Nat. Volatiles & Essent. Oils, 2021; 8(4): 10228-10243

NVEO
Natural Volatiles &
Essential Oils

Hybrid Deep Learning Prediction Model For Blackhole Attack Protection In Wireless Communication

[1]Deepti Joon , [2]Dr. Khyati Chopra

Ph.D scholar, GD Goenka University Gurugram Asst. Professor, JamiaHamdard, New Delhi.

joondeepti@gmail.com

khyatichopra134@gmail.com

Abstract:

Wireless communication consists of minimum battery storage with self organizing devices which are localized in random manner in order to monitor the environment to support the real time applications. Wireless communication maintains open access which leads to increase the malicious activities in the network. Mainly black hole attack is created in the network. As so to increase the battery power and to increase the network security in this paper we introduced Hybrid Deep Learning Prediction (HDLP) model in the wireless network. Our model mainly divided into two sections namely cluster based network and Auto Encoding for Key Management. The wide simulation experiments are conducted to analysis the performance of the network against black hole attack. The proposed model is also simulated and it is compared with the earlier model such as Deep Multi Task Learning (DMTL) and Deep Learning Based Defense Mechanism (DLDM). As the results, we found that our proposed model performed well in terms of Accuracy, End to End Delay, Energy Efficiency and Energy Consumption when compared with the earlier models.

1. Introduction

1.1 Motivation (wireless communication)

Regardless of the omnipresence of “wireless networks”, remarkably little is identified about their “algorithmic complexity and efficiency”: Designing and tuning a wireless network is a substance of knowledge, irrespective whether it is a “Wireless LAN” in an office building, a “GSM phone network”, or a “sensor network” on a volcano [1]. The fundamental communication limits of wireless networks are mentioned in which particularly, about what communication throughput could possibly be attained [2]. Inappropriately, the graph-based models are found to be too simplistic.

Consider for example a case of three wireless transmissions, each two of which could be arranged in a concurrent manner without a conflict. In a “graph-based model” one will determine that all three transmissions might be organized concurrently as well, while in certainty this might not be the case since wireless signals sum up [3]. As a substitute, it might be that two transmissions together create too much interference, deterring the third receiver from suitably receiving the signal of its sender. This “many-to-many” relationship marks understanding wireless transmissions demanding – a model where interference sums up seems dominant to strictly realizing wireless communication [4]. Likewise, a graph-based model generalizes “wireless attenuation”. In graph-based models the signal is “binary”, as if there was an indiscernible wall at which the signal proximately drops. Not remarkably, in reality the signal drops elegantly with distance [5].

Wireless communication system has extended top altitudes in its range of applications wide-reaching. Quick obligation of self-determining mobile users has become an operative area of development in wireless communication systems. Alternative search, “release mission, disaster respite efforts, mine site operations, conferences, and automated classrooms” are some of the examples of diverse mobile applications.

Collective networks of such users are named as “Mobile Ad hoc Network (MANET)”. These kinds of networks do not sustain a continual infra-structure. Each node in the network changes their position consistently. This grade in high active topology triggering cracked wireless links. The routing in “ad hoc networks” has been an active area of research and in former years, reasonably a lot of decisive routing protocols have been offered for MANETs. “Node mobility, constrained physical security, and limited amount of resources” are the major contests tackled by MANET.

“Routing, multicasting, pricing structure, transport layer protocol, security, self-organization, disposition consideration, and scalability” are specific dynamic features which could distress the performance and design of “MANET” [6]. The action of intermediary nodes should be trusted equally to initiate new routing path and make routing protocol of “MANET” to function in an effective manner. These nodes will function as per the protocol rules. In “MANET” operation system, considering any intermediary node to function as per the protocol is an essential theme of issue. This is mostly owing to the dynamic nature of the network. Also these nodes continually join or leave any network with respect to “connectivity and mobility”. There are numerous drawbacks of “MANETs”. They are

- Fortifying broadcast wireless communication in an un-trusted environs

- Nodes commencing individual paths
- Un-static system topology [7].

1.2 Contribution

On the contrary, the learning based “data-driven methods” offer a novel approach for handling the deficiency of the supposed channel models. In recent times, “deep learning” has been applied to enhance the traditional block-structure communication systems, comprising the “multiple-input and multiple output (MIMO) detection” [8], “channel decoding, and channel estimation”. In addition, deep learning centered systems have also shown remarkable progress by equally elevating the conventional communication blocks, which includes “joint channel estimation and detection, joint channel encoding and source encoding”. Further enhancing the traditional communication blocks, “deep learning” delivers a novel pattern for future communication schemes [9].

As a pure “data-driven” method, the features and the constraints of a “deep learning model” could be learned openly from the data, without “handcraft or ad-hoc designs”, by enhancing an end-to-end loss function. Motivated of this approach is end-to-end learning” based communication systems have been examined in some preceding works where both the transmitter and the receiver are signified by “deep neural networks (DNNs). This outline could be inferred as an “auto-encoder system”, which is extensively deployed in learning representations of the data [10]. The “transmitter and the receiver” relate to the auto-encoder and auto-decoder, respectively. The transmitter and the receiver “DNNs” are accomplished offline by using measurement or simulated data set in a “supervised learning manner” improving a loss function that redirects recovery accuracy.

“Machine learning (ML)” has newly reclaimed attention because of the effective applications of “deep learning (DL)” in “computer vision (CV)”, “automatic speech recognition (ASR)”, and “natural language processing (NLP)”. Embedding ML concepts on a catholic series of communication systems has had a broad history and has attained several successes, specifically in the upper layers, such as in “cognitive radio, resource management link adaptation [11] and positioning”. In contrast to the aforementioned straightforward applications, ML faces numerous challenges when applied to the physical layer. Scholars have functional ML to the physical layer for modulation recognition channel modeling and identification, “encoding and decoding”, channel estimation and equalization; conversely, ML has been unused commercially because handling physical channels is an intricate process, and conventional ML systems have restricted learning capacity.

Scholars believe that ML could reach further performance expansions by presenting DL to the physical layer [12]. DL owns crucial characteristics, such as “deep modularization”, which suggestively develops feature extraction and structure flexibility, associated with conventional ML algorithms. In specific, DL-based systems could be used instead of manual feature extraction to learn features from raw data inevitably and modify the model structures flexibly through parameter tuning to optimize “end-to-end” performance. The DL-based communication system has hopeful applications in complex states for more than a few reasons [13].

Newly, deep learning-based “end-to-end” communication systems have been established for “single antenna multiple antenna”, and “multiuser systems” to expand the performance of the traditional attitudes by mutually enhancing the transmitter and the receiver as an auto-encoder instead of optimizing individual elements both at the “transmitter and receiver”. Auto-encoder is a “DNN” that entails of an encoder that learns a (latent) depiction of the given data and a decoder that recreates the input data from the encoded data.

2. Related Works

2.1 Background

2.1.1Attacks in Wireless Communication

The ad hoc networks have been presented in numerous ways with the rapid development in wireless technology and this kind of networks function in a license free frequency band. They does not necessitate any infrastructure investment, thus makes them more fascinating for certain applications such as military and commercial. There exist several unsolved issues in ad hoc networks and securing the network is the major issue noticed currently. Due to several reasons, these ad hoc networks are vulnerable to attacks. Some of the major reasons include “absence of infrastructure, wireless links between nodes, limited physical Protection, and the Lack of a centralized monitoring or management, and the resource constraints” [14].

“Wormhole Attacks”

The Wormhole attacks could be launched using quite a few modes including the following:

1) “Wormhole using encapsulation”
2) “Wormhole Out-of-Band Channel”

3) “Wormhole with High Power Transmission”
4) “Wormhole using Packet Relay”
5) “Wormhole using Protocol Deviations” [15]

The wormhole attacks could be classifies into three types as per the visibility of the attackers on the route. The three types are given as follows:

a) “Open Wormhole Attack”

In this type of wormhole, the attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbors.

b) “Half open Wormhole Attack”

One side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure [16].

c) “Closed Wormhole Attack”

The attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet [17].

“Replay Attack”

The replay attack generally includes passive imprisonment of the data unit. It also involves its subsequent retransmission to create an unapproved significance [18].This is accepted out by an opponent or by an inventor who intrudes the data and retransmits it.

“Selective Forwarding”

“Timely and Secure” transmission of data in the WSN is its crucial requisite of the network. In these attacks, the malicious schemes act as the normal systems and drop selected packets. In “selective forwarding attack”, the selection of “dropping nodes” could be random [19].

“Node Replication”

In “Node Replication attack”, an opponent makes distinct easily affordable wireless sensor nodes and tricks entire network into accommodating them like the authentic nodes [20]. Node replication is difficult to detect without centralized monitoring.

“Sybil Attack”

In Sybil attacks, a node grants as several” duplicate nodes” using the characteristics of other “authentic nodes”. Sybil attack essentially aims to fault tolerant systems such as “distributed storage and multipath routing” [21]. Sybil attack poses an important risk to “geographic routing protocols”. Position significant routing generally entails different nodes to share data with their adjacent nodes to expertly route the geographically addressed packets.

“Sink Hole Attack”

A malevolent node signifies itself as a “black hole” to demand and catch all traffic particularly in WSNs. An invader snoops requests paths then shows to “targeted systems” that it embraces best eminence or shortest distance to “base station”. Attacker insert itself among the cooperating nodes, it is proficient to make any changes in information passing amongst them [22].

“Rushing Attack”

Rushing attack is a modern threat that frequently outcomes in the “denial-of-service (DoS)” when exploited alongside all former network routing practices. An attacker dispenses the “malicious messages” very quickly to open messages that reach late [23].

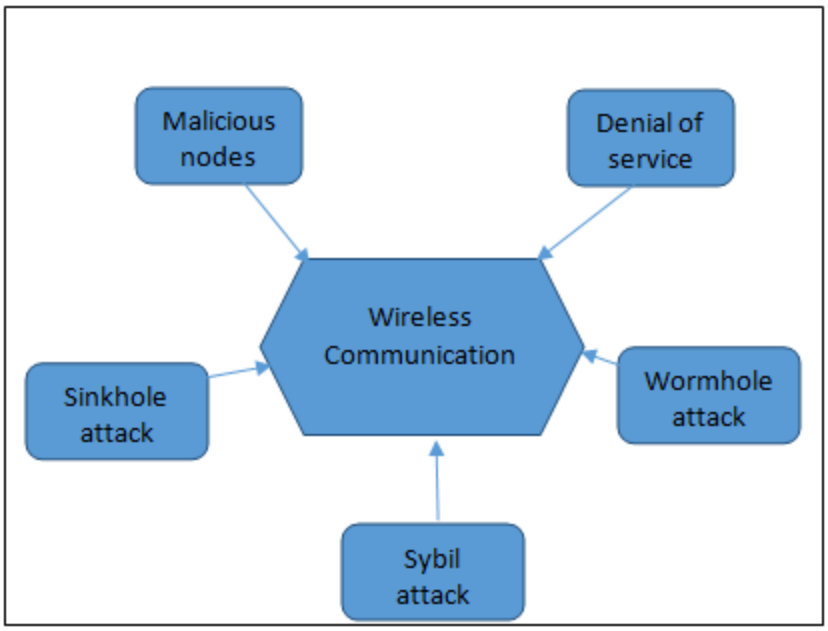

Figure 1 - Security attacks in wireless communication

Proposed Method

3.1 System Model:

In our Hybrid Deep Learning Prediction Model (HDLP), the architecture is based on clustered homogeneous network and it is described in the Figure. At the initial condition the energy values are equally divided to all the nodes in the network. A wireless interface is in cooperated with all the nodes in the network since it is an essential factor for transmission and reception of data. The network coverage area is finalized and the nodes are localized in a 1400m x 1400m area.

3.1.1 Energy Model:

The system energy model is shown in the figure which represents the consumed energy of the nodes during the process of communication. Both the transmitter and the receiver circuit are created and the energy is the core component for this process and it is mentioned as a number of bits (b).

$$E_{Tx/Rx} = E_{elect} \times b \text{ ---------- (1)}$$

Where $E_{elect}$is the major energy component in the network and the energy which is used for the data transfer by an amplifier is the function of the bit count as well as the distance (d).

$$E_{Tx-amp} = \begin{cases} \in_{fs} \times b \times d^2, \text{if } d < d_t \\ \in_{mp} \times b \times d^4, \text{if } d > d_t \end{cases} \text{---------- (2)}$$

Where, d_t is a network threshold value which is used to calculate the free space and the multipath fading model.And the threshold value d_t is calculated as,

$$d_t = \sqrt{\frac{\in_{fs}}{\in_{mp}}} \text{---------- (3)}$$

Where, $\in_{fs}$ = constant value represents free space, $\in_{mp}$= constant value represents multipath model. Then the total transmission energy is evaluated as,

$$E_{Tx} = \begin{cases} \in_{elect} \times b + \in_{fs} \times b \times d^2, \text{if } d < d_t \\ \in_{elect} \times b + \in_{mp} \times b \times d^4, \text{if } d > d_t \end{cases} \text{---------- (4)}$$

3.2 Cluster based Network:

The network is separated into several clusters according to the nodes structure and localization. The node which occupies high residual energy has the highest possibility to become a Cluster Head (CH). After the election of the CH, the nodes which present inside the coverage area of that CH will becomes its Child Nodes (CN). During the transmission the energy values of the CH gets reduced due to the management of data. And in case if the energy value of that CH becomes lower than its threshold value the CH rotation process will be initiated. For the transmission between CH and CN the concepts works inside the MAC layer is dynamic code division multiple access with N bands. This band greatly helps the CHs during communication. Pre-allocated bands are used to monitor the CHs data transmission.

At this condition, the CN or the CH is engaged with any other activity then the attack detection module is initiated. In case if any malfunction is identified then the node or the CH is block-listed. The major parameter which is involved in our HDLP model is received signal strength, message success ratio, data loss ratio, routing overhead. By using this parameters our model identifies the node is malicious or not. The nodes which are identified as malicious they are block listed. Then on the process of communication our model checks that the source node ID is block listed or not. The messages will be automatically dropped if it is in the block list. Dynamic signal strength is maintained by the CH to monitor the CN nodes as well as to reduce the energy consumption in the network. In the network, the major area where the energy is consumed highly are during bandwidth allocation, processing time, likewise the power can be saved if the network is more reliable. The major issue is that the node consumes more energy during the processing time.

The major benefits of our proposed model are given as follows: In our network all the nodes self configured as well as self organized. Because of the usage of the selected routing protocol the lifetime of the network is high. The communication is done with the help of the CH which helps to reduce the energy consumption of the network which likewise increases the network Quality of Service (QoS).

3.3 Frame Pattern

There are several attacks present in wireless communication even if the structure is well designed. The attack which is taken for our research is black whole attack. According to the level of intrusion the deionization of attacker is done. Anomalies creations and misdirection of nodes are the issues created by the black hole attack. This may increase the energy consumption in the network. Our HDLP model is a superior method for attack detection. The major phases of our model are Key management phases, Detection of Attacks and Parameter Details.

3.4 Cluster based Auto Encoding for Key Management:

Figure 2explains the structure of cluster based Auto Encoding process. There are two phases are present in this process which are Generation of Labels and Clustering in Auto-encoding.

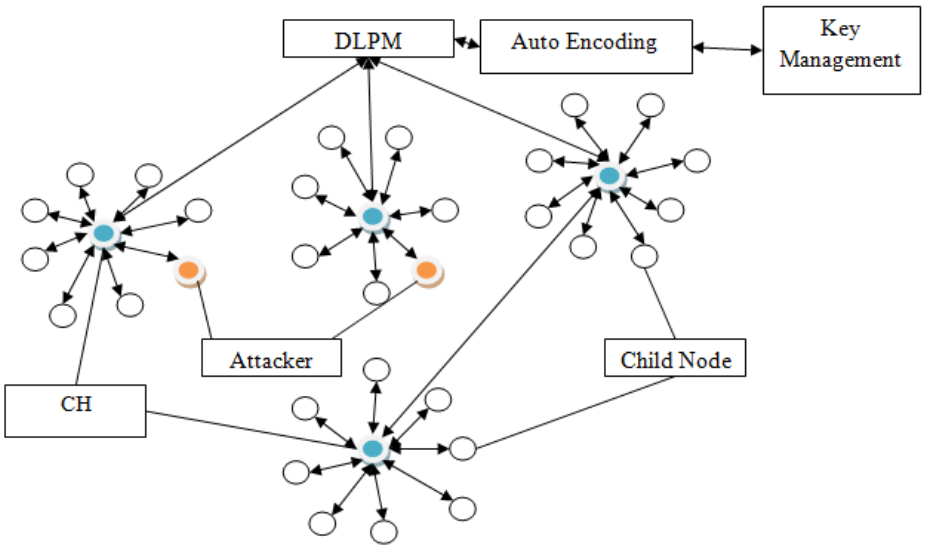

Figure 2 – System Architecture

3.4.1 Phase 1 – Generation of Labels:

- Characteristics and data collection for feature selection to assemble the feature vectors (V_1, V_2, …. V_n) for each and every time slot for data transmission.
- Secondly to selected feature vectors conventional K-Means clustering is applied to recognize the clusters.
- Tags identification using the clusters as labels in all the allocated time slots.
- For the upcoming auto encoding process the collected feature vectors, times slots, tags and labels are used with the help of supervised learning model.

3.4.2 Phase 2 – Clustering in Auto-Encoding:

- Deep Neural Network (DNN) is used for this auto encoding process. DNN works with the help of hidden layers and neurons which is nodes. Here the inner layer nodes are considered as clusters, input layer nodes are considered as feature vectors and the outer layer nodes are considered as labels and data.
- The outer layer nodes are separated into testing and training dataset.
- Primarily training process is initiated into the auto-encoder based deep neural network using the training dataset.
- By the use of trained dataset, testing dataset clusters and labels are predicted.

The primary goal of the encoding process is to find the significant features of the data in each time slot. Then the encoder reduces the features from the selected featured to the most significant features of the data in each time slot. Conversely, the decoder takes that selected most significant features and rebuild to receive that initial value without any lose. Feature spaces are greatly reduced by using this encoding and decoding process then the final features are used for clustering process.

4. Simulation Environment:

In the implementation section, for simulation process we used Contiki which is an open source simulator in order to work in the OS for wide range of deployment in IPv6 stack and that is predefined in Contiki. For network construction 20 nodes used in total and the total number of mobile modes are 5. Likewise by varying the nodes we can able achieve the results of the network. To analysis and prove that our proposed model (HDLPM) is better than others it is compared with the earlier works (DMTL) and (DLDM).

4.1 Accuracy Calculation:

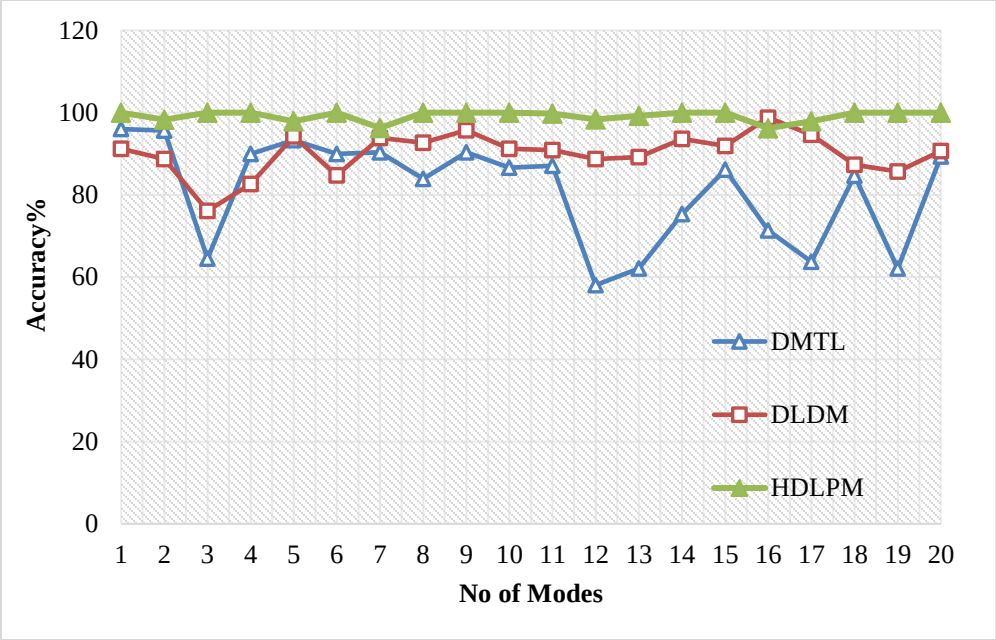

Figure 3 – Accuracy Calculation

Figure 3represents the graphical comparison of the proposed model with the earlier works in terms of Accuracy where x-axis represents the number of modes in the network and y-axis represents the accuracy in percentage. The time interval taken for calculation is 20 seconds. This process greatly increases the accuracy which leads to improve the overall QoS of the network.

4.2 End to end Delay Calculation:

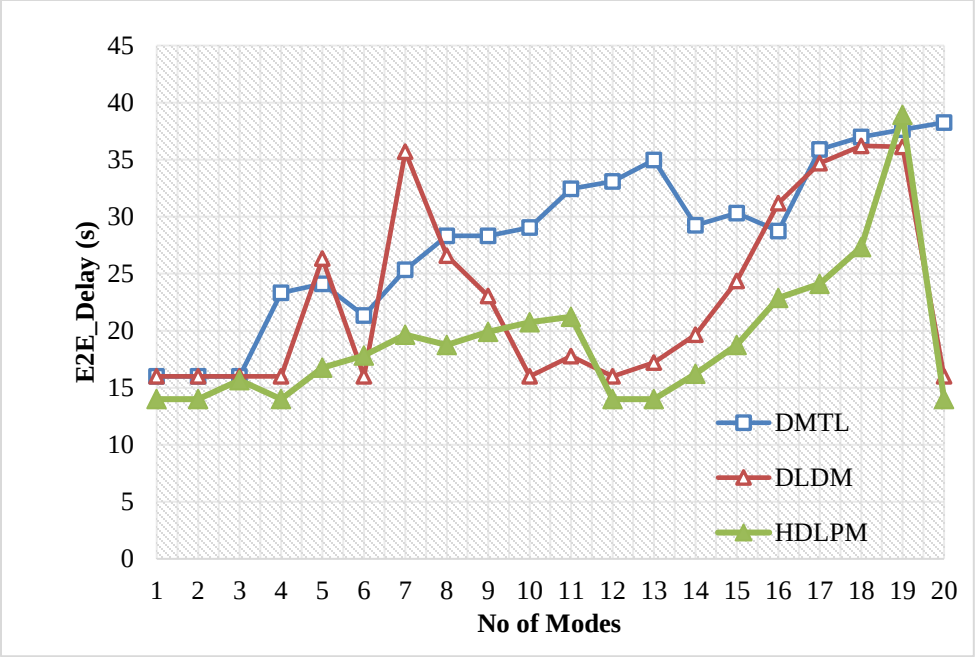

Figure 4 – End to end delay Calculation

The graphical representation of E2E delay calculation is shown in the Figure 4where x-axis represents the number of modes in the network and y-axis represents the delay values. From these results it's understood that our proposed model produces great results in terms of E2E delay when compared with the earlier models

4.3 Energy Consumption Calculation:

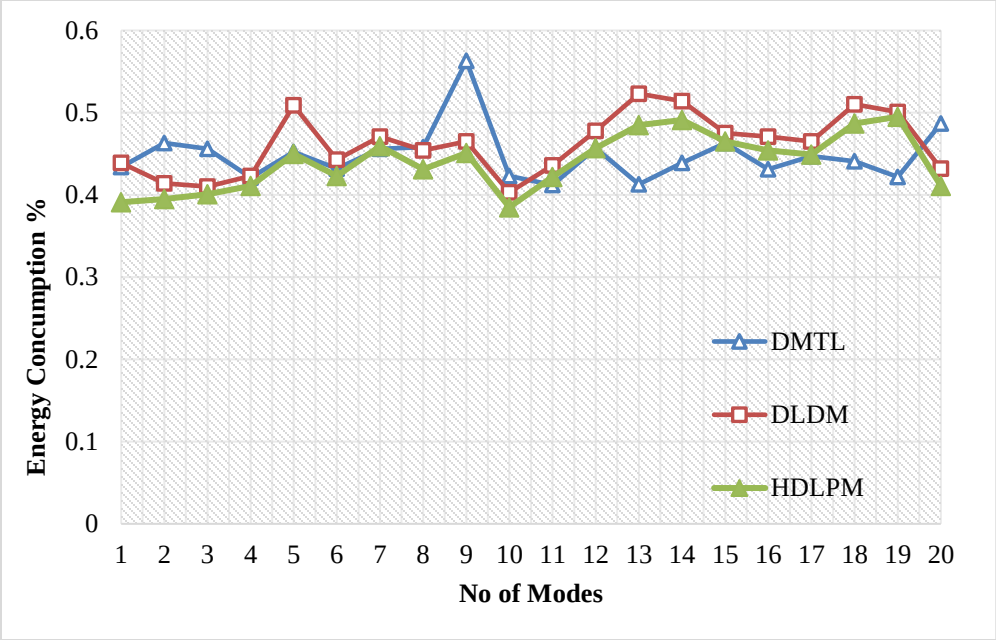

Figure 5 – Energy Consumption Calculation

Network energy consumption is defined as that the energy utilized during the process of communication in the network. The graphical comparison of the proposed (HDLPM) with (DMTL) and (DLDM) is shown in Figure 5. The network energy consumption is calculated in the time interval of 20 seconds. Currently the network is ready to face the improbabilities in it. The process greatly helps to reduce the power consumption in the network compared with the earlier models. The other factors which reduce power consumption are reducing of network overhead by neglecting the additional load during communication. From the graph it's proven that our proposed model plays well when compared with the earlier works.

4.4 Energy Efficiency Calculation:

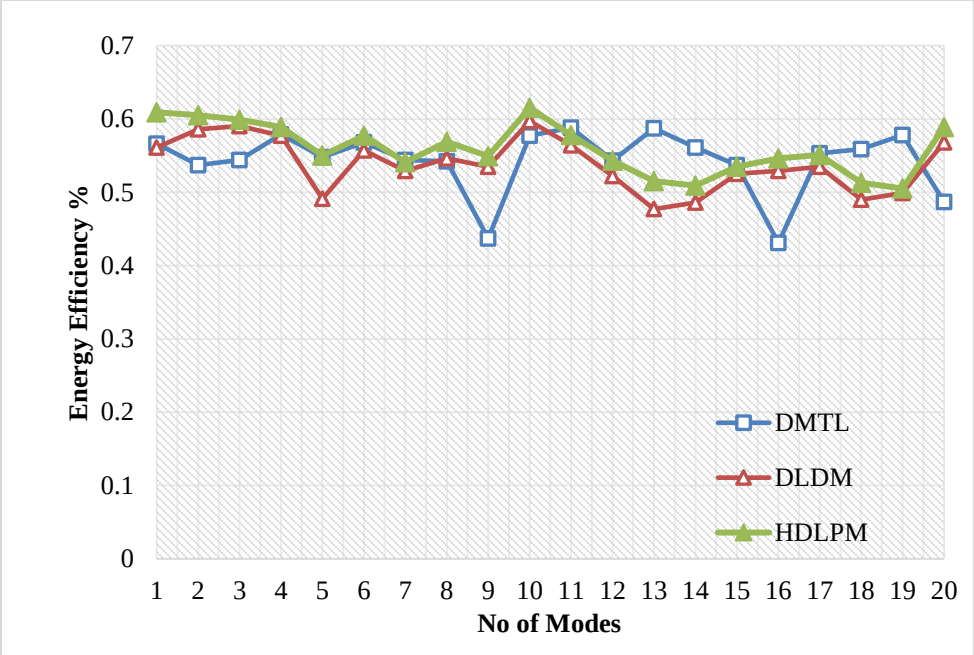

Figure 6 – Energy Efficiency Calculation

The network energy efficiency is referred as that the alive time of each and every node without replacement. The residual energy of each mode is 25 Joules and the time given for the measurement of remaining energy is 20 seconds. During data transfer some of the nodes are declared as dead when it reaches the power below 0.025 Joules. The graphical comparative analysis of the proposed (HDLPM) with (DMTL) and (DLDM) is shown in Figure 6. From these results it's observed that our proposed model produces high energy efficiency when compared with the earlier works. Consequently the lifetime of our proposed model is better than the exiting works.

5 CONCLUSION

Our proposed model is employed to safeguard the network from the black hole attack with the help of clustering model and auto encoding with key managements. The lifetime of the network is greatly increased by the effective utilization of energy in the nodes. Our simulation results are analyzed and compared with the earlier models such as Deep Multi Task Learning (DMTL) and Deep Learning Based Defense Mechanism (DLDM). As the results, we found that our proposed model performed well in terms of Accuracy, End to End Delay, Energy Efficiency and Energy Consumption when compared with the earlier models. For the research continuation our deep learning model can be applied with several optimization techniques to further enhancement.

6 REFERENCES

1. Auletta, V., Moscardelli, L., Penna, P., Persiano, G.: Interference games in wireless networks. In: Papadimitriou, C., Zhang, S. (eds.) WINE 2008. LNCS, vol. 5385, pp. 278–285. Springer, Heidelberg (2008)
2. Avin, C., Emek, Y., Kantor, E., Lotker, Z., Peleg, D., Roditty, L.: SNR diagrams: Towards algorithmically usable SINR models of wireless networks. arXiv:0811.3284v2 (2008)
3. Brar, G., Blough, D., Santi, P.: Computationally Efficient Scheduling with the Physical Interference Model for Throughput Improvement in Wireless Mesh Networks. In: Mobicom (2006)
4. Brar, G.S., Blough, D.M., Santi, P.: The scream approach for efficient distributed scheduling with physical interference in wireless mesh networks. In: ICDCS, pp. 214–224 (2008)
5. Chafekar, D., Kumar, V., Marathe, M., Parthasarathy, S., Srinivasan, A.: Crosslayer Latency Minimization for Wireless Networks using SINR Constraints. In: Mobihoc (2007)
6. Abusalah, L., Khokhar, A., &Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. IEEE communications surveys & tutorials, 10(4), 78-93.
7. Andel, T. R., &Yasinsac, A. (2007). Surveying security analysis techniques in MANET routing protocols. IEEE Communications Surveys & Tutorials, 9(4), 70-84.
8. Z. Qin, H. Ye, G. Y. Li, and B.-H.-F. Juang, “Deep learning in physical layer communications,” IEEE Wireless Commun., vol. 26, no. 2, pp. 93–99, Apr. 2019.
9. N. Samuel, T. Diskin, and A. Wiesel, “Deep MIMO detection,” in Proc. IEEE 18th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC), Jul. 2017, pp. 1–5.
10. H. He, C.-K. Wen, S. Jin, and G. Y. Li, “A model-driven deep learning network for MIMO detection,” in Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP), Anaheim, CA, USA, Nov. 2018, pp. 1–5.
11. R. C. Daniels, C. M. Caramanis, and R. W. Heath, “Adaptation in convolutionally coded MIMO-OFDM wireless systems through supervised learning and SNR ordering,” IEEE Trans. Veh. Technol., vol. 59, no. 1, pp. 114–126, Jan. 2010.
12. S. K. Pulliyakode and S. Kalyani. (2017) Reinforcement learning techniques for outer loop link adaptation in 4G/5G systems. [Online]. Available: https://arxiv.org/abs/1708.00994,preprint.
13. J. Vieira, E. Leitinger, M. Sarajlic, X. Li, and F. Tufvesson. (2017) Deep convolutional neural networks for massive MIMO fingerprintbased positioning. [Online]. Available: https://arxiv.org/abs/1708.06235, preprint.
14. I. Khalil, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless

Networks," in DSN '05: Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05), 2005, pp. 612-621.

15. K. Issa, B. Saurabh, and B. S. Ness, "LiteWorp: Detection and Isolation of the Wormhole Attack in Static Multihop Wireless Networks," The International Journal of Computer and
16. W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending Against Wormhole Attacks in Mobile Ad Hoc Networks," Wiley Journal on Wireless Communications and Mobile Computing, vol. 5, pp. 1- 21, 2005.
17. K. Lee, H. Jeon, and D. Kim, "Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks," in New Technologies, Mobility and Security: Springer Netherlands, 2007, pp. 361-372.
18. Syverson, Paul. "A taxonomy of replay attacks [cryptographic protocols]." Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings. IEEE, 1994.
19. Sharma, Preeti, Monika Saluja, and Krishan Kumar Saluja. "A Review of Selective Forwarding attacks in Wireless Sensor Networks." International Journal Of Advanced Smart Sensor Network Systems (IJASSN) 2.3 (2012): 37-42.
20. Zhu, Wen Tao, et al. "Detecting node replication attacks in wireless sensor networks: a survey." Journal of Network and Computer Applications 35.3 (2012): 1022-1034.
21. Chris Karl of, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier) Page: 299-302, year 2003.
22. Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu. "On the intruder detection for sinkhole attack in wireless sensor networks." 2006 IEEE International Conference on Communications. Vol. 8. IEEE, 2006
23. Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Rushing attacks and defense in wireless ad hoc network routing protocols." Proceedings of the 2nd ACM workshop on Wireless security. ACM, 2003.