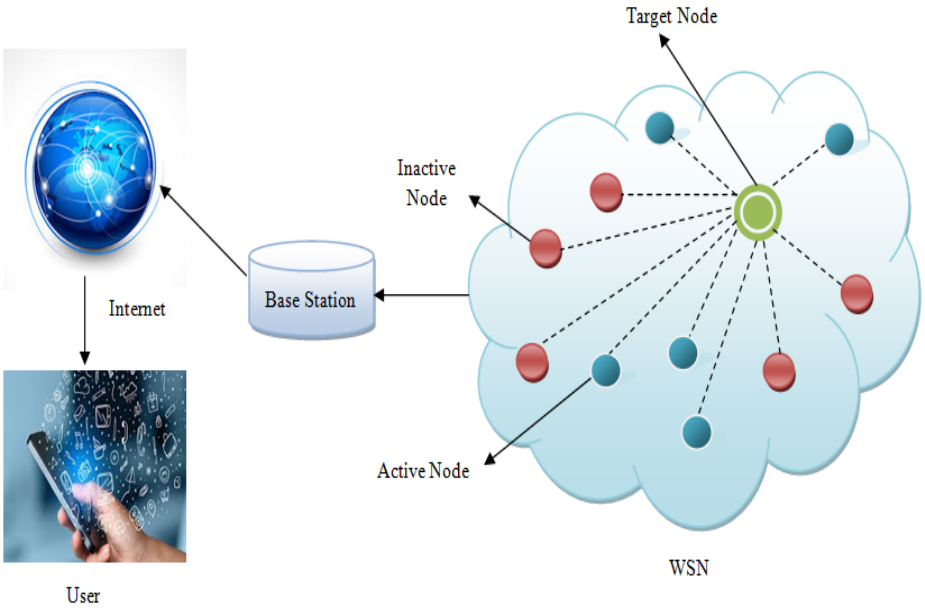

Figure 1. Denial of Service (DoS) on Wireless Sensor Networks

If synchronization is not regarded as a limitation, the lifetime maximization task is significantly minimized. One circumstance for not recognizing synchronization between nodes maybe like this. The sensor field is far away from others, and an automobile passes over the sensor field while the sink gathers data from the sensors. Both effective nodes transmit data to the sink, their sensor nodes, and use about the same energy required to transmit the information. In this case, the model for energy consumption is easy to understand. Both active sensor networks receive the same amount of energy per unit of time; no energy is taken by every sensor node. This lifetime maximization challenge, besides that, can be as difficult as an NP-complete challenge, based on the specific requirement. A multi-phase optimization algorithm ASDA-RSA is proposed in this article, as follows: 1) splitting the network into clusters. Using an energy-based approach, this stage is carried out to identify the suitable cluster head, to enhance the network and minimize energy usage. 2) To avoid a DoS attack, use the ICA algorithm and interconnected protocol, including an authenticated user. An illustration of DoS attacks on WSNs is seen in Figure 1.

The article discussed here is listed as follows. Section 2 outlines the relevant work on methods that protect the device against the assault of Denial of Service. The specifications of our proposed ASDA-ICA system are presented in section 3. Also, the criteria used for performance assessment are explored and the effects of the simulation are described in Section 4. Finally, the article concludes in Section 5.

II. RELATED WORKS

Different kinds of security metrics have been introduced and used in different researches to overcome Denial of Service attacks and efficient WSNs from DoS attacks. This is not a recent issue and has been thoroughly

discussed before. To function with such threats, there are different methods suggested by researchers.

In [7], the frameworks known in the WSN Windows platform are analyzed, serving as defensive measures against attacks targeting MAC layers in WSNs. A stable hybrid MAC framework named 'Green and Secure Hybrid Medium Access Control' is thus proposed here to reduce the impact on WSN Microsoft windows of such threats. Examples of functionality offered within this framework are Threshold-based MAC mode conflict protection and detection systems on WSN Microsoft windows with the aid of specific MAC frameworks. In, [8], an IDS model is assumed to be extended to the sense of wireless sensor networks via the perfection of the human immune system. In this algorithm, a modified decentralized and modified variant of the Dendritic Cell technique is used to get the functionality for nodes, like neighborhood surveillance and coordination in detecting attackers. Also, the findings are associated with a Negative Selection Model application to show the performance concerning denial-of-service attack detection and also energy consumption.

In [9], two primary proposals are given. Initially, the new methods of protection for denial of service attacks in ContikiMAC, because of CSL's dominance over ContikiMAC, are suited to CSL. Next, for the province-of-the-art security features against denial-of-service, some safety upgrades are recommended. Zhu et al.[10] given a strong research study on different wireless sensor network coverage and communication problems. In WSN, this issue could be divided into three primary types: aim coverage, field coverage, and barrier coverage. Next, the issue of point coverage is to measure a series of network goals implemented. Targets are static or defined each. Secondly, the purpose of area coverage is to track the type of network implemented. Mostafaei et al.[11, 12] suggested a method focused on learning automata to extend the existence of the network of wireless sensor networks so each node in the network is fitted with learning automata and allows nodes to choose an active or sleeping mode. Third, the subject of firewall protection is to classify breached pathways by intruders.

A learning automaton-based approach was proposed in [13] for energy-efficient control of thresholds in WSNs. In [14], the authors constructed a low-cost protective sensor in sensor nodes. They presented a distributed algorithm to address the issue of minimum-cost firewall protection in asynchronous wireless sensor networks. A distributed methodology based on learning computations about the issue of stochastic firewall protection is suggested in [15]. In WSN, the purpose of dynamic object detection is to identify such loading reference points in the network region to use as many sensor nodes in the network. Another best way to solve this issue is to schedule the sensor network so that a node is only enabled when the target point is in its sensing area. The authors suggested a scheduling scheme based on a learning algorithm in [16] to resolve the question of complex point range. To provide the right nodes to cover complex goals, they used learning automatons. Each device in the network is fitted with a series of learning machines in their suggested algorithm.

The learning automata existing in each node aim to decide the time limit of work for the node in such a sense that the node's target point detection rate could not significantly degrade. The authors found the issue of specific units in [17] and suggested a sub-set-based approach to separate sensor nodes into separate cover sets, as each support system should protect all network goals. Enhancing the number of cover sets is the goal of their strategy. Authors in [18] suggested an algorithm focused on learning automata to achieve maximal disjointed set coverage. To make a great position of each node at every specified period in the network, they included learning things automatons.

To solve the maximum lifespan problem in WSNs, Mostafaei, et al.[19] invented a learning automatic algorithm. To schedule sensor nodes into separate cover sets and extend network lifespan, they used the characteristics of learning automata. A novel and successful coverage algorithm were built in [20] by the authors that can generate all types of disjoint cover sets, i.e. covers sets without typical sensor nodes as well as non-disjoint cover sets. An Improved Particle Swarm Optimization strategy for the identification of sinkhole attacks in WSN was proposed by the author Keerthana and Padmavathi [21]. The suggested algorithm is given the optimum packet distribution ratio, message drop, average message drop, false alarm incidence relative to the current ACO and PSO algorithms.

In [22], a two-phase scheme is suggested in the MANET, DAWA, to detect wormhole attacks and secure them. There are two steps in the proposed technique. Initially, by fuzzy logic, the strong and successful routes are chosen in the system; then, in the selected routes, the artificial immune system is used to classify the effectively

immune path. In this article, the design of wormhole tunnels using the out-of-band high-power channels help in the detection of successful wormhole attacks. There is, however, a condition major consideration in this current paper that they should not receive any packets while the destination nodes are hit by wormhole attacks, which is necessarily not accurate. In an unsecured wireless sensor network containing multiple static source nodes and a mobile sink in the presence of adversaries, [23] authors presented the issue of safe data transfer and controlled energy consumption. The proposed framework consists of three phases: data collection point detection, mobile sink route preparation, and safe data transfer.

For defining data gathering features for data transfer to the mobile sink, an energy-aware edge detection optimization is used. Data is effectively distributed for access control through the ElGamal system based on cryptographic encryption. There is a unique identifier connected to a mobile node. Wireless sensor networks as being part of the Internet of Things framework consists of resource-constrained detectors that are commonly battery-powered. Thus, when operating with these instruments, careful energy control is important. The lack of security protection, though, may make space for energy-drain threats like denial-of-service attacks, that have a greater detrimental effect on the sensor's life cycle than the existence of security mechanisms. By detecting several Media Access Control (MAC) protocols-Sensor-MAC, Timeout-MAC, and Tunable MAC-under various network sizes [24], this article concentrates on denial-of-service attacks. For all of these protocols, it tests, assesses, and interprets the signal intensity obtained and the relation quality metrics.

III. PROPOSED WORK

It explains our suggested approach based on ICA in this module to overcome the maximum set cover issue in wireless sensor networks. Initially, all sensor nodes in the network are believed to be the same, and every network may have different types of nodes, such as the active node and the idle mode. These aim to find the right active nodes in the network region to track the targets implemented. Active and inactive structures in the proposed algorithm are allocated to nodes depending on the ICA framework. It also assumes that there is a random deployment of all sensor nodes and goals and that each node does have the same frequency bandwidth.

This article analyzes the following issues to specify the set cover issue in WSNs. The sensor system consists of a series of fixed-location strategies to be continually tracked, a range of sensor nodes distributed at once, and a sensor node. It recognizes the issue of maximum set cover in which dispersed nodes in networks are separated into subsets called set covers. The designed set covers would not need to be disjointed by either solution. It suggests that there should be more than one fixed cover for every node in the network. It suggests that in the active phase, all nodes in the network have the same amount of actual energy and would have the same effect on energy utilization. If it is enabled, all the time, the lifespan of a sensor node is considered as a single specific time. Both sensor nodes in the network are often believed to have the same sensor range and could differentiate between effective and sleep modes. It also finds that the effect of sensor networks installed in the controlled region is higher than that needed for target information monitoring. To conserve their energy and maximize the network lifespan, who want to prepare the operation state of the sink node.

The major issue is how to organize sensors into multiple cover sets so that all goals can be monitored by every cover sequence and thus maximize the life of the sensor. Developing the sensors in this article is referring to identifying the feature of the sensing devices both as offensive or defensive.

Imperialist Competitive Approach (ICA)

Over the past three decades, meta-heuristic algorithms have been one of the most important functions for finding solutions to evolutionary computation. These techniques, like memetic algorithm, virtual annealing, optimization of particle swarm, and optimization of an ant colony, are being effectively implemented to several complicated optimization issues, namely TSP, issue of route optimization, issue of quadratic selection, issue of task scheduling, etc. A few of the meta-heuristic algorithms that scientists and experts had also made a significant impact commonly is the ICA. The author Atashpaz Gargari integrated the ICA solution that combines human socio-political development as a theoretical base for the development of a strong technique for optimization [25]. This classifier sees globalism as a stage of human technological development and uses it as a method for holding an integrated by numerically modeling this complex political and historical system. The ICA is a new analytical tool used in diverse fields of computer science

technology, communication systems, etc. to address objective functions.

It begins with an initial sample taken the state, as with evolutionary computation, and is separated into different forms of colonies and imperialists that also create economies. In this technique, imperialistic existing firms between these societies types. Great powers with attractive bonds disintegrate in this conflict and dominant entities take control of their dependencies. Imperialist competition corresponds to a system in which only imperialism remains, and settlements have the same importance as the imperialist for objective functions. Every state supports a sensor network in the suggested solution. Our ICA community coverage approach consists of two phases: a scheduling system and a system of internal control of every sensor network interface.

The first aspect is the strategy for scheduling which aims to schedule nodes into cover sets. In the scheduling strategy, any fort's domain attempts to schedule nodes in the best offensive range of least duplication of protected targets from each sensor network, depending on the covered target details of each node. In various cover sets, the following sections present the monitoring plan for each node. Active imperialism nodes execute aim supervising activities in this strategy, and other nodes migrate to service mode to conserve resources. The initial set of states is computed separately in the ICA method. Each state is specified as a 1 x j set where j represents the size of goals for the network. Points in-nation are the goals protected by this node. In this case, for analyzing the goals, continuous-loop networks are assumed and A1, A2, and A3 are tested to track the attacks B1 to B9. The cost of each state is measured in Equation (1) by the activity objective functions.

$$F_c = M_c \tag{1}$$

The relatively low computation time of a state, as per the objective functions, thus the valid the system, it defines for handling the scheduling issue would be. Several states are developed in the early stage, and a proportion of the newest members of this community are chosen as imperialist powers. The rest of the states of the Ncol are territories, most belonging to a state. In the ratio of the strength of the imperialists, the colonies are distributed among the imperialists. The normalized impact (m_x), of imperialist 'X', is measured to do everything based on an analysis of all imperialists by Eq. (2):

$$M_c = \max(m_x) - m_c \tag{2}$$

Where the value of the c[th] imperialist is m_c, and its computed price is M_c. The colonies, depending on their Euclidean, are transmitted by many imperialists. So every imperialist's computed authority is defined by:

$$E_n = \left| \frac{M_c}{\prod_{x=1}^{X_c} m_x} \right| \tag{3}$$

Then the sum of a ruler's dependency would be,

$$CM_c = \max(E_n . C_s) \tag{4}$$

Where max is a feature that generates a numerical rounded to the nearest digit. The basic number of particles is chosen arbitrarily of every imperialist. The imperialistic conflict starts, considering the original condition of the imperialists. The mechanism of selection proceeds until the preventing criteria are fulfilled. Significantly, its most effective imperialists would get more states in the separation of provinces. All rulers are competing in the ICA method to capture more provinces and add to their latest provinces. Imperialist innovation is slowly causing the power of poorer nations to reduce and the power of the biggest states to raise. This imperialist challenge is modeled as follows; the least effective group of the lowest republic is distributed from its latest imperialist province and gets ready for either empire to exhibit it. Thus, every ruler would also provide a probability of getting control of the liberated province predicated on their power factor during the different competitive processes, i.e. rulers with more power factor will become more likely to recognize it.

As suggested previously, in an imperialist contest, every army that refuses to make it stronger is minimized. This reduction happens incrementally. Over time, ineffectual rulers are losing their provinces, and more powerful rulers are beginning the process of those provinces and increasing their authority. Some or all of the most important provinces of a ruler are chosen at each step of the analysis, and competition among all rulers for control of these provinces exists.

Achievement of these provinces will not generally have some of the most powerful rulers, but there are greater opportunities for more different rulers to take control. Each empire's normalized actual cost $J \cdot R \cdot M_x$ can be evaluated as per equation to framework the competition between empires for the defense of these provinces. (5),

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 2 December 2020

based on the average cost of the rulers, R · M_x, and equation (6), based on the average cost of the rulers, R · M_x, and

$$J \cdot R \cdot M_x = max_j\ (T \,.\, M_y) - R \cdot M_x \quad (5)$$

Rulers with considerably lower expenditures would have significantly better-normalized expenses. The risk Q_{q^x}, of every ruler, properly disposing of during the conflict for provinces is then determined by Equation (6)

$$Q_{q^x} = \left| \frac{J \cdot R \cdot M_x}{\prod_{x=1}^{X_c} J \cdot R \cdot M_y} \right| \quad (6)$$

$$Q = [Q_{q^1}, Q_{q^2}, Q_{q^3}, \ldots, Q_{q^{X_c}}] \quad (7)$$

Then a function G of a certain scale as Q is generated and its components are spread equally over different characters:

$$G = [g_1, g_2, g_3, \ldots, g_{M_x}] \quad (8)$$

$$g_1, g_2, g_3, \ldots, g_{M_x} \in V\ (0, 1) \quad (9)$$

Instead, by only deducting G from Q, a function F is generated:

$$F = Q - G = [F_1, F_2, F_3, \ldots, F_{M_x}] = [Q_{q^1} - g_1, Q_{q^2} - g_2, Q_{q^3} - g_3, \ldots, Q_{q^{X_c}} - g_{M_x}] \quad (10)$$

Each optical remote sensing lifespan would be accessed during specified data collection. The concentration of every specific evaluation phase is greater than unity, which demonstrates that all specified systems produce an upper bound of their power consumption on every process. Once the detector has completed its moment, it is excluded from the improved product schedule series.

IV. PERFORMANCE EVALUATION

In this section, in comparing the results to the efficiency of related previous techniques, this performs a set of computations to assess the results of the proposed predictive control scheduling approach, known as the great proposed scheduling framework. A specified detection system is predicted in these computations, in which those sensor networks are individually distributed across a two-dimensional interval of 5 m x 5 m. Within this province, a percentage of specified objectives are often integrated spontaneously. It is predicted that the sensing distances of all sensor networks are equivalent. The following major experimental variables are identified to measure the effectiveness of the new scheduling technique. The sensor variable range is used to examine whether the proposed system satisfies the DSC major issue. In various forms of where the performance of the system is increased with the varying weights of goals and sensors, then evaluate the results of the ICA based system.

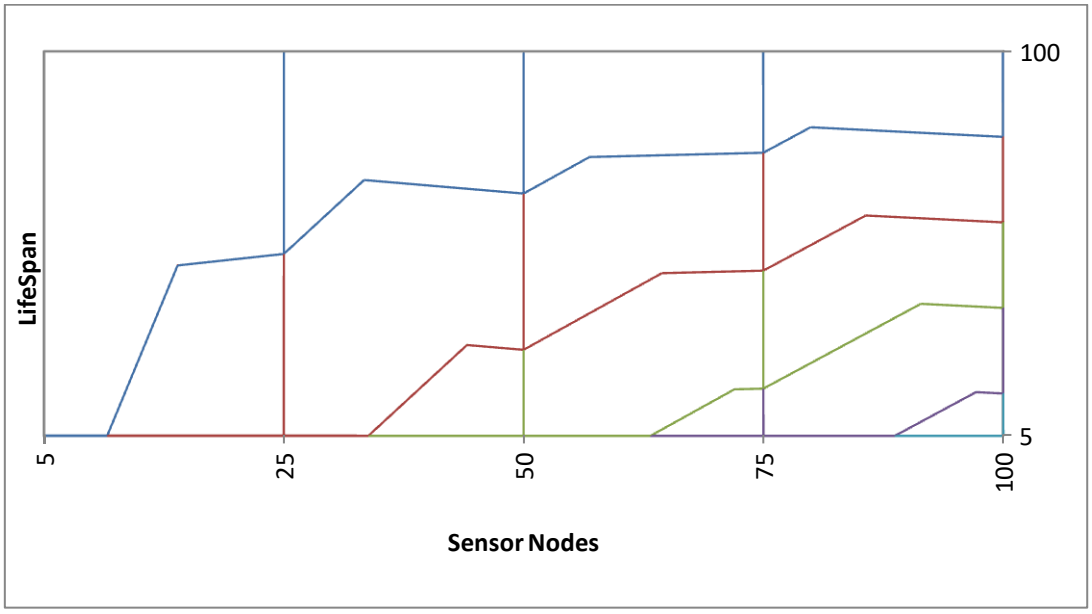

Figure 2. Comparison of network lifespans by different sensors

The sensing frequency feature is used to examine the effectiveness of the proposed system in addition to the following sensing frequencies of the sensor nodes. In ratio, the specified access of detection is based as it enhances the frequency bandwidth. To determine the optimal cover series, it is crucial to analyze the results of the selection of sensors with different detecting parameters of different optical sensing limits. This feature is used to analyze the efficiency of the proposed system with the availability of the number of sensor nodes across various activation frequencies and to evaluate how the varied impacts the efficiency of the different systems.

The result of the sensor nodes on the network lifespan of the suggested scheduling technique framework is seen in Figure 2. From this statistic, it has been shown that the lifespan of the network for 5 goals is greater than for 25 objectives. Since goals, implement a random homogenous density, the lifespan is proportional to the set of input data in this method. Increasing the number of goals significantly extends the lifespan of the network. In this figure, another output is provided. The extended lifespan is obtained proportionally higher as it expands the frequency bandwidth. It must be remembered that the increase in the proportion of nodes in the sensor will correspond to further cover sets being identified.

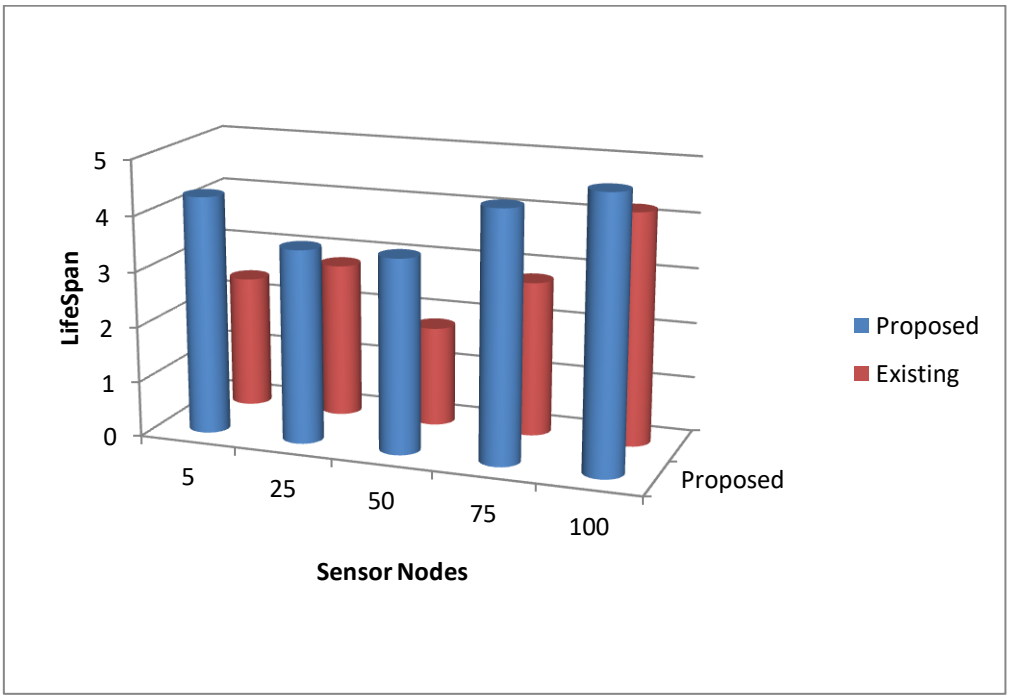

Figure 3. Comparative analysis of network lifespan as the sensor nodes for large network transformations.

In the proposed scheduling approach of various activation frequencies, it may fix the sensor nodes to 50 to analyze the impact of the sensor field of nodes on the network's lifespan. The findings obtained from this experiment are demonstrated in Figure 3. As could be shown, when the suggested scheduling technique is used than about the heuristic Greedy-DSC system or learning adaptive discontinuous set protect in [18] and [26], the network lifespan is greater. It does have the same results in [20], where finding protects collections in the network is an almost optimal process. Because the state of every state aims to determine the right network devices in our ICA-based approach to maintain goals and bring redundant networks in a high sampling state before the next stages are chosen. This result also indicates that in aspects of maintaining the network lifespan, our suggested methodology exceeds the existing algorithm [26].

V. CONCLUSION

In this article, with the main objective of expanding the network lifespan, the specified protection issue in wireless sensor networks was explored. In the WSNs, we suggested an ICA-based technique for solving the issue. In the proposed technique, with the aid of ICA, connected devices are separated into subsections. Imperialist nodes in the risk-weighted are attempting to help their provinces plan their optimal position in our experiments at any particular time. Some many modeling studies were performed to explore the effectiveness of the proposed

framework in addition to expanding the network lifespan. The simulation results indicate that, because of the frequency of the sensor nodes, the quantity of sensor nodes, and the sensing frequency of the sensor nodes, the proposed approach outperforms equivalent current approaches in terms of network lifespan.

REFERENCES

[1] Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using the RSA cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, *33*(4), e4234.

[2] Juneja, V., & Gupta, D. V. (2018, August). Security against vampire attack in ADHOC wireless sensor network: detection and prevention techniques. In *International Conference on Wireless Intelligent and Distributed Environment for Communication* (pp. 25-38). Springer, Cham.

[3] Mostafaei, H., & Shojafar, M. (2015). A new meta-heuristic algorithm for maximizing the lifetime of wireless sensor networks. *Wireless Personal Communications*, *82*(2), 723-742.

[4] Slijepcevic, S., & Potkonjak, M. (2001, June). Power efficient organization of wireless sensor networks. In *ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No. 01CH37240)* (Vol. 2, pp. 472-476). IEEE.

[5] Behzad, S., Fotohi, R., & Dadgar, F. (2015). Defense against the attacks of the black hole, gray hole and wormhole in MANETs based on RTT and PFT. *International Journal of Computer Science and Network Solutions (IJCSNS)*, *3*(3), 89-103.

[6] Zhang, D., Ge, H., Zhang, T., Cui, Y. Y., Liu, X., & Mao, G. (2018). New multi-hop clustering algorithm for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *20*(4), 1517-1530.

[7] Pawar, P. M., Nielsen, R. H., Prasad, N. R., & Prasad, R. (2018). GSHMAC: Green and Secure Hybrid Medium Access Control for Wireless Sensor Network. *Wireless Personal Communications*, *100*(2), 267-281.

[8] Salmon, H. M., De Farias, C. M., Loureiro, P., Pirmez, L., Rossetto, S., Rodrigues, P. H. D. A., ... & da Costa Carmo, L. F. R. (2013). Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques. *International journal of wireless information networks*, *20*(1), 39-66.

[9] Krentz, K. F., & Meinel, C. (2019). Denial-of-sleep defenses for IEEE 802.15. 4 coordinated sampled listening (CSL). *Computer Networks*, *148*, 60-71.

[10] Zhu, C., Zheng, C., Shu, L., & Han, G. (2012). A survey on coverage and connectivity issues in wireless sensor networks. *Journal of Network and Computer Applications*, *35*(2), 619-632.

[11] Mostafaei, H., Meybodi, M. R., & Esnaashari, M. (2010). A learning automata based area coverage algorithm for wireless sensor networks. *Journal of electronic science and technology*, *8*(3), 200-205.

[12] Mostafaei, H., Meybodi, M. R., & Esnaashari, M. (2010, February). EEMLA: Energy efficient monitoring of wireless sensor network with learning automata. In *2010 International Conference on Signal Acquisition and Processing* (pp. 107-111). IEEE.

[13] Mostafaei, H., & Meybodi, M. R. (2014). An energy efficient barrier coverage algorithm for wireless sensor networks. *Wireless personal communications*, *77*(3), 2099-2115.

[14] Gu, Y., Zhao, B. H., Ji, Y. S., & Li, J. (2011). Theoretical treatment of target coverage in wireless sensor networks. *Journal of Computer Science and Technology*, *26*(1), 117-129.

[15] Mostafaei, H. (2015). Stochastic barrier coverage in wireless sensor networks based on distributed learning automata. *Computer Communications*, *55*, 51-61.

[16] Esnaashari, M., & Meybodi, M. R. (2010). A learning automata based scheduling solution to the dynamic point coverage problem in wireless

sensor networks. *Computer Networks*, *54*(14), 2410-2438.

[17] Cardei, M., & Du, D. Z. (2005). Improving wireless sensor network lifetime through power aware organization. *Wireless networks*, *11*(3), 333-340.

[18] Mostafaei, H., & Meybodi, M. R. (2013). Maximizing lifetime of target coverage in wireless sensor networks using learning automata. *Wireless Personal Communications*, *71*(2), 1461-1477.

[19] Mostafaei, H., Esnaashari, M., & Meybodi, M. R. (2014). A coverage monitoring algorithm based on learning automata for wireless sensor networks. *arXiv preprint arXiv:1409.1515*.

[20] Zorbas, D., Glynos, D., Kotzanikolaou, P., & Douligeris, C. (2010). Solving coverage problems in wireless sensor networks using cover sets. *Ad Hoc Networks*, *8*(4), 400-415.

[21] Keerthana, G., & Padmavathi, G. (2016). Detecting sinkhole attack in wireless sensor network using enhanced particle swarm optimization technique. *International Journal of Security and Its Applications*, *10*(3), 41-54.

[22] Jamali, S., & Fotohi, R. (2017). DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system. *the Journal of Supercomputing*, *73*(12), 5173-5196.

[23] Renold, A. P., & Ganesh, A. B. (2019). Energy efficient secure data collection with path-constrained mobile sink in duty-cycled unattended wireless sensor network. *Pervasive and Mobile Computing*, *55*, 1-12.

[24] Udoh, E., & Getov, V. (2018, March). Performance Analysis of Denial-of-Sleep Attack-Prone MAC Protocols in Wireless Sensor Networks. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)* (pp. 151-156). IEEE.

[25] Atashpaz-Gargari, E., & Lucas, C. (2007, September). Imperialist competitive algorithm: an algorithm for optimization inspired by imperialistic competition. In *2007 IEEE congress on evolutionary computation* (pp. 4661-4667). Ieee.

[26] Mohamadi, H., Ismail, A. S., Salleh, S., & Nodehi, A. (2013). Learning automata-based algorithms for solving the target coverage problem in directional sensor networks. *Wireless personal communications*, *73*(3), 1309-1330.

