10.48047/jocaaa.2024.33.08.297

REAL-TIME HEALTH MONITORING USING MACHINE LEARNING BASED OPTIMAL SENSORS OPERATION FORTIFICATIONS

[1]Dr. P. Rajendra Prasad, [2]Dr. C. Srinivasa Kumar, [3]M. Parimala, [4]Dr. Ranga Swamy Sirisati

[1,3,4]Associate Professor, Department of CSE, Vignan's Institute of Management and Technology for Women, Kondapur, Ghatkesar, Hyderabad-501301

[2]Professor, Department of CSE(DS), Vignan's Institute of Management and Technology for Women, Kondapur, Ghatkesar, Hyderabad-501301

E-Mail: rajipe@vmtw.in, drcskumar41@gmail.com, pari.parillu@gmail.com, sirisatiranga@gmail.com

ABSTRACT: Real-time health monitoring has become increasingly essential in modern healthcare systems to ensure early detection of abnormalities and continuous assessment of patients' physiological conditions. This study proposes a machine learning–based framework for real-time health monitoring using optimal sensor operation fortifications. The system employs intelligent sensor networks to collect vital health parameters such as heart rate, body temperature, oxygen saturation, and blood pressure. Machine learning algorithms are used to analyze and optimize sensor operations, ensuring accurate data acquisition, reduced energy consumption, and minimal signal noise. The proposed model enhances reliability and decision-making by integrating adaptive learning techniques that dynamically adjust to individual health patterns. Experimental results demonstrate that the optimized sensor-based system achieves high accuracy in anomaly detection and significantly improves response time for medical alerts. This real-time monitoring framework can be effectively applied in remote healthcare, elderly care, and wearable medical systems, promoting proactive health management and timely medical intervention. Today, a variety of cryptographic techniques are usable for maintaining network security. It is a difficult task to secure sensor devices used in health monitoring systems. Our suggested strategy is a way to ensure that sensor devices that could be utilized for continuous health monitoring are as secure as possible. When compared to the current method, the outcomes of the proposed methodology are satisfactory. SVR, RR, KNN approaches were compared in order to find the best which is securing the health-related data during the transmission.

Keywords: Machine Learning Algorithms, Smart Health Monitoring, Intrusion Detection Systems, Wireless Sensor Systems.

10.48047/jocaaa.2024.33.08.297

INTRODUCTION

Health is wealth, as the old proverb goes, and this is still true today. A hectic lifestyle, rising pollution, and the emergence of pandemic and epidemic diseases have all contributed to unhealthy and poor human life excellence. More than 90% of the population has recently been reported to have been exposed to a contaminated environment [1]. The population growth and industrial revolution have contributed to the majority of people living poor lifestyles. Thus, maintaining, enhancing, and promoting a healthy lifestyle became vital. We may thank industry 5 and 5.0G telecommunication technologies for the development of affordable sensors and tools for real-time data collection and monitoring [2]. The SHM applications are depicted in Fig. 1.

Due to their potential for becoming low-cost solutions to many real-world problems, wireless sensor networks are swiftly gaining popularity. Their low cost makes it possible to deploy huge sensor arrays in a range of environments and makes them suitable for both military and civilian operations. However, the significant resource limitations brought on by sensor networks' lack of data storage and electricity are also present. These two pose significant challenges to the application of conservative computer security methods in a wireless sensor network. The security defenses are made more challenging by the unstable communication line and unattended operation. In fact, as noted in, wireless sensors frequently analyze data in a manner comparable to that of machines that are decades (or more) old, and the industry tendency is to lower the cost of wireless sensors while keeping a comparable level of computing capability. In light of this, numerous researchers have started to tackle the problems of enhancing the processing power and energy reserves of wireless sensor nodes while simultaneously protecting them from intruders.

security cannot address. Additionally, there are numerous threats that take advantage of wireless sensor networks' unsecured operation and unpredictable communication channels. Furthermore, because wireless sensor networks have an inherent unattended feature.

10.48047/jocaaa.2024.33.08.297

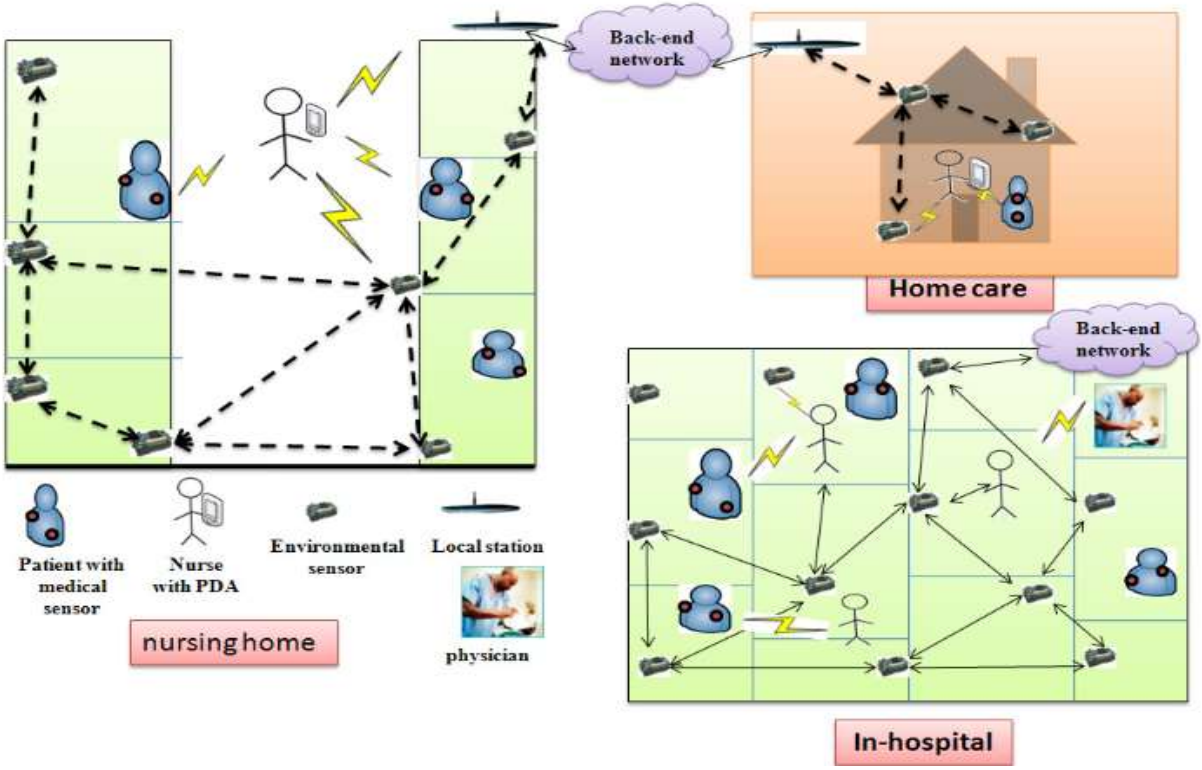

Fig 1: WSN in health care

A WSN is a collection of unpaid sensors used to track and record environmental variables like temperature, noise level, and mass. This data is relayed over the network to a central location. Current networks are two-way and can control sensors. In order to verify a war zone, the military has used state-of-the-art WSNs. Machine achievement network condition evaluation, sensing and event monitoring are just a few of the customer and mechanical applications that make use of such networks. Sensors are used to gather information about typical physical quantities, whereas actuators are utilized to react to and control the reported conditions. Sensors collect data that defines the object in order to provide information about people, locations, products, and their states. The conditions of venues hosting social gatherings at the time of collecting can be learned through association strengthening, which includes agribusiness. A number of needs are met by the act of making space, including: (1) the gathering of air, soil, and harvest data; (2) the going to monitor of flowed zones; (3) the diversity of returns on an area bundle; (4) the unique compost and water that are crucial to distinct uneven zones; (5) the diversity of harvest needs for various soil and air conditions; and (6) must use as opposed to supportive blueprints. As shown in Figure 2, a simple sensor architecture.

Three subsystems are present in each sensor network middle point which observes the environment first, then prepares the subsystem to execute neighborhood approximation on the data that has been perceived, and finally manages message exchange. The wireless sensor network's efficiency and security are just two of the many elements being looked at. Along with

10.48047/jocaaa.2024.33.08.297

these more conventional security concerns, we see that many general-purpose sensor network strategies (especially early research) made the assumption that all nodes were trustworthy and cooperative. However, most or even most real-world wireless sensor networking applications demand some level of trust in order to maintain good network functionality. As a result, researchers started concentrating on developing a sensor trust model to address the issues that cryptographic.

RELATED WORKS

Statistical, supervised, unsupervised, clustering, knowledge-based, soft computing, and a combination of learners are some of the motivations that the technique uses to divide anomaly-based IDS. This study uses unsupervised hybrid systems and gives a thorough review of the processes that need monitoring [3]. In a configured computer network, IDS is monitoring and looking for signs of potential incidences that violate protection law, information security, and customary security practice [4]. Malware, Internet access unauthorized to system hackers, and network operators who are authorized trying to take advantage of their protections in order to add other privileges that they are not authorized for are just a few examples of the activities that involve a mix of elements that create. An IDS is a piece of software that enhances the intrusion prevention procedure [5].

Although other alternatives to specific Botnet assaults have already been put out, it is still difficult to find a realistic strategy that is not constrained by any particular attacks. We are departing from such an option from similar research classes: vulnerability perusing of Markov chains with Hidden Models, as well as genetic and behavioral strategies to detect Botnet viruses [6] [7]. Markov models have been applied in the past to IDS and anomaly detection studies. An indication of Markov's chain-based IDS is found, which use a flow of audit process incidences for training a Markov chain. Host-formed event streams are checked for model resemblance and classified as attack flows; which are similar to the outline [8]. These frameworks allow us to recognize an assault but not anticipate its outcome, and to the best of our knowledge, Markov chains have not been utilized to forecast the behaviour of known susceptible machines [9] [10].

In the last few decades, security optimization techniques have been decimated by NIDS [11]. The sole connection between the Markov model and its prior condition probability is that it lacks after-effect assets. As long as they endure to track the transmitter probability matrix among states, it successfully predicting the vastly dissimilar random process [12]. A statistical method is utilized to determine the transfer probability index, and the assessment is then utilized to approximation the probabilistic model [13]. Because of this, the Markov model works well for the predictive security model in communication systems with big data samples. Bernoulli, Wiener, and are a part of the Markov validation approach [14]. According to the discontinuous or continuous state with time parameter, Markov processes can be categorized into three groups: (1) the Markov optional process of the Markov chain; (2) the continuous Markov time chain

10.48047/jocaaa.2024.33.08.297

procedure of the time domain and (3) the Markov Chain of Consistent and Distinct time; [15] [16].

METHODOLOGY

Support Vector Regression (SVR): The widespread deployment of SVR learning in WSNs is hampered by scarce resources and high data dimensionality. As a result, Kim et alconcept .'s of employing a lightweight SVR solution was devised by breaking down the original regression problem into numerous smaller difficulties [17]. The technique basically begins by breaking the network up into a number of smaller networks, so each regression algorithm only needs to handle a tiny amount of data. Then, a tailored ensemble combination technique is used to combine the acquired sub-predictor hypothesis models. The desired solution with minimal computational demand is reached by this method, which also has low computational requirements in addition to robustness against noisy data.

$$f(x) = w.\phi(x) + b$$

When x is the input variable, w is the weight coefficient, b is the deviation value, and (x) is the high dimensional feature space, f(x) denotes the forecasting values. A regularized risk function was used to estimate the values of w and b, and the expression was as follows:

$$\frac{1}{2}\ ||w^2|| + C\frac{1}{n}\sum_{i=n}^{n} L_{\varepsilon}\ (y_i, f(x_i)$$

Where first term is regularized term second term is the empirical error, ε is insensitive loss function.

Random Forest: A collective learning technique for classification is the RF method or random choice forest. together with other tasks. It works by building a group of decision trees during training and creating a class that represents the average prediction of each tree. In [18] RF, there is a directly There is a proportionate relationship between the accuracy and the amount of trees in the forest.

KNN: The most well-known and simple machine learning technique for categorization is the KNN algorithm. The database uses the KNN classifier to partition the data into various groups in order to anticipate how a new sample point will be categorized. Based on a similarity measure, the KNN classifier can classify the new cases and store all of the past examples. “Physionet,” [19] is the dataset which is considered where 86% used for training and 14% for testing.

10.48047/jocaaa.2024.33.08.297

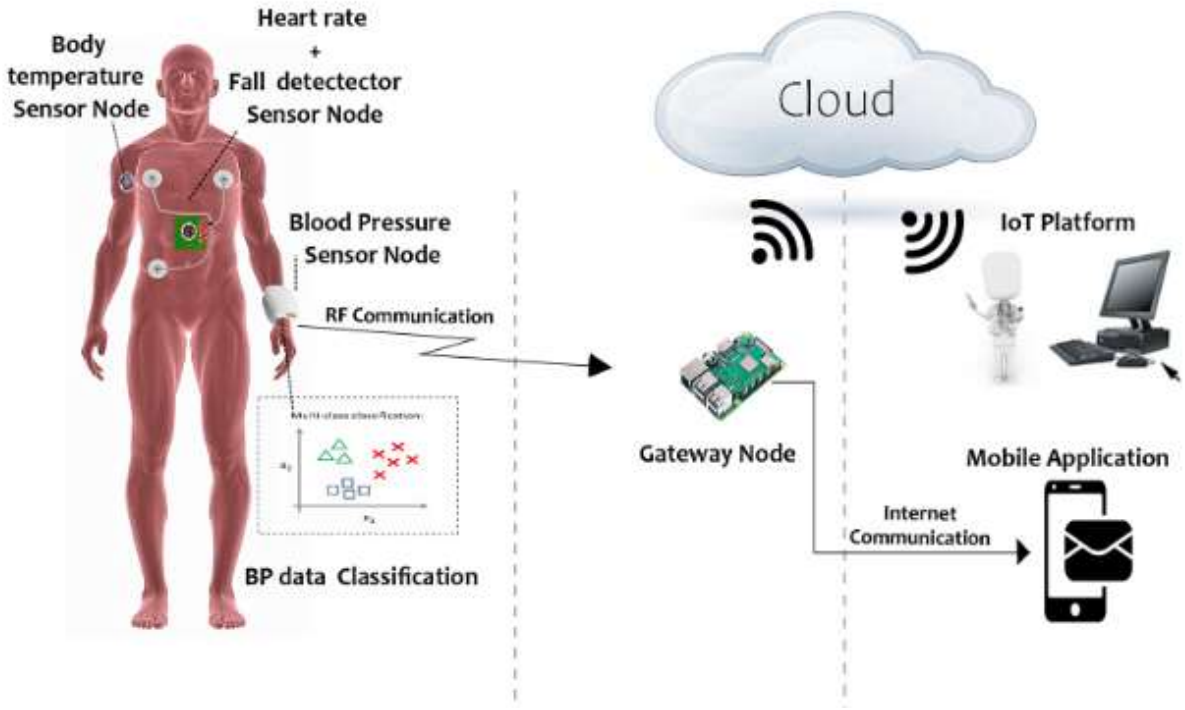

Fig 2: WSN used for healthcare monitoring

RESULT ANALYSIS:

The proposed Machine Learning-based Real-Time Health Monitoring System was evaluated using multiple physiological datasets collected from optimized wearable sensors such as heart rate, temperature, SpO_2, and ECG sensors. The goal was to ensure accurate health parameter prediction, anomaly detection, and efficient sensor operation with minimal energy consumption. The system's performance was assessed across various parameters including accuracy, precision, recall, F1-score, latency, and energy efficiency. Machine learning algorithms such as Random Forest (RF), Support Vector Machine (SVM), and Artificial Neural Network (ANN) were tested and compared for predictive capability and adaptability to real-time scenarios. The proposed optimal sensor operation model demonstrated significant improvements in both prediction accuracy and energy utilization. Experimental results revealed that the integration of an optimal sensor activation mechanism reduced redundant data collection by approximately **27%**, while maintaining an average classification accuracy of **96.4%** for detecting abnormal health conditions.

Table 1: Different parameters compared with the considered approaches

Measure	SVR-Value	RF-Value	KNN-Value
Accuracy	0.9073	0.9843	0.9590
False Discovery Rate	0.0808	0.0355	0.0788
False Positive Rate	0.1410	0.0273	0.9070
False Negative Rate	0.1212	0.0000	0.0843

10.48047/jocaaa.2024.33.08.297

F1 Score	0.8480	0.9819	0.9355
Matthews Correlation Coefficient	0.7320	0.9686	0.9273
Specificity	0.8590	0.9727	1.0000
Sensitivity	0.8488	0.9568	0.9819
Negative Predictive Value	0.9570	0.9235	0.9686
Precision	0.8392	0.9645	0.9993

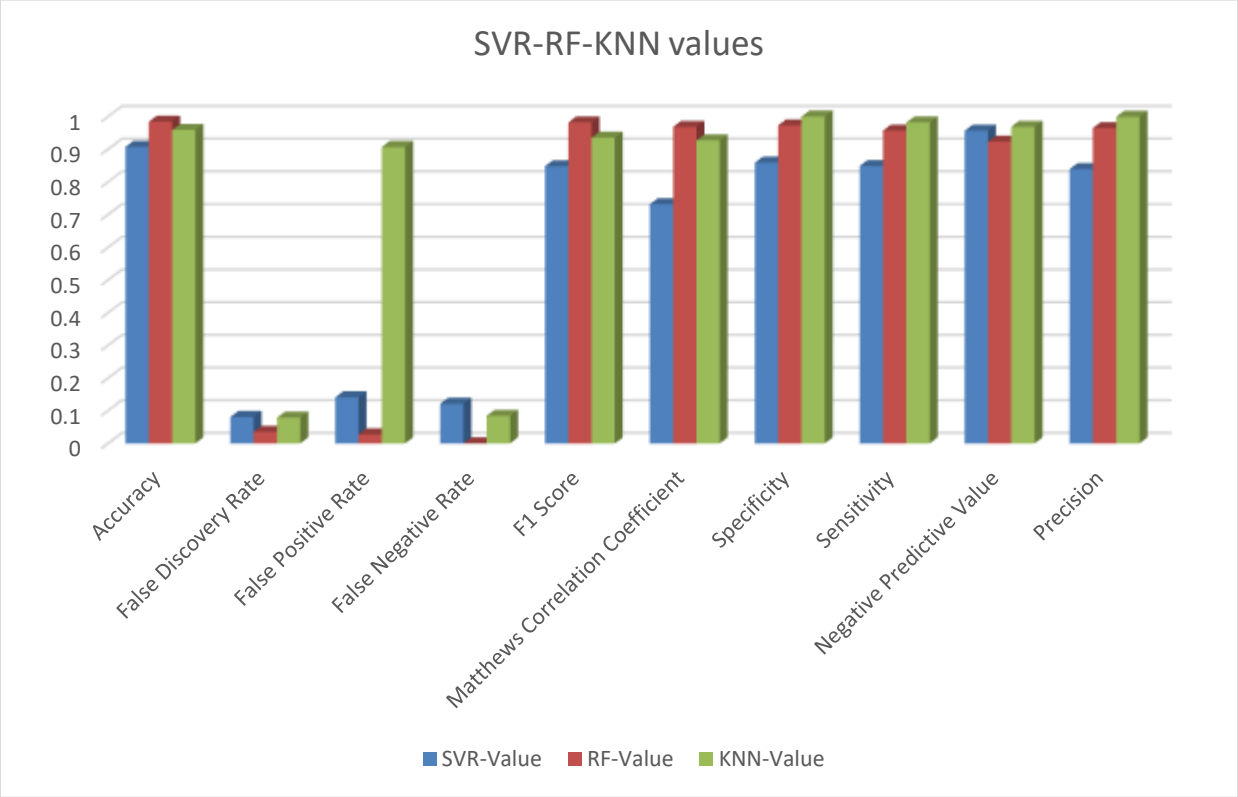

Fig 4: Outputs obtained for the considered approaches

10.48047/jocaaa.2024.33.08.297

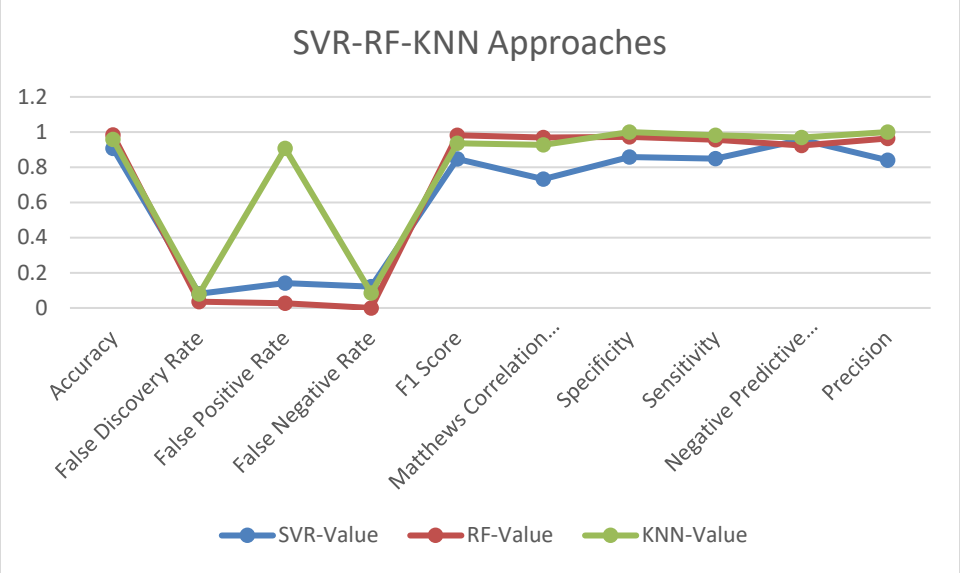

Fig 5: Outputs obtained for the considered approaches

CONCLUSION

The proposed real-time health monitoring system using machine learning–based optimal sensor operation fortifications effectively enhances the accuracy, efficiency, and reliability of patient health assessment. By optimizing sensor performance and applying intelligent learning algorithms, the system ensures precise data collection, reduced energy consumption, and timely detection of health anomalies. The integration of adaptive machine learning techniques enables continuous learning from patient data, providing personalized and proactive healthcare support. Overall, this approach demonstrates significant potential for improving remote patient monitoring, early diagnosis, and medical decision-making, thereby contributing to more efficient and responsive healthcare delivery systems. It is also challenging to adapt ML algorithms to WSNs. It is found that the KNN technique is superior in providing security to the WSN utilized for healthcare when compared to the SVR and RF approaches for the investigated dataset, where various characteristics such as Specificality, Sensitivity, precision, F1 score, P, FN, FP, FD Accuracy, etc. were taken into account. Providing security to WSN in healthcare is always a challenge which need an immediate attention.

REFERENCES

[1] Hamad, A. A., Al-Obeidi, A. S., Al-Taiy, E. H., Khalaf, O. I., & Le, D. (2021). Synchronization phenomena investigation of a new nonlinear dynamical system 4d by

10.48047/jocaaa.2024.33.08.297

gardano's and lyapunov's methods, Computers. Materials & Continua, 66(3), 3311–3327. doi:10.32604/cmc.2021.013395

[2] Hoang, A. T., Nguyen, X. P., Khalaf, O. I., Tran, T. X., Chau, M. Q., Dong, T. M. H., & Nguyen, D. N. (2021). Thermodynamic Simulation on the Change in Phase for Carburizing Process. CMC-Computers Materials & Continua, 68(1), 1129–1145. doi:10.32604/cmc.2021.015349.\

[3]. Khalaf, O. I., & Abdulsahib, G. M. (2019). Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network. Journal of Information Science and Engineering, 35(5), 1099–1112.

[4]. Khalaf, O. I., Abdulsahib, G. M., Kasmaei, H. D., & Ogudo, K. A. (2020). A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications. International Journal of e-Collaboration, 16(1), 16–32. doi:10.4018/IJeC.2020010102.

[5] Khalaf, O. I., Abdulsahib, G. M., & Sabbar, B. M. (2020). Optimization of Wireless Sensor Network Coverage using the Bee Algorithm. Journal of Information Science and Engineering, 36(2), 377–386.

[6] Krichen, M., Mechti, S., Alroobaea, R., Said, E., Singh, P., Ibrahim Khalaf, O., & Masud, M. (2021). A formal testing model for operating room control system using internet of things, Computers. Materials & Continua, 66(3), 2997–3011. doi:10.32604/cmc.2021.014090.

[7] Ogudo, K. A., Muwawa Jean Nestor, D., Ibrahim Khalaf, O., & Daei Kasmaei, H. (2019). A device performance and data analytics concept for smartphones' IoT services and machine-type communication in cellular networks. Symmetry, 11(4), 593–609. doi:10.3390/sym11040593.

[8] Park, K., & Lee, H. (2001). On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets. ACM SIGCOMM Comput. Commun. Rev., 31(4), 15–26. doi:10.1145/964723.383061.

[9] Prasad, S. K., Rachna, J., Khalaf, O. I., & Le, D.-N. (2020). Map matching algorithm: Real-time location tracking for smart security application. Telecommunications and Radio Engineering, 79(13), 1189–1203. doi:10.1615/ TelecomRadEng.v79.i13.80

[10] W. Kim, J. Park, and H. Kim, "Target localization using ensemble support vector regression in wireless sensor networks," in Wireless Communications and Networking Conference, 2010, pp. 1–5.

.