Development of Secured Memory Efficient CloningDetection Protocol in WSNS Using RSA Algorithm

Pranav Pradip Chippalkatti[1]
Research Scholar VTU RRC Belagavi

Swagat Madhav Karve[2]
Research Scholar VTU RRC Belagavi

Rajesh Maharudra Patil[3]
Co-Supervisor, VTU RRC Belagavi

Dr. Nagaraja[4]
B.G. Jain Institute of Technology,
Devanagere

Abstract

This paper is related to the developing an improvised of secured memory efficient cloning detection protocol in WSNs using RSA Algorithm and is used for efficient transfer of data packets with security. NS2 is usedas the simulation tool to simulate the outputs. The main aim or objective of the proposed work presented in this paper is to develop a secured memory efficient cloning detection protocol in the mobile adhoc wireless sensor networks. The simulation results shows the effectivity of the methodology that is being proposed by us.

I. Introduction

It is a well-known fact that the WSNs are being used widely & deployed for a large range of applications from monitoring the environment to medical applications, space applications, tracking of objects, etc… In this paper, a routing protocol which is efficient in energy and cloning aware detection procedure is being developed that too in a densely populated areas. Here, the WSN developed can detect successful cloning attacks on the WSN and hence the lifetime of the network can be increased [1][2][3].

A ring like structure can be developed and this could be used to facilitate an energy efficient data which can be forwarded along the path towards the sink sensor nodes. The sensor's location information and the witnesses which are there in the WSN can randomly be selected which are located in a ring like structured area in order to verify the legitimacy of the sensor

network. In this context, the detected clone attacks can also be detected and reported to the base station. The hubs in the network system needs to transmit the information, it initially sends the solicitation request to the observers (witnesses) for authenticity confirmation, and these witnesses will report an identified assault/attack if the hub node fails to certify in this context [4][5][6].

For productive & efficient detection of the clone & its location, typically, a lot of nodal hubs are chosen, in the sense selected, which are called observers or witnesses, to help confirm the authenticity of the nodal hubs in the wireless network system. In order to achieve a very good successful rated detection of clone, selection of the witnesses and verification of the legitimacy verification should satisfy 2 important requirements, they are

1. Random selection of the witnesses

2. One witness should successfully receive all the verified messages

for the detection of the clone [7][8][9].

Here, we have used the RSA Algo (Rivest–Shamir– Adleman) which is an algorithm that is used by the current generation computers for encrypting & decrypting of the datas. This RS Algo is used to avoid the collision attacks and device a secured robust clone detection process. As a result of this proposed concept, one can avoid the attacks and eliminate them by the use of some malicious sensor nodes. In the work proposed, we have got 100 percent probability detection using trusted witnesses. The secured protocol can achieve a very long network life time by the effective distribution of the traffic load throughout the *m*- WSN [10][11][12].

II Background work done by the researchers

Quite a number of researchers have worked on the chosen research topic in this paper. Few of them are being addressed here. Y. Xuan, Y. Shen, N.P. Nguyen, and M.T. Thai did some studies on the clone detection protocols & in the literature, this can be classified into two different categories, i.e., centralized and distributed clone detection protocols. In centralized protocols, the sink or witnesses generally locate in the center of each region, and store the private information of sensors. When the sink or witnesses receive the private information of the source node, they can determine whether there is a clone attack by comparing the private information with its pre-stored records. Normally, centralized clone detection protocols have low overhead and running complexity. However, the security of sensors' private information may not be guaranteed, because the malicious users can eavesdrop the transmission between

the sink node and sensors. Moreover, the network lifetime may be dramatically decreased since the sensor nodes close to the sink will deplete their energy sooner than other nodes [13][14][15].

The authors, M. Conti, R.D. Pietro, L. Mancini and A. Mei worked on the distributed clone detection protocols, a set of witnesses are selected to match with every sensor which prevents the transmission between the sink and sensors from being eavesdropped by malicious users. There were 3 different types of witness selection schemes in distributed clone detection protocols, viz.,

❖ deterministic selection,

❖ random selection, and

❖ semi random selection.

The deterministic witness selection based clone detection protocols like RED choose the same set of witnesses for all the sensor nodes. By using of the deterministic witness selection, a low communication overhead and a high clone detection probability can be achieved. In addition, the required buffer storage capacity of such protocols is very low, which is only related to the number of witnesses without considering network scale and node density [16][17][18].

In another research work done, a team of networking researchers led by Y. Zeng, J. Cao, S. Zhang, S. Guo and L. Xie did extensive research work on the enhancement of the network security, the distributed clone detection protocols with random witness selection like LSM were proposed in their work, which were closely related to our work. In random witness selection, it is difficult for malicious users to acquire the information of witnesses since the witnesses of each sensor are randomly generated [19][20][21].

However, the randomness of mapping function also increases the difficulty for the source node to reach its witnesses, which makes it challenging to achieve a high clone detection probability. To ensure the clone detection probability, LSM lets all the nodes in the route between source and witnesses store the private information of the source node, which leads to a high requirement of data buffer and energy consumption. Thus, it is essential to guarantee the clone detection probability with low energy consumption and required buffer storage in clone detection protocols with random witness selection approach [22][23][24].

Research engineers, M. Zhang, V. Khanapure, S. Chen and X. Xiao did an extensive research on the distributed clone detection protocols, such as Parallel Multiple Probabilistic Cells (P-MPC) & the quad let proposed a semi-random witness selection approach trying to combine the advantages of both random and deterministic witness selection approaches. In this kind of witness selection scheme, a deterministic region is generated for the source node according to the mapping function, and then witnesses of the source node will be randomly selected from the sensors in this region. However, the two-phases witness selection and randomness of the witnesses for each sensor leads to a high overhead and time complexity. The energy consumption and the required buffer storage of such protocols are lower than the random witness selection approach but higher than the deterministic ones [25].

III   Existing System

In most of the existing clone detection protocols such as Randomized Efficient and Distributed protocol (RED) and Line-Select Multicast protocol (LSM), the required buffer storage size depends on the network node density, i.e., sensors need a large buffer to record the exchanged information among sensors in a high-density WSN, and thus the required buffer size scales with the network node density. Such requirement makes the existing protocols not so suitable for densely-deployed WSNs. Most existing approaches can improve the successful clone detection at the expense of energy consumption and memory storage, which may not be suitable for some sensor networks with limited energy resource and memory

storage. Quite a number of dis-advantages exist, to list, some of them are

❖ High energy consumption

❖ More memory storage

❖ Not be suitable for some sensor networks with limited energy resource and memory storage.

❖ The required buffer storage of sensors is usually dependent on the node density

IV Proposed System

In order to overcome the drawbacks of the existing system, a new method of securing and avoiding the clone attack is proposed in this paper. Besides the probability of clone detection, also the energy consumption and memory storage in the design of clone detection protocol is considered in the research work, i.e., an energy & memory efficient distributed clone detection routing protocol using some random witness selection concepts are used in the wireless sensor networks. The work done here is applicable to any type of general densely populated sensor nodes that too in multi-hop sensor nets [26][27][28].
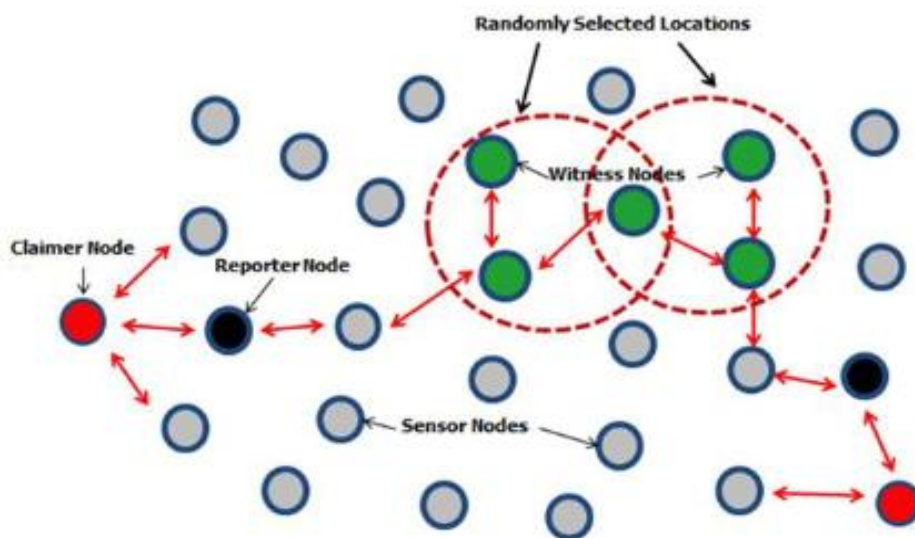

Fig. 1 : Architectural layout of the security in cloning detection WSNs [42]

Adversaries may be required to compromise for the clone sensor nodes for launching of the phishing attacks. An energy efficient *ring type cloning detection* procedure is developed as shown in the Fig. 1 [42], which is done in order to achieve high degree of detection probability. This used some random node selection as the witnesses. At the same time, normal network operations with good network life time can be achieved using this concept where the entire work is being divided into 2 stages, viz., selection of the witness & verification of the legitimacy as shown in the Fig. 2 [42].
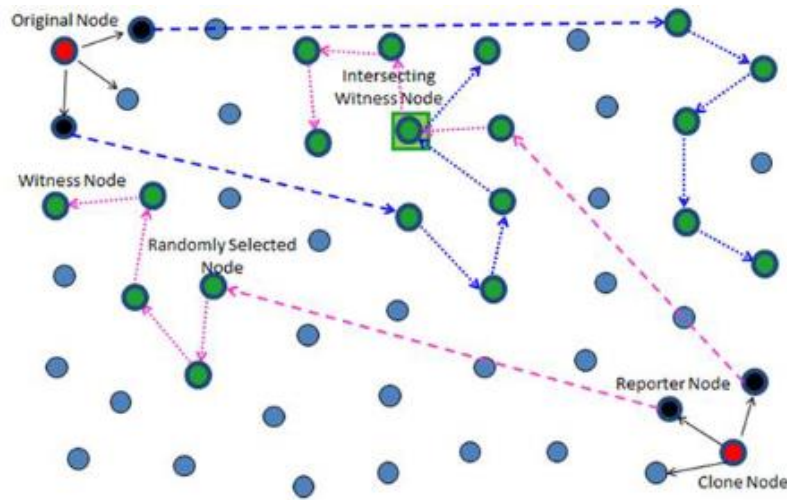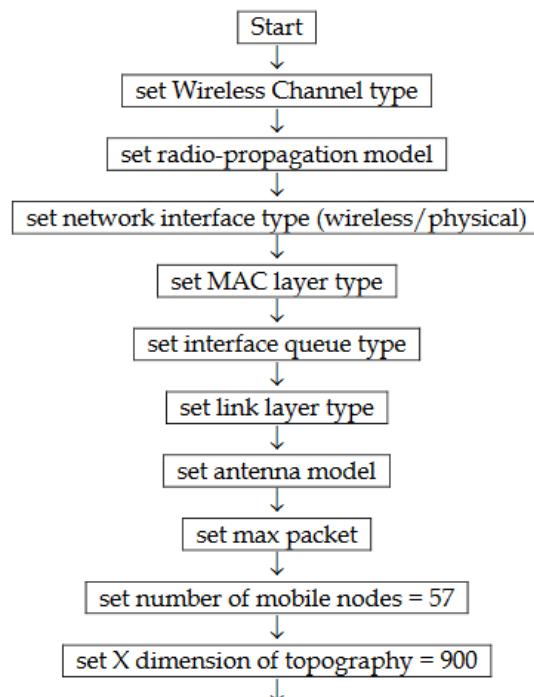
Fig. 2 : Working principle of the security in cloning detection WSNs [42]

In the former case, the source node (S) sends a private info/data to a set of witness nodes, say hello packets and these witness nodes are selected randomly by the use of a mapping function. In the latter case, the verification message along with the private data of the source node (S) will be transmitted to all the witnesses' nodes (W). Suppose if any of the witness node receives the message successfully, the witness node (W) will forward the message to its witness node header for verification. Once the key (similar to the OTP) is given, it will take the message packet and forward to another, else it will not. This is how the data is secured and the process of legitimate verification is shown in the Fig. 4 [43].

V Data Flow Diagram / Flow – Chart

```
set Y dimension of topography = 550
        ↓
Set simulation time = 50 ms
        ↓
set time of simulation
        ↓
Create a NS simulator
        ↓
Set up topography object
        ↓
Set up GOD node system
        ↓
Open NS trace file
        ↓
Open the NAM trace file
        ↓
Mobile node parameter set-up
        ↓
Define the nodes
        ↓
Assign sensor node positions
        ↓
Set up instance of simulator
        ↓
Create a constant bit rate (CBR) system
attach it to the node
        ↓
Attach CBR source to sink
        ↓
Calculate neighbour node
Euclidean distance calculation
        ↓
Broadcast the information
        ↓
Witness the selection process
        ↓
Network witness head selection process
        ↓
Packet forwarding process
        ↓
Detect the clones
        ↓
Avoid the clones
        ↓
Authenticate key action
        ↓
Transfer data securely
        ↓
End
```
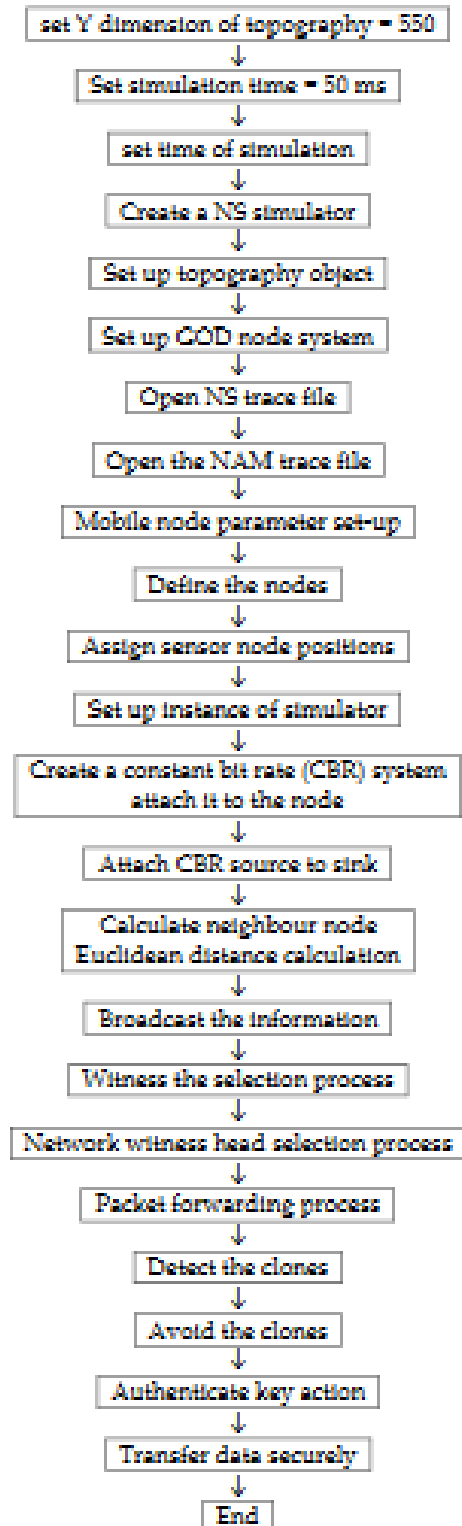
Fig. 3 : Flow chart of the proposed coding process in the secured clone detection efficient energy routing protocol

VI Procedure

Once the witness node receives the hello data packet message, the witness header will compare the aggregated verified messages with the records which are stored. Suppose if there are multiple copies of verification messages which were received by the witness node, then the clone attack is

detected by the node and a revocation process has to be set into action. There are a few existing iterative filter algos, while fundamentally more strong against arrangement collision attacks by the malicious or phishing nodes, than the straightforward averaging techniques, are all things considered susceptive to a novel advanced collision attack concepts we present here in this paper [29][30][31].

An improvement for RSA security algo is proposed in this context by addressing & implementing the security issue. The algo developed could be utilized in getting private & public keys as the RSA algo uses the multiplication of 2 large prime numbers and thus this RSA algo could be used for encryption, decryption as well as for authentication purposes. It has to be noted in this context that the keys that are used for encryption & decryption are both different. One pair of numbers, say (e,N) is actually called as the public key & is known to all, i.e., public like a global variable [32][33][34].

Another pair of numbers say, (d,N) is called as the private key or the confidential key and this has to be kept secret at any cost and this will be used for the decryption of the text that had been encrypted with the public keys. Note that our developed algo has 3 important steps, viz., generation of the key, key encryptions & key decryptions. The work proposed has got a wide number of advantages such as - it achieves high degree of clone detection probability with random witness node selections, can achieve superior performance in terms of the WSN's n/w life time with good data buffering & finally the actual number of buffer storage sensors is independent of the sensor nodes, but will be a function of the hop length of the WSN's radii h, i..e, $O(h)$ [35][36][37].

Probability of clone detection is achieved as follows. Note that in the distributed type of clone detection like the one considered in our work with random witness sensor node selection, the clone detection probability actually refers to whether the witness node can successfully receive the VFN info or not. The probability of clone detection is defined as the probability that the verification info can be transmitted successfully from S to W sensor nodes. In the routing protocol designed, the VFN message is actually broadcasted when it is near the witness node rings in order to guarantee the security of the WSN. It is proved in our case that at least 1 of the witness node could receive the message, viz., the clone attack can be detected with 1 probability. This is how the clone detection is designed in our research work [38][39][40].
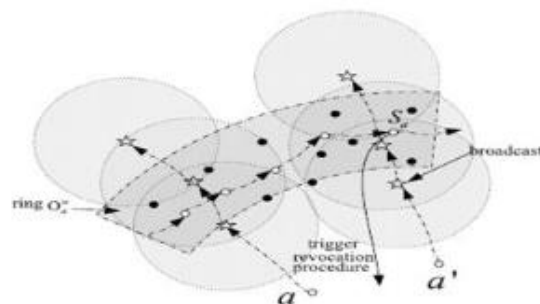

Fig. 4 : Legitimate verification procedure of the S, D, W nodes [33]

VII NS-2 Simulation Results

In this research work, we have proposed a secured memory efficient cloning detection protocol in

the mobile adhoc wireless sensor networks using encryption, decryptions keys & by the use of the RS algorithm. The coding (script writing) for the development of a wireless sensor networks for efficient data transfer schemes is developed in the .NS2 tool by writing .tcl scripts and once it is completed, it is tested for its effectiveness as per the algo steps given below as per the flow chart shown in the Fig. No. 3. The following specs are used in the simulation process. The sensor network of 57 nodes will be deployed in a dimension of (900×550) m^2. The source will be located in the centre of the networking field. The transmitting antenna range is 50 meters. It has to be noted that the sensor nodes will be moving in the random direction with a minimum speed of 1 m/s upto 5 m/s. The simulation time interval is taken as 50 ms [41][42][43].

Next, the developed code is saved in a particular folder in the Ubuntu environment. The Ubuntu is started next. At the terminal, commands like sudo –s is being used to enter the kernel. The password is being set. Next, the source code in which the directory / folder is present is changed using cd command. The developed code is run using ns filename.tcl. The command window of the NS-2 simulator appears with the simulator start button along with the network animator. Once the simulation is started, the node deployment appears on the NS-2 animator screen as shown in the Fig. 4 along with the 2 malicious & attacking phishing nodes. Here, we have taken the value of n = 57 with number of active sensor nodes as 55, remaining 2 are the attacker nodes, which can be seen from the Fig. 5 [41].

The proposed algorithm developed is incorporated in the .tcl file in the NS2 environment. The coding is developed in such a way that 57 sensor nodes are deployed in the network similar animator window, the code pattern can be observed in the flow chart shown in the figure 3. The data transfer starts from the source node by sending "hello" packets to the sink via the nodes as shown in the Figs. 5 – 9 respectively. Once the data transfer starts, attacker nodes starts attacking in the middle & starts to steal the information by using phishing nodes, but the proposed algorithm immediately identifies which nodes has been attacked by the attacker, ensures the keying is done in a proper manner and immediately makes the effect of attacking node on the attacked node ineffective and the normal process of the data packet transfer starts [41].

In the work considered, first verification of the keys is done first step by step starting from n = 2 & ending with n = 55. Simulation takes couple of minutes, passes different stages of data packets [44][45][46]

❖ sending,
❖ verification,
❖ encryption,
❖ decryption,
❖ cloning,
❖ witness node selection,
❖ witness node header selection,
❖ key verification process

until the sink or destination node. The simulation step size is taken as 50 ms. Once the data transfer is fully successful, the final step is to observe the simulated results from the NAM window command prompt by using the commands chmod 777 results.sh & running the shell script

./results.sh & the plots of throughput, packet delivery, packets drop, etc… are plotted & the results are analyzed from which we can come to a conclusion that the proposed work done is better compared to the others, thus establishing the supremacy of the proposed work [47][48][49].
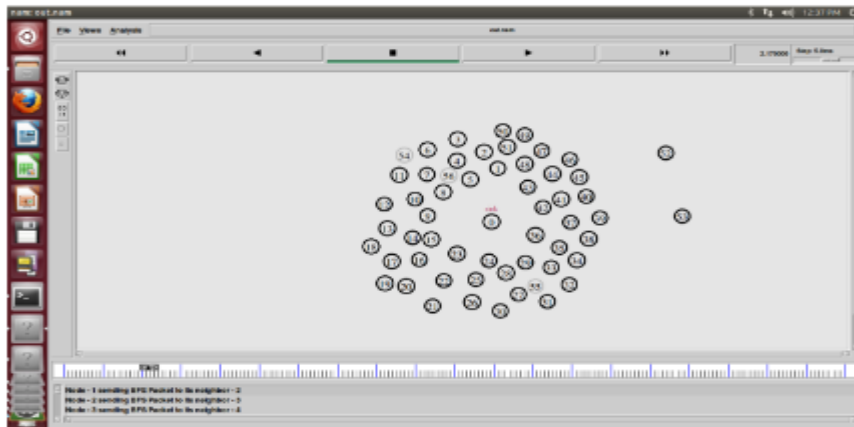

Fig. 5 : Initial deployment of the 57 nodes with the 2 attacking or malicious nodes (52 & 53)
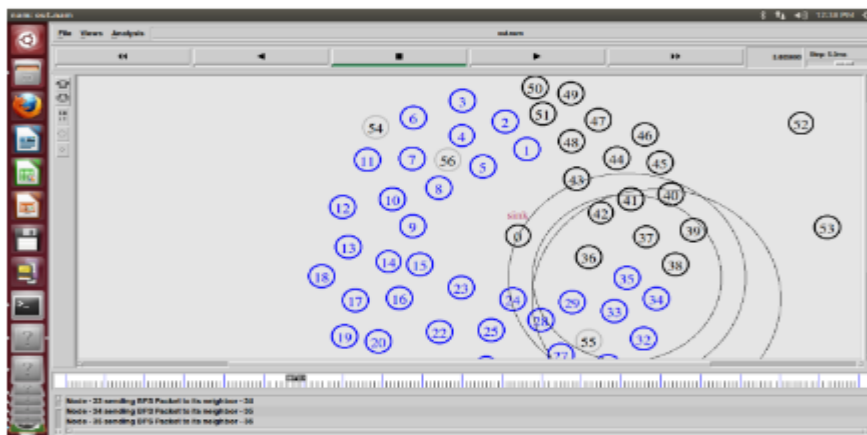

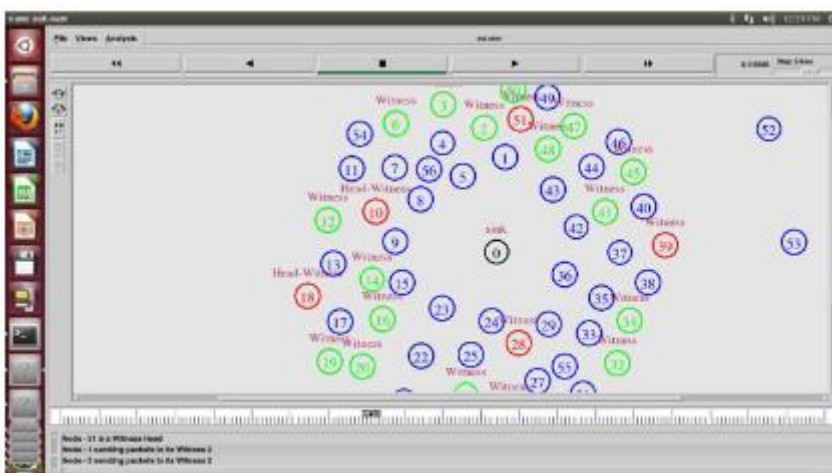Fig. 6 : Data transfer process (shown in concentric circles)

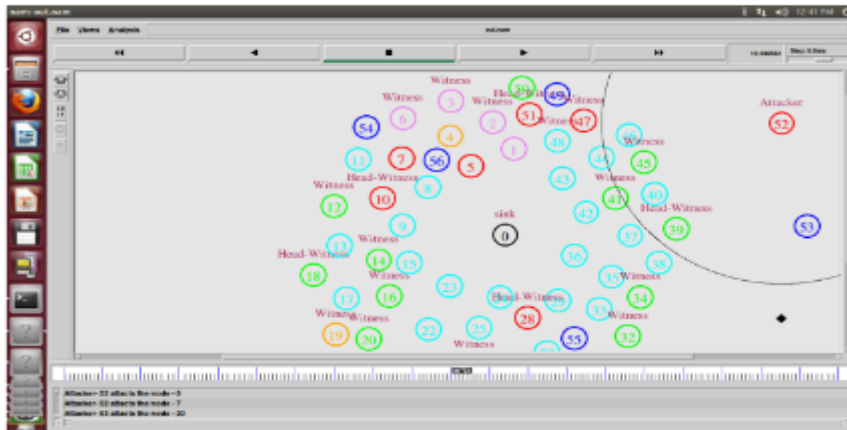Fig. 7 : Some of the nodes acting as the witness nodes

Fig. 8 : Some of the nodes acting as Head-Witness along with attacker nodes dropping off the data packets
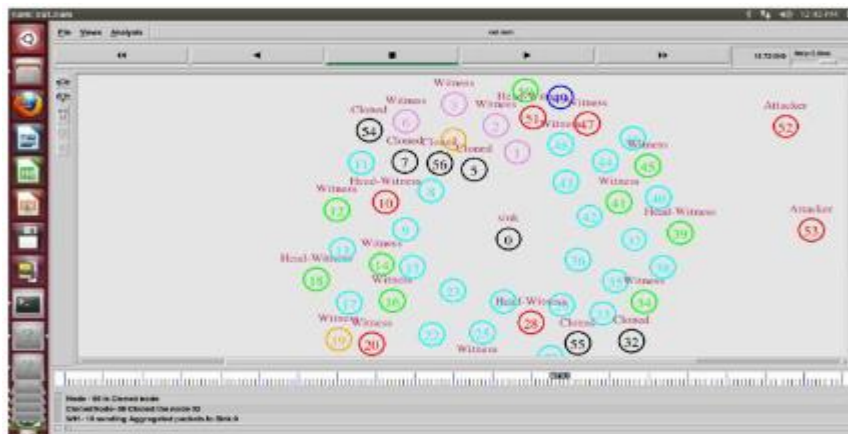

Fig. 9 : Some of the nodes that have been cloned during the process of attack by the malicious nodes (Cloned nodes shown in the black colour)

Fig. 10 : Structure of the main program "main.tcl" showing the syntaxes, blue shows the steps involved in the development of the code

The simulation result shown in the Fig. 11 gives a brief idea about the life of the network vs. the number of nodes in the wireless sensor network. The proposed work (red colour) is compared with the work done by the other authors by using the MPCL protocol (green colour) which shows that our method is far better than MPCL method, thus showing the profoundness of our method. The network life time (months) is excellent compared to the other methodology [50][51].

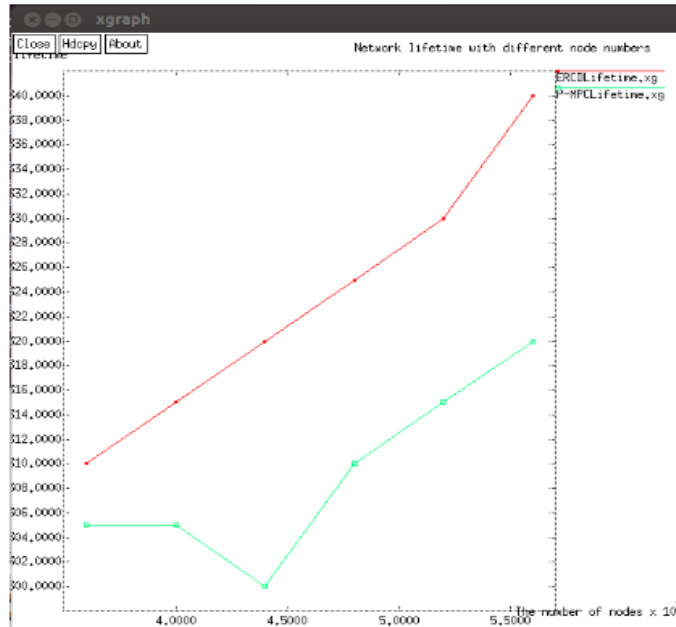Fig. 11 : Plot of network life time with different sensor code numbers vs. the no. of nodes
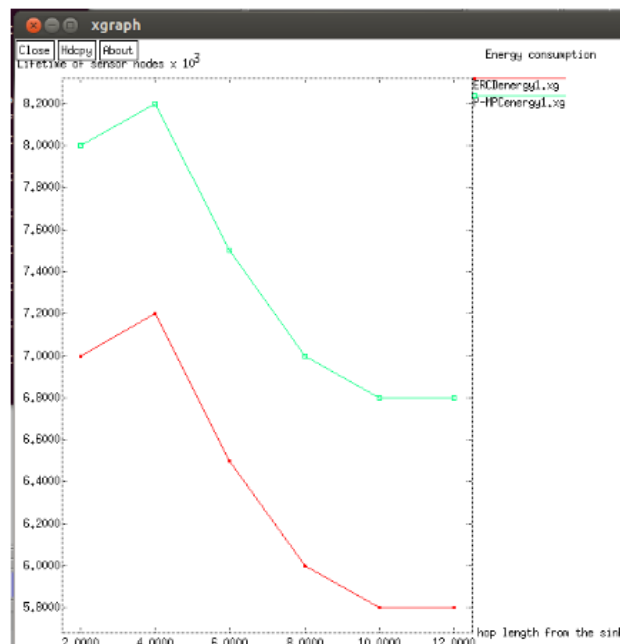

Fig. 12 : Plot of average energy vs. the hop length from the sink node

The simulation result shown in the Fig. 12 gives the graph of average energy vs. the hop length from the sink in the wireless sensor network. The proposed work (red colour) is compared with the work done by the other authors by using the MPCL protocol (green colour)

which shows that our method is far better than MPCL method, thus showing the profoundness of our method. The average energy consumption is excellent, very low compared compared to the other methodology. It shows that the hop length from the sink node increases, the energy consumption of the proposed method decreases far better than the other method [4][5][6].
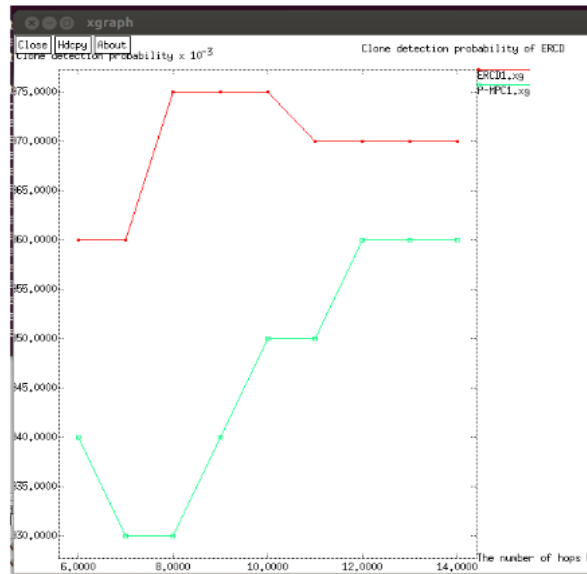
Fig. 13 : Plot of the clone detection probability vs. the number of hops

The simulation result shown in the Fig. 13 gives the graph of clone detection probability vs. the number of hops in the wireless sensor network. The proposed work (red colour) is compared with the work done by the other authors by using the MPCL protocol (green colour) which shows that our method is far better than MPCL method, thus showing the profoundness of our method. The probability of the clone detection in the proposed method is very significant, very high compared to the other methodology. It shows that the number of hops from the sink node increases, the clone detection probability varies but is more significant than the other method [1][2][3].
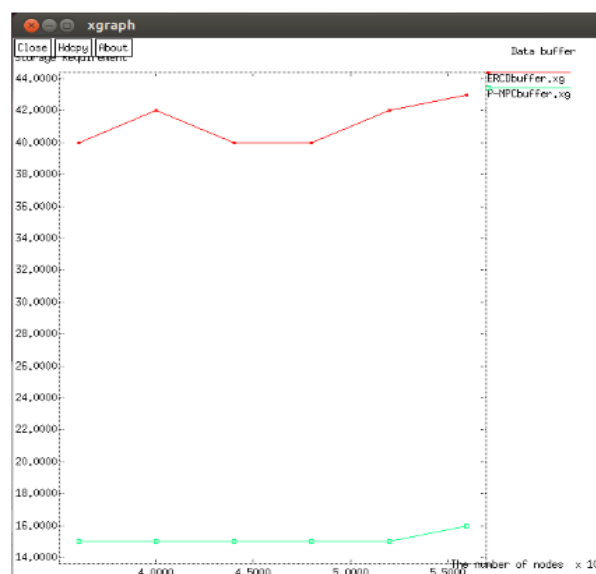

Fig. 14 : Plot of the data buffering vs. the number of nodes in the wireless sensor network

The simulation result shown in the Fig. 14 gives the graph of data buffering vs. the number of nodes in the wireless sensor network. The proposed work (red colour) is compared with the work done by the other authors by using the MPCL protocol (green colour) which shows that our method is far better than MPCL method, thus showing the profoundness of our method. The data buffering or the storage requirement in the proposed method is very significant, very high compared to the other methodology. It shows that the data buffering is varying, but very high compared to the other method [7][8][9].

VIII Conclusions

In this paper, the development of secured memory efficient cloning detection protocol in adhoc mobile wireless sensor networks using RS algorithm is presented. Simulation was carried out for 50 ms & 4 performance characteristics were plotted. From the performance characteristics of the network life time with different sensor code numbers vs. the no. of nodes, average energy vs. the hop length from the sink node, clone detection probability vs. the number of hops, data buffering vs. the number of nodes in the wireless sensor network, it can be observed that the proposed system is faring better compared to the work done by others, thus showing the efficacy of the methodology developed by us. A routing protocol which is efficient in energy and cloning aware detection procedure is being developed that too in a densely populated areas. The main application of the WSN routing protocol developed can detect successful cloning attacks on the WSN and hence the lifetime of the network can be increased, which could be observed from the simulated results.

References

[1] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, J. Lopez, "A novel key update protocol in mobile sensor networks", *Proc. 8th Int. Conf. ICISS*, Vol. 7671, pp. 194–207, 2012.

[2] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks", *MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force*, ISBN : 0-7803-7225-5, pp. 1- 5, August 2002.

[3] T. Hayes and F.H. Ali, "Location aware sensor routing protocol for mobile wireless sensor networks", *IET Wireless Sensor System*, ISSN 2043-6386, pp. 49-57, Jan. 2016.

[4] M. Kalantari and M. Shayman, "Energy efficient routing in wireless networks", *CISS*, pp. 1- 15, March 2004.

[5] N.A. Pantazis, S.A. Nikolidakis and D.D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey", *IEEE Communications Surveys & Tutorials*, Vol. 15 , Issue 2, pp. 551- 591, 2nd Quarter 2013.

[6] G. Kaur, "Reliability of wireless sensor networks", *International Journal of Advanced Research in Computer Engineering & Technology* (IJARCET), Vol. 3, pp. 1926-1928, May 2014.

[7] C. Karlof and D. Wagner, "Secure Routing in wireless sensor networks: attacks and countermeasures", *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, ISBN: 0-7803-7879-2, pp. 293-315, Jun. 2003.

[8] A.S. Pathan, H.W. Lee, C.S. Hong, "Security in WSNs: Issues & Challenges", *ICACT2006, MIC and ITRC Project ISBN 89- 5519-129-4*, 20-22, pp. 1043-1048, Feb.

2006.

[9]   M.U. Aftab, O. Ashraf, M. Irfan *et.al*., "A review study of wireless sensor networks and its security", *Journal of Communications and Network*, *SciRes*, pp. 172-179, Oct. 2015.

[10]   P. Sherubha and M.M Priya, "A detailed survey on security attacks on wireless sensor network and its communication", *Int. Journal of Soft Computing*, Vol. 11, No. 3, pp. 221-226, ISSN: 1816-9503, 2016.

[11]   N.A. Alrajeh, S. Khan, B. Shames, "IDS in wireless detector networks : A Review", *Int. Journal of Distributed Detector Network*, pp. 1-7, April 2013.

[12]   G. Kalpana, T. Bhuvaneswari, "A Survey on Energy Efficient Routing Protocols for Wireless Sensor Networks", *2nd National Conference on Information and Communication Technology* (NCICT), 2011.

[13]   Mohammad Masdari1 and Maryam Tanabi, "Multipath Routing protocols in Wireless Sensor Networks: A Survey and Analysis", *Int. Jour. of Future Generation Communication and Networking* Vol. 6, No. 6, pp.181-192, 2013.

[14]   K. Vinoth Kumar, S. Karthikeyan, "Multi-hop Energy Efficient Reliable and Fault Tolerant Routing Protocol for Wireless Sensor Networks", *Int. Jour. of Emerging Tech. &Advanced Engg, IJETAE*, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2, February 2013.

[15]   Ning Sun, Young-bok Cho, Sang-ho Lee, "A Distributed Energy Efficient and Reliable Routing Protocol for Wireless Sensor Networks", *IEEE International Conference on Computational Science and Engg.*, CSE/I-SPAN 2011.

[16]   Ali Norouzi, Faezeh Sadat Babamir, Abdul Halim Zaim, "A Novel Energy Efficient Routing *Protocol in Wireless Sensor Networks*", IEEE 2011.

[17]   Satvir Singh, Meenaxi, "A Survey on Energy Efficient Routing in Wireless Sensor Networks", *IEEE Transactions*, Vol. 3, Issue 7, July 2013.

[18]   Monica R Mundada, Savan Kiran, Shivanand Khobanna, Raja Nahusha Varsha and Seira Ann George, "A study on energy efficient routing protocols in wireless sensor networks", *International Journal of Distributed and Parallel Systems* (*IJDPS*) Vol. 3, No. 3, May 2012.

[19]   Ahmed Ali Saihood, Rakesh Kumar, "Enhanced Location Based Energy-Efficient Reliable Routing Protocol for Wireless Sensor Networks", *International Journal of Inventive Engineering and Sciences* (*IJIES*) ISSN: 2319–9598, Volume-1, Issue-6, May 2013.

[20]   S. Gupta and K.C. Roy, "Comparison of different energy minimization techniques in wireless sensor network," *International Journal of Computer Applications*, Vol. 75, No. 18, pp. 20–26, 2013.

[21]   N.A. Pantazis, S.A. Nikolidakis, and D.D. Vergados, "Energy efficient routing protocols in wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 2, pp. 551–591, 2013.

[22]   Muhammad Nadeem Akhtar, Arshad Ali, Zulfiqar Ali, Muhammad Adnan Hashmi, Muhammad Atif, "Cluster Based Routing Protocols for Wireless Sensor Networks: An Overview*", International Journal of Advanced Computer Science and Applications*

(IJACSA), Vol. 9, No. 12, 2018.

[23] Singh S.K., Singh M.P. & Singh, Dharmendra, "A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks", *International Journal of AdvancedNetworking and Appn.* (*IJANA*), Vol. 2, pp. 570-580, 2010.

[24] Bilal Jan, Haleem Farman, Huma Javed, Bartolomeo Montrucchio, Murad Khan and Shaukat, "Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey", *Hindawi Wireless Communications and Mobile Computing*, Vol. 2017, Article ID 6457942, 14 pages, 2017.

[25] Gajendran Malshetty, Basavaraj Mathapati, "WSN Clustering Based on EECI (Energy Efficient Clustering using Interconnection)", *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), *Published By: Blue Eyes Intelligence Engineering & Sciences Publication*, ISSN: 2278-3075, Vol. 9 Issue 1, pp. 3564, Madhya Pradesh, India, Nov. 2019.

[26] Pavithra G.S., Babu N.V., "Energy Efficient Hierarchical Clustering using HACOPSO in Wireless Sensor Networks", *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*) ISSN: 2278-3075, Vol. 8 Issue 12, pp. 5219-5225, October, 2019.

[27] Thesiya Khushbu , Viraj Daxini, "Novel Clustering Approach to Reduce Energy Consumption in Wireless Sensor Network based on LEACH", *International Journal of Computer Science and Mobile Computing*, Vol. 4 Issue 6, pg. 945-953, Jun. 2015.

[28] A. Babu Karuppiah, J. Dalfiah, "An Improvised Hierarchical Black Hole Detection Algorithm In Wireless Sensor Networks", *IOSR Journal of Electronics and Communication Engineering* (*IOSR-JECE*) e-ISSN: 2278- 2834,p- ISSN: 2278-8735, (ICEICT 2016), Second International Conference on Electrical, Information and Communication Technology, pp. 134-141, 2016.

[29] Ganesh, "Efficient and secure routing protocol for wireless sensor network", *Ph.D. Thesis*, *Sathyabama University*, Jeppiaar Nagar, Chennai-119, India, August 2014.

[30] Rajesh Kumar Varun, R.C. Gangwar, "Hierarchical Energy Efficient Routing in Wireless Sensor Networks and its Challenges", *International Journal of Engineering and Advanced Technology* (*IJEAT*), ISSN: 2249 – 8958, Vol. 9 Issue1, pp. 4024-4027, Oct. 2019,

[31] Anil. G.L, J.L. Mazher Iqbal, "Implementation of Secure Energy Efficient Network Priority Routing (SEENPR) Protocol with Secure Key Management in WSN", *International Journal of Recent Tech. and Engg.* (*IJRTE*), ISSN: 2277-3878, Vol. 8, Issue 2S11, pp. 3096-3103, Sep. 2019.

[32] Anand Nayyar, "Improvised Energy Efficient Routing Protocol based on Ant Colony Optimization (ACO) for Wireless Sensor Networks", *Ph.D. Thesis*, *Department of Computer Science Desh Bhagat University*, Mandi Gobindgar, Punjab, 2017.

[33] Musheer Vaquar, Sanjay Kumar Agarwal, "HETRP: High Energy Efficient Trustable Routing Protocol for Wireless Sensor Network International", *Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), ISSN: 2278- 3075, Vol. 9 Issue 3, pp. 1034-1042, Jan. 2020.

[34] S. Ganesh and R. Amutha, "Efficient and Secure Routing Protocol for Wireless Sensor

Networks through Optimal Power Control and Optimal Handoff-Based Recovery Mechanism", *Hindawi Publishing Corporation's Journal of Computer Networks and Communications*, Vol. 2012, Article ID 971685, 8 pages , 2012.

[35] Anil. G.L, J.L. Mazher Iqbal, "Implementation of Secure Energy Efficient Network Priority Routing (SEENPR) Protocol with Secure Key Management in WSN", *International Journal of Recent Technology and Engineering* (*IJRTE*), ISSN: 2277-3878, Vol. 8, Issue 2S11, pp. 3096 – 3103, Sep. 2019.

[36] Qu Y., Zheng G., Wu H., Ji B. & Ma H., "An Energy- Efficient Routing Protocol for Reliable Data Transmission in Wireless Body Area Networks", *Journal of Sensors, Basel, Switzerland)*, Vol. 19, No. 19, pp. 4238. 2019.

[37] Rajdip Pau & Banani Das, "A Survey on Energy Efficient Routing Techniques and Security Measures in Wireless Sensor Network", *Conf. Paper*.

[38] Muhammad Kamran Khan, Muhammad Shiraz , Kayhan Zrar Ghafoor, Suleman Khan, Ali Safaa Sadiq and Ghufran Ahmed, "EE-MRP: Energy-Efficient Multistage Routing Protocol for Wireless Sensor Networks", *Hindawi Wireless Communications and Mobile Computing*, Vol. 2018, Article ID 6839671, 13 pages, 2018.

[39] K. Nattar Kannan and B. Paramasivan, "Development of Energy-Efficient Routing Protocol in Wireless Sensor Networks Using Optimal Gradient Routing with On Demand Neighborhood Information", *Hindawi Publishing Corporation's International Journal of Distributed Sensor Networks*, Vol. 2014, Article ID 208023, 7 pages, 2014.

[40] Yogini Anant Patil, Rahul Gaikwad, "A Study on Enhanced Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks with authentication", *International Journal of Innovative Research in Computer and Communication Engineering*, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798, Vol. 5, Issue 1, pp. 259-263, Jan. 2017,

[41] R. Logeswari & V. Manimaran, "A Survey on Secure and Energy Efficient Routing in Wireless Sensor Networks", *International Journal of Latest Engg. Science* (*IJLES*) E-ISSN: 2581-6659, Vol. 3, IJLES pp. 9-20, Issue 1, Jan – Feb. 2020.

[42] Zhongming Zheng, Anfeng Liu, Lin X. Cai, Zhigang Chen, Xuemin (Sherman) Shen, "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol. 15, No. 5, Jan. 2015.

[43] Wazir ZadaKhan, Mohammed Y. Aalsalem, N.M. Saad, "Distributed Clone Detection in Static Wireless Sensor Networks : Random Walk with Network Division", *PLOS ONE Journal*, Taiwan, pp. 1-22, May 18, 2015.

[44] E. Sujatha, R. Christy Priya, N. Kanimozhi, L. Joys Kiruba, D. Deborah, "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks", *International Journal of Advanced Research Trends in Engineering and Technology* (*IJARTET*), Vol. 3, Special Issue 19, April 2016.

[45] Heesook Choi, Sencun Zhu, Thomas F. La Porta "SET: Detecting node clones in sensor networks", *Security and Privacy in Communications Networks and the Workshops, Third International Conference on Secure Communications*, pp. 341–350, IEEE. 2007.

[46] W. Lou and Y. Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," *IEEE Trans. Vehicular Technology*, Vol.

55, No. 4, pp. 1320- 1330, Jul. 2006.

[47] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Transactions on Mobile Computing*, Vol. 9, No. 7, pp. 941–954, Jul. 2010.

[48] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random- walk based approach to detect clone attacks in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, Vol. 28, No. 28, pp. 677–691, Jun. 2010.

[49] R. Brooks, P.Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the detection of clones in sensor networks using random key pre-distribution," *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 37, No. 6, pp. 1246–1258, Nov. 2007.

[50] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," *Proc. IEEE ICNP*, *Princeton*, *NJ, USA*, pp. 284–293, Oct. 13-16 2009.

[51] Avneet Kaur, P.S. Mann, "Detection of Clone Attacks In Wireless Sensor Networks: A Survey", *International Journal of Research in Computer Applications & Robotics*, Vol. 2, pp. 49-57, 2014.

[52] Patale, Jayshri Prakash, et al. "A Systematic survey on Estimation of Electrical Vehicle." Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN: 2799-1156 3.01 (2023): 1-6.

[53] Makarand M. Jadhav, et al. "Painless Machine Learning Approach to Estimate Blood Glucose Level with Non-Invasive Devices." Artificial Intelligence, Internet of Things (IoT) and Smart Materials for Energy Applications. CRC Press, 2022. 83-100.

[54] Rahul, G. Ghodake, et al. "Microcontroller Based Drip Irrigation System." (2016): 109-115.

[55] Patale, Jayshri Prakash, et al. "Python Algorithm to Estimate Range of Electrical Vehicle." Telematique (2022): 7046-7059.

[56] Takale, Swapnil, et al. "DWT-PCA based Video Watermarking." Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN: 2799-1156 2.06 (2022): 1-7.

[57] Shinde, Rahul, et al. "Analysis of Biomedical Image‖." International Journal on Recent & Innovative trend in technology (IJRITT) (2015).

[58] Mandwale, Amruta, et al. "Different Approaches For Implementation of Viterbi decoder." IEEE International Conference on Pervasive Computing (ICPC). 2015.

[59] Takale, Swapnil, et al. "Video Watermarking System." International Journal for Research in Applied Science & Engineering Technology (IJRASET) 10.

[60] Maske, Yogita, et al. "Development of BIOBOT System to Assist COVID Patient and Caretakers." European Journal of Molecular & Clinical Medicine 10.01 (2023): 2023.

[61] Gadade, Bhanudas, et al. "Automatic System for Car Health Monitoring." International Journal of Innovations in Engineering Research and Technology (2022): 57-62.

[62] Yogita Maske, Mr. A. B. Jagadale et al. "Implementation of BIOBOT System for COVID Patient and Caretakers Assistant Using IOT". International Journal of Information Technology &Amp; Computer Engineering (IJITC) ISSN : 2455-5290, vol.

2, no. 01, Jan. 2023, pp. 30-43, doi:10.55529/ijitc.21.30.43.

[63]   Godse, A. P., et al. (2009)." Embedded Systems (First Edition). pp.(1-5).

[64]   Birajadar, Ganesh, and Channappa Bhyri. "Comprehensive survey on EEG analysis for detecting brain disorders." Mukt Shabd Journal IX (VI) (2020): 2258-2262.

[65]   P. B. Mane, et al. "High speed area efficient FPGA implementation of AES algorithm", International Journal of Reconfigurable and Embedded Systems (IJRES), Vol 7, Is. 3, 157-165

[66]   Mr. Dharmesh Dhabliya, M. A. P. (2019). Threats, Solution and Benefits of Secure Shell. International Journal of Control and Automation, 12(6s), 30–35.

[67]   Verma, M. K., & Dhabliya, M. D. (2015). Design of Hand Motion Assist Robot for Rehabilitation Physiotherapy. International Journal of New Practices in Management and Engineering, 4(04), 07–11.

[68]   Birajadar, Ganesh, and Channappa Bhyri. " cap sleep disorder identification using EEG analysis" Eur. Chem. Bull. 2023, 12 (S3), 1709 – 29.

[69]   A. O. Mulani, Watermarking and Cryptography Based Image Authentication on Reconfigurable Platform. Universitas Ahmad Dahlan, 2017.

[70]   Akshata Kambale. et al., "HOME AUTOMATION USING GOOGLE ASSISTANT", UGC care approved journal, Vol 32 Issue 1, 2023

[71]   Dr. K. S. L. Kazi, et al. "Effect of Rotation and Projection on Real Time Hand Gesture Recognition System for Human Computer Interaction", Journal of Gujrat Research Society, Volume 21 Issue 16, Dec 2019.

[72]   Birajadar, Ganesh. "Epilepsy Identification using EEG signal monitoring." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.2 (2021): 2366-2371.

[73]   R. A. Sawant, et al. "Automatic PCB Track Design Machine", International Journal of Innovative Science and Research Technology, Vol 7, Issue 9, Sept 22.

[74]   Rutuja Abhangaro, et al. "DESIGN AND IMPLEMENTATION OF 8-BIT VEDIC MULTIPLIER", International Journal of Research Publications in Engineering and Technology (ISSN No: 2454-7875), March 2017.

[75]   Mahesh Seth, et al. "Painless Machine learning approach to estimate blood glucose level of Non-Invasive device", Artificial Intelligence, Internet of Things (IoT) and Smart Materials for Energy Applications, 2022.