Alinteri J. of Agr. Sci. (2021) 36(2): 76-81
e-ISSN: 2587-2249
info@alinteridergisi.com

http://dergipark.gov.tr/alinterizbd
http://www.alinteridergisi.com/
DOI:10.47059/alinteri/V36I2/AJAS21117

RESEARCH ARTICLE

Mobile Ad Hoc Networks Intrusion Detection in Co-Operative Motion

K. Pazhanisamy[1*] • Dr. Latha Parthiban[2]

[1]Research Scholar, Pondicherry University, Pondicherry, India. E-mail: kpsamy09@gmail.com*

[2]Assistant Professor, Department of Computer Science, Pondicherry University (CC), Pondicherry, India.

E-mail: athaparthiban@yahoo.com

A R T I C L E I N F O

Article History:
Received: 30.04.2021
Accepted: 10.06.2021
Available Online: 12.07.2021

Keywords:
Partial Swarm Optimization
Intrusion Detection
Support vector Regression(SVR)
Cooperative Algorithm
Anomaly Detection

A B S T R A C T

As the number of wireless devices continues to increase rapidly, mobile ad hoc networking (MANET) has emerged as an exciting and significant technological advance. MANETs were susceptible to attacks because of their open media, continuously changing network design, cooperation mechanisms, lack of a protective measure and management point, and a coherent layer of attack. However, regular functioning frequently generates traffic corresponding to a "signature attack," which leads to false alerts. One of the significant disadvantages is the inability to identify new attacks without established signatures. In this article, we describe our efforts towards creating the capability for MANET intrusion detection (ID). Based on our previous works on outlier detection, we explore how Intrusion Detection in Partial Swarm Optimization (IDPSO) and Support vector Regression(SVR) may improve an anomaly detection method to give additional information about attack kinds and origins. We can use a basic formula to determine the attack type for many well-known assaults whenever an anomaly is detected.

Please cite this paper as follows:

Pazhanisamy, K. and Dr. Parthiban, L. (2021). Mobile Ad Hoc Networks Intrusion Detection in Co-Operative Motion. *Alinteri Journal of Agriculture Sciences, 36*(2): 76-81. doi: 10.47059/alinteri/V36I2/AJAS21117

Introduction

With wireless devices like Wireless telephones, PDAs and mobile laptop computers rapidly spread over the past several years, the potential and significance of mobile Ad Hoc networking are becoming evident. A MANET create by a collection of wireless mobile nodes which frequently have no fixed network support. The nodes must collaborate by sending packets to connect with nodes across the radio range. Many major MANET applications are available [3].

All wireless communication technology needs collaboration since the systems to need to work cooperatively, and at least the edge hosts need compatible and somewhat defined transmission methods and protocols. However, the cooperation requirement for Ad Hoc networks is extremely severe and maintained at all levels of the system. In the appropriate environment, cooperative did not always anticipate these difficulties.

The downloading of sensitive information to public cloud providers present safety concerns, including accessibility, privacy and business integration. In addition, non-stop cloud providers have resulted in high levels of infiltration and abuse. The only permanent option to safeguard information and cloud resources for users is the deployment of firewalls and intruder detection systems. Some attacks, such as DOS, are too sophisticated for firewalls; you may employ attack detection techniques to identify different kinds of attacks.

Intelligent and meta-heuristic algorithms have recently become the most utilises methods of attack detection. Meta-heuristic algorithms may use to analyse attack databases or to maximize and improve classifier accuracy. These techniques are thus trustworthy and appropriate for assaults and abnormalities. SVR was used to categorize the assaults, and then IDPSO utilises the method Particle Swarm to improve and enhance the accuracy of this classification. Figure 1 shows the intrusion detection architecture for MANET.

In this work, the IDPSO functions are implemented and SVR utilises as evaluator for the PSO genetic algorithm using

* Corresponding author: kpsamy09@gmail.com

a single-to-rest approach arising a multi-user issue literature. The findings show that our approach has shown a higher accuracy compared to the classification methods.

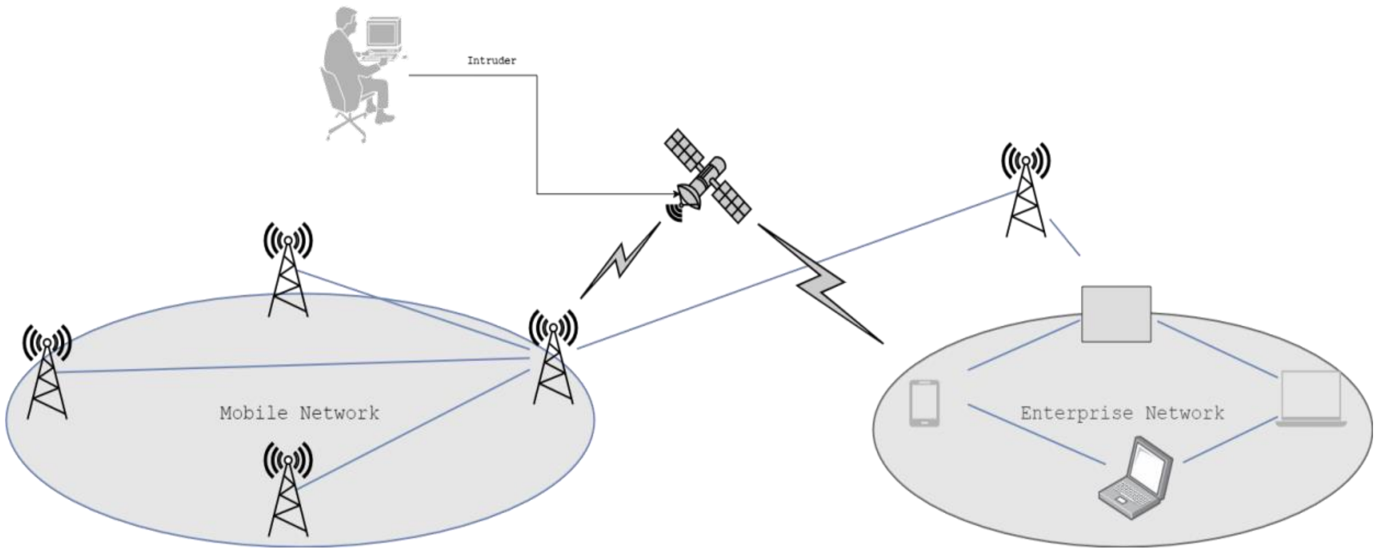

Figure 1. The intrusion detection architecture for MANET

Related Work

Attacks on a node as an individual can occur in a network, and the attack locations are not limited to a specific layer of protocol, and may impact multiple protocol layers simultaneously. Malicious attacks can occur on a node as an individual in a network, and they are not limited to a specific protocol layer[1]. A technique for detecting[2] the lost packages on the basis of only one hashing chain and a unique hash tag commitment. The way the technique is implemented largely relies on the way redundant data packets are sent and secret keys are shared across nodes. The source node must also anticipate the transmitted status of the next packet header. The main disadvantage of the method is that latency management is already too large, especially whenever the networking size is larger, a public key can be guaranteed of being transmitted.

The FS method [7] and classification using a (SVM) Vector Support Machine. The study also included the examination of intrusion detection and FS categorization methods. In addition, soft computing methods emphasize the research difficulties of intrusion detection: PCA and (PSO) FS particle swarm optimization for transformation features. The theoretical approach for intrusion detection presented using the SVM Classification on the datasets KDD Cup 99. This study effort further expanded utilizing the NSL-KDD datasets neural network. [9]evaluated various computing SR techniques and found that regression methods have disadvantages in identifying and usually out performance of unknown parameters. The unknown regression technique parameters calculated via optimization.

A novel distributed clustering[10] technique for lengthy, prototype-implemented Ad Hoc sensor networks. Besides the available load levels in sink node, The approach provided doesn't really assume any infrastructure presence or node characteristics in general. An energy-efficient distributed clustering technique, Hybrid Energy-Efficient Distributed clustering (HEED), is given here that chooses heads of cluster on an ongoing basis that are appropriate for each node's remaining energy and its closeness to node degree or other nodes. HEED completes the job with O-turns, makes a little overhead message that obtains a fairly consistent distribution of cluster heads throughout the networks.

A method to hybrid node scheduling[11], it includes sleep schedules in time-drived modes for regular monitoring areas of interest and weather schedules event-driven modes for tracking emergencies. A error rate is incorporated in the sleeping pattern to improve reliability in the sensor nodes. A wake-up sensors threshold and normal sleep restriction are provided in the awakening plan to minimize energy use.

The Extended Version of the SEER Protocol is a Basic Energy-Aware Routing Protocol (BEAR) [12]. In-network set-up authors introduce a novel method to balance the network by computing a likelihood for each neighbouring node and using the probability for selecting the delivery node instead of remaining energy in SEER. They also utilized an apprenticeship to maintain the level of power of each node where the significance of the sender added to the data header. There is thus no requirement for energy communication such as the SEER protocol.

Proposed Work

In this part, we review our previous anomaly detection work and explain how to figure out the kinds of attacks and origins of certain known assaults after reports of an abnormality. Let's start by describing various MANET assaults and the incursions in our tests.

MANET Attacks

About intrusion detection and reaction, abnormalities related to both the result and the method of the assault should be observed and analyzed. While this shows that an assault occurred or is spreading, the technique may frequently assist in determining the attacker's kind and even the identity.

According to their effects, MANET attacks may be classified as follows:

Deprivation of sleep: a node is obliged to expend its power.

Egoism: A node is not a conduit to other nodes.

Rushing: may be utilized to enhance the messages from the manufactured route. Certain routing communication classes have the characteristic that the receiver recognizes only a message arriving first in multiple routing protocols. The attacker merely distributes a fraudulent control signal to prevent subsequent legal communications.

Routing Loop: Added a loop in a route path.

Partition of Network: A linked network subdivided into k subnetworks, where nodes in various subnetworks cannot interact while a route exists between them.

Dropping packet: A node loses packets of data it should transmit.

Spoofing: injecting or controlling packets with amended source addresses.

Denial-of-Service: A node cannot receive and transmit data packets to destinations.

Blackhole: All traffic routed to a particular node that cannot transmit any traffic.

Manufactured route message: harmful content messages (route requests, route responses, etc.) will injected into a network. The techniques specified include:

Poisoning cache: the information saved in the tables is either amended, erased or misrepresented.

Wormhole: between two nodes, a tunnel used for the covert transmission of packets formed.

Malignant swamping: Deliver extraordinarily vast amounts of information or controlling messages to the entire network or specific target nodes.

Particle Swam Optimization

The next branch of evolutionary algorithms, based on team dynamics and synergy, is Particle Swarm Optimization (PSO). It was born of coordinated action simulators in big birds or in fish schools. Such algorithm utilize n-dimension particles to look for solutions for an n-variable operational optimization process, since these animals wander about a 3-dimensional world, seeking food or avoiding predators. Individuals in PSO are referred to as particles, while the whole community referred to as a swarm[4].

The starting swarm usually generated to disperse the populations of the particle uniformly across the search area. Every particle is updated at all times, following two "best" values, termed p_{best} and g_{best}. Each particle maintains records of its locations in the issue space linked with the particle's best solution (fitness). Stored this fitness value and named p_{best}. When a particle accepts whole populations as its topographical neighbour, the best deal is a "best" global value and is termed g_{best}. The PSO's pseudo-code provided below.

Input : $f : x^D \rightarrow R.\ N \in N$
  For such particles $n \in \{1,\ldots,N\}$ *do*
  Chow position $x^n \in R^D$ *at random;*
  $v^n := \{0\}^D$;
  $L^n := X^n$;
  end
  $G ; = arg\,min\,\{f\,(L^n)\}$:;
  While termination criterion not fulfilled do
    For each particle $n \in \{1,\ldots,N\}$ ***do***
      Update velocity V^n according to movement Equation in Def. 1;
      $p_{best} = g^n + g_{best}$;
      $C^n = arg\,min\,\{f\,(A^n), f\,(C^n)\}$;
      $B = arg\,min\,\{f\,(A^n), f\,(B^n)\}$;
    end
  end
  return G

We first selected the necessary particle number based on particle swarm principles and then randomly generated the initial alphabetical string coding for each particle. We encoded each particle in evolutionary algorithms for the imitation of the chromosomes. The S=F1 K Fn, n=1, 2, k, m binary alphabetic string has coded for each particle; the bit {1} indicates a chosen feature, while the bit {0} indicates a non-selected function.

Each renewal of particles is dependent on their adaptive value. For each particle renewal, the best adaptive value is p_{best}, and the most significant adaptive value within such a p_{best} group is g_{best}. Once we have p_{best} and g_{best}, we can monitor p_{best} and g_{best} particle characteristics in terms of their location and speed. The research uses a binary representation of a PSO algorithm for optimizing particle swarm[5]. The area within each particle provided in a binary number from which the fitness required.

Initially, SVMs (Support Vector Machines) developed to solve issue classification[31]. SVR is an SVM variant[6]. The SVR model's fundamental functions intended to give a non-linear mapping function that can map the training data to ample functional space. The training data set is indicated by the input location, the actual output and the amount of the data; it is the SVR function

$$a = f(b_i) = \omega^M \varphi(b_i) + z \quad \ldots\ldots\ldots\ldots. 1$$

$$f(b) = \sum_{i=1}^{n} (\alpha_i - \alpha_i^*) m(b_i, b) + z \ldots\ldots\ldots\ldots\ldots\ldots\ldots 2$$

$\alpha_i \wedge \alpha_i^*$ consists of the Lagrange multipliers and is a kernel function. When applied to the SVR input space, the kernel function produces a nonlinear decision hypersurface. The Stochastic radial basis (RBF) kernel, the most commonly used kernel, conducts a mapping function between the spatial domain and a high-dimensional space. Still, it is also simple to construct, making it ideal for addressing nonlinear issues; it was the motivation for using the Stochastic RBF kernel in this research:

$$k(b_i, b) = exp(-\sigma \vee b - b_i \vee^2) \ldots\ldots\ldots\ldots 3$$

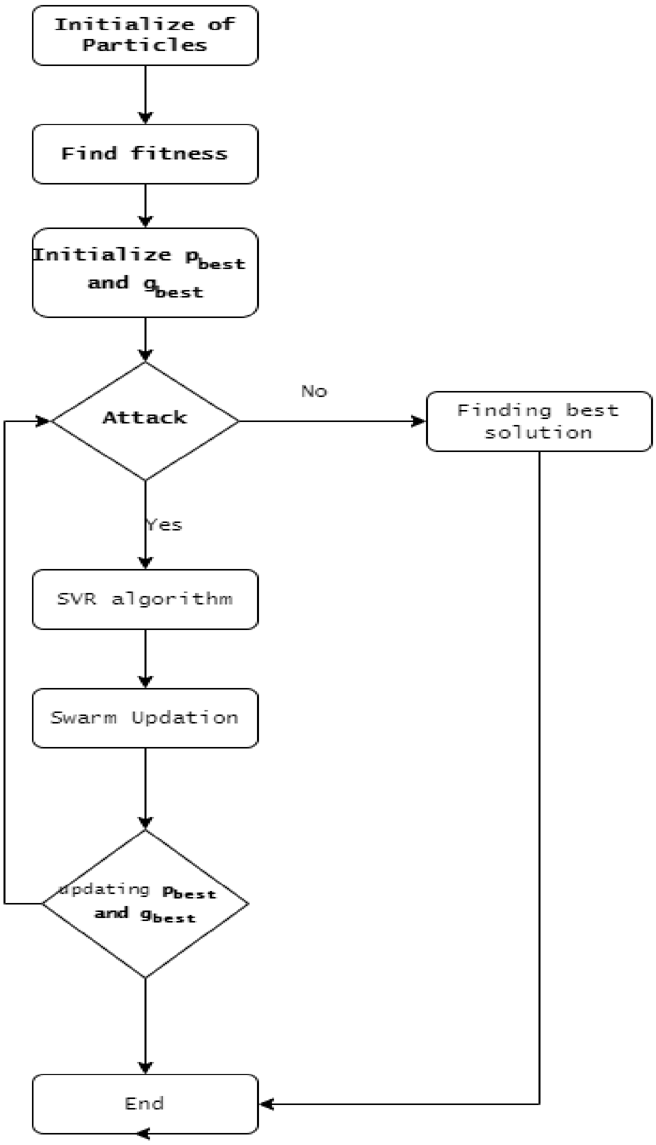

Figure 2. Flowchart for IDPSO and SVR

Results and Discussions

In this research, we use a standard datasets, which is the raw data from the 2019 intrusion detection competition. This database contains a large number of intrusions that modeled in a militarized network environment, and it serves as a standard benchmark for the assessment of intrusion detection methods in general. In general, probes and denial-of-service assaults account for the majority of all attacks. Compromises, for example, are among the most intriguing and hazardous assaults, but they are severely underrepresented. Each connection record in the data set contains 41 characteristics, plus one class label, which totals 42 attributes in total. There are 24 different attack kinds, but we consider them all as a single attack group. It is necessary to process a data collection of size N. The nominal characteristics transformed into nonlinear numerical values via a linear discrete value transformation (integers). After the labels removed, the data set may represent a vector X with N row and m=41 column (attributes). There are eight discrete-value characteristics and thirty-three continuous-valued attributes in the database. Table 1 describes the daaset of KDD intrusion detection.

Table 1. Intrusion detection KDD dataset

Category types	Occurrence percentage	Instances
Network	20.0134	55,236
Blackhole	0.023	5,266
Dos	5.377	2,11,853
Probe	1,370	100
Whitehole	71.002	17,432

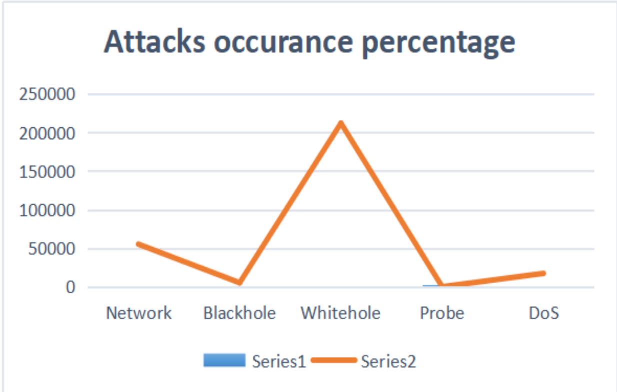

Figure 3. Occurrence of attacks percentage

Table 2. Comparison with proposed work

Methods	Accuracy
MI-BGSA[13]	88.36
Proposed approach	99.32

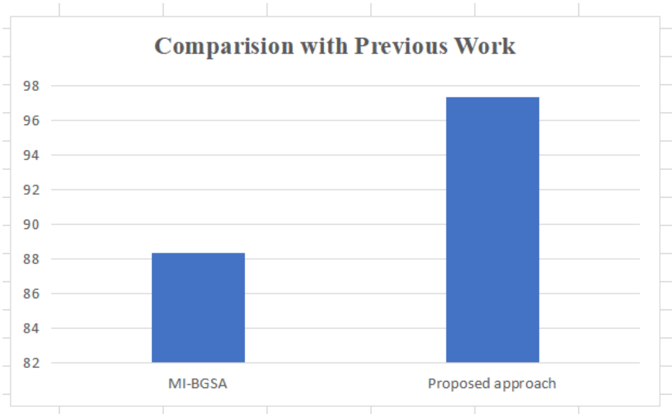

Figure 4. Comparison chart

Conclusion and Future work

In this work we use vector regression techniques and optimization of particle swarm for intrusion detection in order to avoid a harsh characterization among-st regular class and specific intrusion classes. We discuss the current state of IDPSO and SVR based intrusion detection systems, and propose potential data mining-based solutions. PSO, SVR based techniques for network security data minimization are explored. The detection model of intrusion is a compositional model requiring several theories and methods. Either one two models can rarely provide satisfactory results. We intend to use additional intrusion detection theories and methods in our research plan.

References

M. Karthigha, L. Latha, K. Sripriyan, A comprehensive survey of routing attacks in wireless mobile Ad Hoc networks. *In 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India,* pp. 396–402 (2020).

C. Jiang, R. Li, T. Chen, C. Xu, L. Li, S. Li, A two-lane mixed traffic flow model with drivers' intention to change lane based on cellular automata. *Int. J. Bio Inspired Comput.* 6(4), 229–240 (2020).

Balaji, K., P. Sai Kiran, and M. S Kumar. "An energy efficient load balancing on cloud computing using adaptive cat swarm optimization." *Materials Today: Proceedings* (2021).

J. Kennedy, R.C. Eberhart, Particle Swarm Optimisation, *in: Proceedings of the IEEE, International Conference on Neural Networks, Piscataway,* 1995.

Ganesh, D., Kumar, T.P. and Kumar, M.S., 2020. A Dynamic and adaptive learning mechanism to reduce cross layer attacks in cognitive networks. *Materials Today: Proceedings.*

H. Drucker, C. J. Burges, L. Kaufman, A. J. Smola, and V. Vapnik, "Support vector regression machines," in *Proceedings of Advances in Neural Information Processing Systems,* pp. 155–161, Denver, CO, USA, May 1997.

Ganapathy S, Kulothungan K, Muthurajkumar S, Vijayalakshmi M, Yogesh P and Kannan A 2013 Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. *EURASIP J. Wirel. Commun. Netw.* 1: 242–255.

Sushama, C., Kumar, M.S. and Neelima, P., 2021. Privacy and security issues in the future: A social media. *Materials Today: Proceedings.*

Khatib T, Mohamed A, Sopian K. A review of solar energy modeling techniques. *Renew Sustain Energy Rev. Pergamon;* 2012;16: 2864–2869.

O. Younis, S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks," *IEEE Trans. Mob. Comput.* 3 (2004) 366–379.

Davanam, G., Kumar, T.P. and Kumar, M.S., 2021. Novel Defense Framework for Cross-layer Attacks in Cognitive Radio Networks. *In International Conference on Intelligent and Smart Computing in Data Analytics: ISCDA 2020* (pp. 23-33). Springer Singapore.

Kumar MS, Harshitha D. Process Innovation Methods on Business Process Reengineering. *Int. J. Innov. Technol. Explor. Eng.* 2019.

Sangamithra, B., Neelima, P., & Kumar, M. S. (2017, April). A memetic algorithm for multi objective vehicle routing problem with time windows. *In 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE)* (pp. 1-8). IEEE.

K. Pazhanisamy and Dr. Lathaparthiban, "RFR Algorithm Using Secure Route Creation for Ad Hoc Networks," *in Australian Journal of Basic and Applied Sciences,* 2015, vol. 9, issue 21, pp. 43-46.

Deepa, N & Pandiaraja, P (2019) "A novel data privacy-preserving protocol for multi-data users by using genetic algorithm," *in journal of Soft Computing (Springer),* vol. 23, issue 18, 8539–8553, Annexure I, Impact Factor: 3.050.

A.Saranya, R.Naresh "Cloud Based Efficient Authentication for Mobile Payments using Key Distribution Method", *Journal of Ambient Intelligence and Humanized Computing,* Springer, 02 January, 2021. DOI: 10.1007/s12652-020-02765-7

R.Naresh, P.Vijayakumar, L. Jegatha Deborah, R. Sivakumar, "A Novel Trust Model for Secure Group Communication in Distributed Computing", *Special Issue for Security and Privacy in Cloud Computing, Journal of Organizational and End User Computing, IGI Global,* Vol.32, No. 3, Septemer 2020, Pp. 1-14. DOI: 10.4018/JOEUC.2020070101

A.Saranya, R.Naresh "Efficient mobile security for E health care application in cloud for secure payment using key distribution", *Neural Processing Letters, Springer,* 2021, DOI: 10.1007/s11063-021-10482-1

R.Naresh, M.Sayeekumar, G.M.Karthick, P.Supraja, "Attribute-based hierarchical file encryption for efficient retrieval of files by DV index tree from cloud using crossover genetic algorithm", *Soft Computing, Springer,* Vol.23, No. 8, 2019, Pp. 2561-2574. https://doi.org/10.1007/s00500-019-03790-1

R. Naresh, M Meenakshi, G Niranjana, "Efficient study of Smart Garbage Collection for Ecofriendly Environment", *Journal of Green Engineering,* Vol.10, No.1, pp.1-10, Feb 2020.

R Divya Mounika, R.Naresh, "The concept of Privacy and Standardization of Microservice Architectures in cloud computing", *European Journal of Molecular & Clinical Medicine,* Vol 7, No 2, Pages 5349-5370, Dec 2020.

M Meenakshi, R Naresh, S Pradeep "Smart Home: Security and Acuteness in Automation of IOT Sensors", *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* Vol. 9, No. 1, pp. 3271- 3274, Nov 2019.

K. Venkatesh, S. Parthiban, P. Santhosh Kumar, C.N.S. Vinoth Kumar, "IoT based Unified approach for Women safety alert using GSM", *Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021), IEEE Xplore Part Number: CFP21ONG-ART;* 978-0-7381-1183-4, pp.no. 388-392, 978-1-6654-1960-4/21/$31.00 © April 2021 IEEE

Raghav Rathi, Nishant Balyan, C.N.S Vinoth Kumar," Pneumonia Detection Using Chest X-Ray", *International Journal of Pharmaceutical Research (IJPR),* Volume 12, issue 3, ISSN: 0975-2366 July - Sept, 2020

Praharsha Sarma, Utkarsh Kumar, C.N.S. Vinoth Kumar, M.Vasim Babu, "Accident Detection And Prevention Using Iot & Python Opencv", *International Journal Of Scientific & Technology Research(IJSTR),* Volume 9, Issue 04,pp no. 2677-2681, ISSN No: 2277-8616 April 2020.

Gautam Srivastava, C.N.S. Vinoth Kumar, V Kavitha, N Parthiban, Revathi Venkataraman, "Two-Stage Data Encryption using Chaotic Neural Networks", *Journal of Intelligent and Fuzzy systems,* Vol. no.38, Issue.

No.3, pp no.2561-2568, ISSN No: 1875-8967. March 2020

M.Vasim Babu, C.N.S. Vinoth Kumar, M.Venu, International journal entitled "Improvisation of localization accuracy using ERSSI based on ADV-HOP algorithm in wireless sensor network", *International journal of innovative technology and exploring engineering (IJITEE),* ISSN No.2278-3075 Feb 2019.

C.N.S. Vinoth Kumar, A.Suhasini, "Secured Three-Tier Architecture for Wireless Sensor Networks Using Chaotic Neural Networks", 'Advances in Intelligent Systems and Computing' *AISC Series, Springer Science + Business Media Singapore* 2017 Vol. No. 507, Chapter No. 13, pp. No. 129-136, ISSN 2194-5357, DOI 10.1007/978-981-10-2471-9_13

Deepa, N & Pandiaraja, P 2020, Electronic healthcare system data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption", *in Journal of Ambient Intelligence and Humanized Computing,* DOI: 10.1007/s12652-020-01911-5, Annexure I, Impact Factor: 4.594.

B. Baron, P. Spathis, M. Dias de Amorim, Y. Viniotis, and M. H. Ammar, ''Motion as an alternative communication channel: A survey,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 289–314, 1st Quart., 2019.