iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** VIII **Month of publication:** August 2018

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue VIII, August 2018- Available at www.ijraset.com*

# Bio-Inspired Ant Colony Optimization Based Clustering Algorithm with Mobile Sink for Home Automation and Cyber Security

Tejaswini D[1], Dr. Chandrakala V[2]
[1]*M.Tech Student,* [2]*Associate Professor, Dept of Telecommunication Engineering, Dr. Ambedkar Institute of Technology, Bengaluru*

***Abstract:*** ***The rapid development of wireless Communication, Zig-bee and Semiconductor devices leads to evolution in home automation network. Tiny and limited batteries are used in home automation to power the deployed consumer products. To prolong home network lifetime of consumer device energy reduction as well as energy consumption balancing across the network are most challenging research issues. Home automation network performance can be improvised by implementing Ant colony Optimization (ACO) based c1ustering algorithm with sink mobility strategy. Optimal mobile trajectory for mobile sink can be found by implementing ACO. Along with the network lifetime and energy consumption Cyber security also plays vital role in Wireless Communication. Dynamical overture in communication automation have bring about evolution of Cyber-Physical Systems (CPS). WSNs are subjected numerous forms of cyber-attacks such can cause harm, extortion or destruction of sensitive data. A generic bio-inspired model based on Swarm intelligence knowledge enhancement along with MLP is proposed to identify cyber attacks. Reactive AODV and TORA Routing Protocols are compared for the better performance.***
***Keywords: Ant Colony Optimization, Clustering, Home Automation, Sink Mobility, Attacks, Cyber Security, MLP, Routing protocol-TORA***.

## I. INTRODUCTION

A Wireless sensor network [14] can be defined as a distributed autonomous network which monitors physical and environmental factors such as temperature, humidity, sound and vibration. Each node in a sensor can sense over sensing area and certain range. Each sensor node can sense, Compute and communicate with each other. Each device that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks. Wireless sensor network is a wireless self-organizing and data-centric network which is composed of a large number of micro sensor nodes with computing and communication ability . Because of the low cost and low power consumption characteristics of WSN, it has been used widely in the field of industry, agriculture, environmental monitoring, etc.

With the fast improvement of minimal effort and low-powered gadgets and correspondence advances, numerous sorts of home consumer items have been deployed to make home automation systems. To collect data the home consumer products are distributed in home environment say humidity, temperature. BS will receive the sensed data through wireless communication. Due to the intrinsic self-organizing as well as collaborative nature home automation in WSNs are based on the Zigbee technology. Surrounding raw data are collected by the small low-cost sensors and towards BS it is transmitted in collaborative way. Because, nodes which are close to sink will have burden of more traffic the hotspot problem will arise.Clustering is one of the vital strategies for drawing out the system lifetime in Wireless Sensor Networks. It includes gathering of sensor hubs into groups and choosing cluster heads (CHs) for every one of the groups. The fundamental capacity is to verify the node.

LEACH[10] is the main system convention that utilizations progressive directing for WSNs to expand the existence time of system. Every one of the nodes in a system sort out themselves into neighborhood clusters, with one node going about as group head CH. All non-cluster head hubs transmit their information to the group head, while the group head node get information from all the group individuals, and transmit information to the remote base station. In this way, being a bunch head hub is substantially more energy concentrated than being a non-cluster head node. Ant Colony Optimization[8] is a bio-inspired algorithmic technique inspired by the behavior of ant colonies and this work postulates and demonstrates ACO is applicable to the guidance of sink mobility. The ants only have very limited local capability, but they can achieve globally optimal performance, e.g. finding the shortest path from their nest to a food source. Ants release pheromones to mark their path as they traverse their journey. The probability of an ant choosing a specific path is proportional to the concentration of pheromone which itself varies via evaporation or reinforcement. Through this mechanism,

ants can finally find an optimal path from their nest to a food source. The first ant optimization systems were applied to combinatorial optimization problems, such as the famous Travelling Salesman Problem (TSP) and also quadratic assignment problems.

The basic idea of the ant colony optimization[8] is taken from the food searching behavior of real ants. When ants are on they way to search for food, they start from their nest and walk toward the food. When an ant reaches an intersection, it has to decide which branch to take next. While walking, ants deposit pheromone, which marks the route taken. The concentration of pheromone on a certain path is an indication of its usage. With time the concentration of pheromone decreases due to diffusion effects. This property is important because it is integrating dynamic aspect into the path searching process.

As per the multi-hop information transmission[5] demonstrate information packets are sent to the sink hub through various sensors and sensors closer to the sink need to get and forward information from different sensors that are far from the sink.

The closer to the sink a sensor is, the more information it needs to forward. Thusly a great deal of computational and correspondence assets are required to process the information handing-off work for those sensors which are near the sink, particularly those sensors that are just a single hop far from the sink, which implies they can transmit information straight forwardly to the sink node. This prompts a circumstance where these sensors requires more energy and subsequently drain their energy considerably quicker than the others.

These influence the system lifetime. This happens in light of the fact that a substantial segment of sensors are relying upon those "closer-to-the-sink" sensors and when they die, a lot of information can't reach the sink, causing system downgrade performance. This issue has been recognized and tended to as a "Hotspot" problem.

Sensor hubs in Wireless Sensor Networks (WSNs) are typically battery-controlled and stay stationary after organization. At the point when a sensor hub comes up short on vitality it will never again give detecting and information handling.

This can prompt an immense misfortune in the system because of the directing way re-distribution and disappointment of detecting and detailing occasions in nature. Henceforth energy protection has been getting expanded consideration in WSN investigate works. The idea of mobile sink for WSNs is introduced as it moves the weight of energy utilization from the sensor hubs to sink hubs, which are commonly considered to have unconstrained vitality supply and bigger computational power**.**

## II. RELATED WORK

Harpreet Kaur in Attacks in Wireless Sensor Networks(WSN) [3] explains about the WSN cyber security. The tremendous deployment of Information Technology (IT) in various cyber-physical systems (CPSs) consisting of smart grids, healthcare systems, and pc networks has made them at risk of various sorts of security assaults referred to as cyber assaults. Such attacks are getting an increasing number of sophisticated and perilous, trying to gain unauthorized get admission to a carrier or data, or looking to compromise a computational system's confidentiality, availability, or integrity. The previous few years have added a superb increase within the range of cyber assaults, together with the emergence of various varieties of cybercriminals who continuously expand new attack strategies

Kavitha, T et al., in Security vulnerabilities in Wireless Sensor Networks[11] explained about WSN cyber attacks There are five kinds of surely understood digital attacks (assaults) against a WSN.

1) *Passive/Inactive Attack:* An assailant bargains and catches an aggregator hub in the system, reviews it, tunes in, and peruses helpful information in it, attempting to realize which hubs include more an incentive inside the topology. One way of secure hubs, WSNs must have the capacity to cover messages from unapproved access (secrecy/ confidentiality).
2) *Active/Dynamic Attack:* In this situation, an assailant means to disturb the system's usefulness (accessibility). The communication will be jammed by the attacker of active type by changing the stored data in the wireless sensor network. Along with that, the parameters of the component which have been configured before will also be modified.(i.e. sensors) Along with it, the sensors end up inaccessible as well as normal services are cancelled.
3) *Impersonation Attack:* Here assault, a foe or opposer can straightforwardly supplant a hub's media access control . Ordinary node is taken on the appearance of another node, which gets false information packets and bargains the reliability of the data transferred.
4) *Modification/Fabrication Attack:* In this type of attack the permission will not be given to the attacker for modifying , accessing as well as creating the data. Without any actual permission granted the assault will tries to modify the transmitted data. Black hole attack is one such where it will destroy the information moving from source to destination. In wormhole attack, information will be collected from the attacker and sent to some other location area.
5) *Denial-of-Service (DoS) Attack:* In DoS the information sent from the source to destination is ceased somewhere in between due to the node failure otherwise malicious activities. DoS avoid the data from some of sensors to reach the destination (BS).

Any of previously mentioned assaults that can conceivably disturb or wreck a system, or lessen a networks's capacity to give an administrative service, are viewed as a DoS assault/attack. Salim Bitam et al., in Bio-Inspired Cybersecurity for Wireless Sensor Networks[ 4] explained about Neural networks. In order to distinguish the DoS assault in the sensor network, the concept of Neural Network is utilized. The Neural network is advanced with minimum stockpiling as well as security of time. For recognizing the DoS caused by the enemy two parameters are key factors they are, Arrival Rate (Rr) along with Collision Rate(Rc) These two parameters contribute for Neural Networks and also for Multi Layer Perceptron.

### *A. MLP(Multi Layer Perceptron)*

Each nodes in the network are provided with same energy before the transmission begins. During each transmission every nodes in network send its Arrival Rate and the Collision Rate to the MLP.

*1)* Rc (Collision Rate): Rc is the quantity of impacts distinguished by a hub in a second.
*2)* Rr (RTS landing rate): Rr is the quantity of RTS bundles got effectively by a hub in a second.
*3)* Tw (Average holding up time): Tw is the holding up time of a parcel in MAC cushion before transmission. Above basic parameter are occasionally checked for various prospect of assau1t running from 0.1 to 1.

It's observed that the estimation of Tw is irrelevant on contrasting and the estimations of Rr and Rc. Henceforth basic parameters Rr and Rc are utilized for distinguishing the prospect of DoS assault. In the neural system1 (NN) based approach, sources of info speak to the parameters Rc and Rr and the comparing prospect of assault is spoken to as objectives to the multilayer perceptron (MLP).

It will calculate the probability of the every single node. The node which has probability very less than predefined threshold value will be considered as an attacker node. And the same node will be causing the DoS. This node will be deactivated i.e., it shuts itself down till the transmission gets over and once its over node will be re activated.

In the event that the MLP's yield (the figured likelihood of assault at that specific hub) is more prominent than a preset limit esteem STH, at that point the hub briefly close itself down, and reactivates in this way when the assault is finished. The decision of STH esteem is picked relying upon the degree of movement variety in the typical task of the WSN. Regardless of the great outcomes given by this plan as far as the power sparing because of closing down the assaulted hubs, this security instrument may trigger a false caution and make the hub close down in ordinary conditions with no assaults.

Anuj K et al., in Performance Analysis of AODV, DSR and TORA Routing Protocols[7] gave a brief idea about Routing Protocols. Routing protocol is one of the focus areas in the research of mesh-based space information network. The functionality of routing protocol is determining the path of packets from source node to destination node. According to the way of how routing is constructed, the routing protocols in wireless mesh network can be divided into proactive (table-driven) routing protocols and reactive (on-demand) routing protocols as shown in Figure 1.


Figure 1: Classifications of routing protocols

### *B. Ad-Hoc On Demand Vector Routing Protocol (Aodv)*

AODV is an enhancement of Destination- Sequenced Distance-Vector (DSDV) routing protocol
algorithm which contains the characteristics of DSDV and DSR. The AODV develop a route using two routers one for route request and another one is for route reply. The route is maintained only when it is being used by the router and if it is not maintained accurately the probability of getting expired is more. This protocol is completely based on source-initiated on-demand routing. Only when the source node desired the routes have been created. Source when it demands the route discovery process starts.

This procedure is completed once a route is found or each and every one possible routes have been explored. It provides unicast, broadcast, along with multicast communication in networks. Routes are maintained as extended they are wanted by the source node. AODV nodes maintain a route table in which nexthop routing information for destination nodes is stored.

*C. Temporally-Ordered Routing Algorithm (Tora)*

It is a hybrid, disbursed, notably adaptive routing protocol which is also called link reversal protocol. TORA uses an arbitrary peak metric to establish an instantaneous acyclic graph and the period of the direction that physically (DAG) rooted on the destination. consequently, more than one routes regularly exist for a given destination but none of them are necessarily the shortest direction. instead of the usage of the shortest route for computing the routes, the TORA set of rules continues the course of the following vacation spot to forward the packets. therefore a supply node keeps one or more downstream. TORA reduces the manage messages inside the community by using having the nodes to query for a direction most effective whilst it desires to ship a packet to a vacation spot. In TORA 3 steps are concerned in organizing a network

*1)* Developing the routes from source to vacation spot,
*2)* Preserving the routes and
*3)* Erasing invalid routes.

Initially to create a direction, the node proclaims a query packet to its acquaintances. This query is re-broadcasted thru the community until it reaches the vacation spot or an intermediate node that has a course to the destination. The recipient of the question packet then pronounces the update packet which lists its peak with respect to the vacation spot. whilst this packet propagates in the network, every node that receives the replace packet sets its top to a cost extra than the height of the neighbour from which the update became obtained. This has the impact of making a sequence of directed links from the authentic sender of the question packet to the node that to start with generated the replace packet.

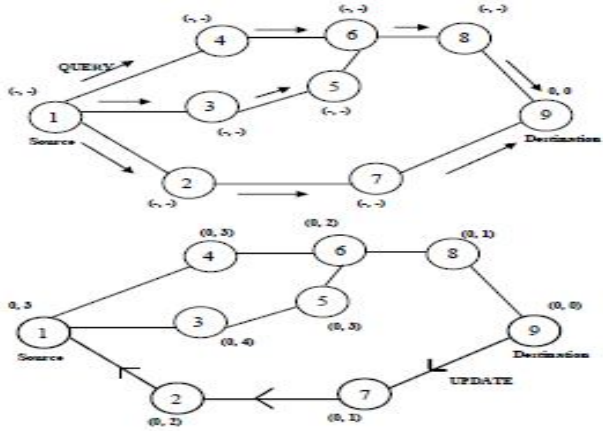



Figure 2: Route creation in TORA

As shown in figure 2, hub 6 does not spread QUERY from hub 5 as it has just observed and propagated QUERY message from hub 4 and the source may have gotten an UPDATE each from hub 2, it holds that stature. At the point when a hub identifies a system parcel, it will produce a CLEAR bundle that outcomes in reset of directing over the specially appointed system. The foundation of the course depends on the DAG system in this manner guaranteeing that every one of the courses is sans circle. Bundles move from the source hub having the most noteworthy tallness to the goal hub with the least stature like best down approach.

## III. PROPOSED METHODOLOGY

The flowchart of proposed system is shown in Figure 3. In a process of data transmission in Wireless Sensor Network the nodes (sensors) nearest to the sink node will be having more traffic. Due to the burden the nodes near sink are subjected to the depletion of energy very quickly than other nodes away from destination. This causes hotspot problem of the network.

Proposed the system with mobile sink node. Follows Ant Colony based Clustering algorithm . In order to remove the hotspot problem and also to balance requirement of energy we introduce mobile sink. To achieve this, sink node physically move all over the network. Whole network is divided into group of cluster , each one is provided with CH.

The following assumptions regarding the system model are made in this paper:

*1)* Sensor nodes are homogeneous;
*2)* Sensor nodes have the same initial energy;
*3)* Wireless links are bi-directional and symmetric;
*4)* The sink node is energy unconstrained and has free movement;
*5)* There is no obstacle between each pair of sensor nodes..

In this segment, a mobile sink is used to gather information from sensor nodes. The home network performance can be improved by combining clustering along ACO algorithm

One of the major enhancement is providing security to the network. To identify the DoS attack MLP is utilized. The Multi Layer Perceptron in every cluster will calculate the probability of DoS attacker. Every nodes in the network sends its Collision rate (Rc) and Arrival rate (Rr) as inputs to the MLP and resultant output will decide attacker node. The attacker node will shuts itself down until process gets over. Also comparing the performance of reactive routing protocols AODV and TORA for Packet drop, Packet Delivery Ratio, Throughput parameters.

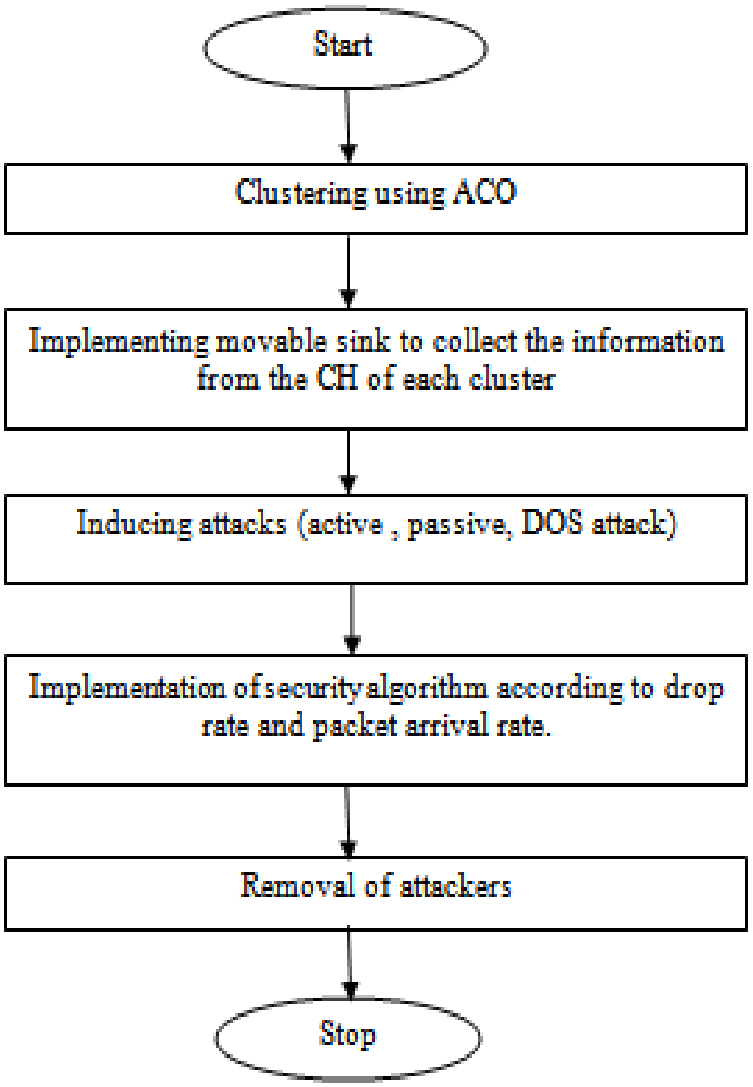



Figure 3: Proposed System

## IV. IMPLEMENTATION

The flowchart of the proposed algorithm is in Fig. 4. CHs will be selected according to the algorithm, in which all raw data are sent towards the CHs from the nodes. Then to find the optimal path for mobile sink to reach CHs ACO is executed.

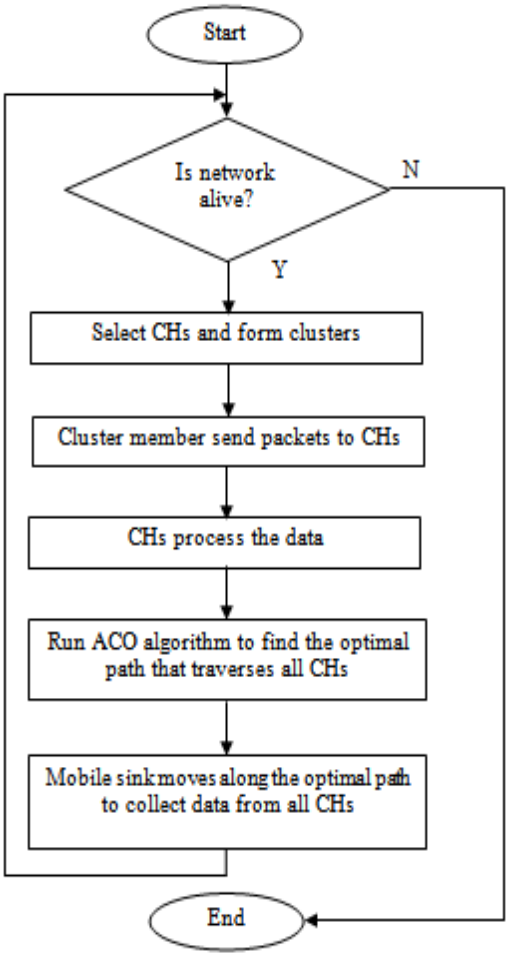



Figure 4: Selection of CH and mobile sink

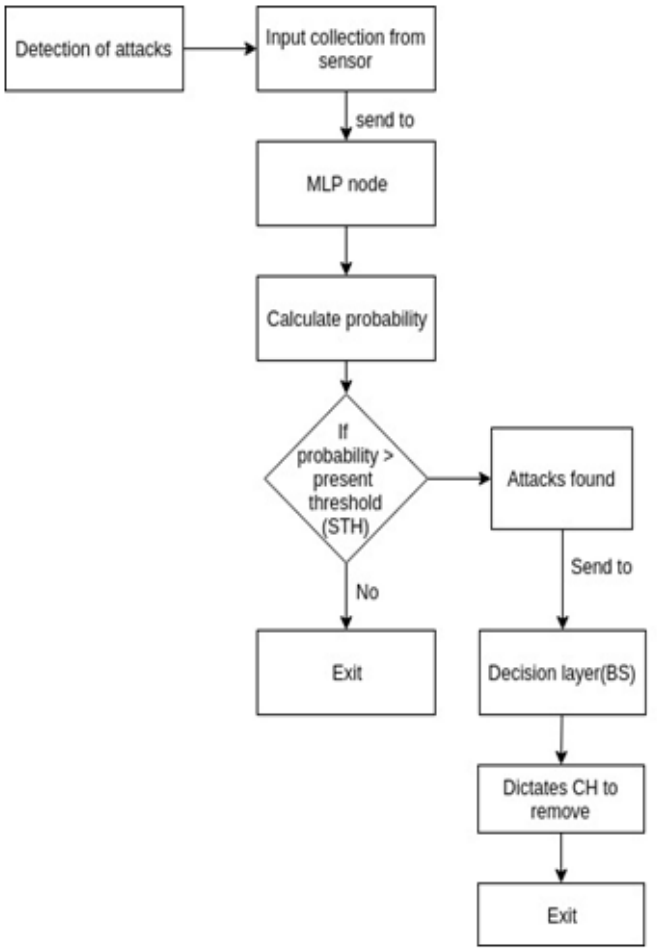



Figure 5: Attack detection and removal from MLP node

Next half of the implementation procedure is shown in figure 5. After detection of attacks the MLP node calculates the probability of collision rate and arrival rate. If probability is greater than threshold then the node is considered as the attacker. Later Base station dictates the CH to remove the attacker. The node shuts itself down until the transmission.

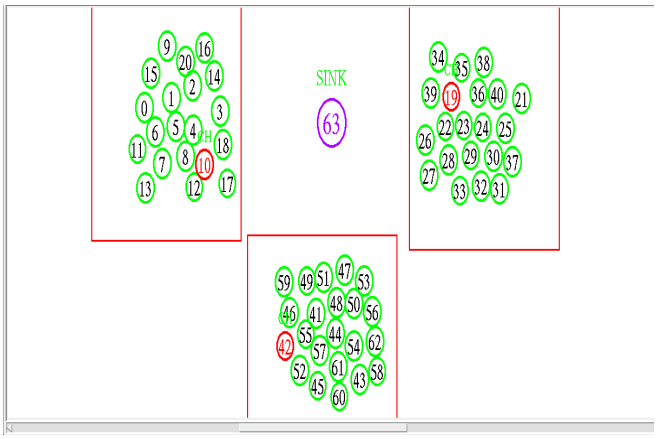



Figure 6: Cluster formation and CH selection

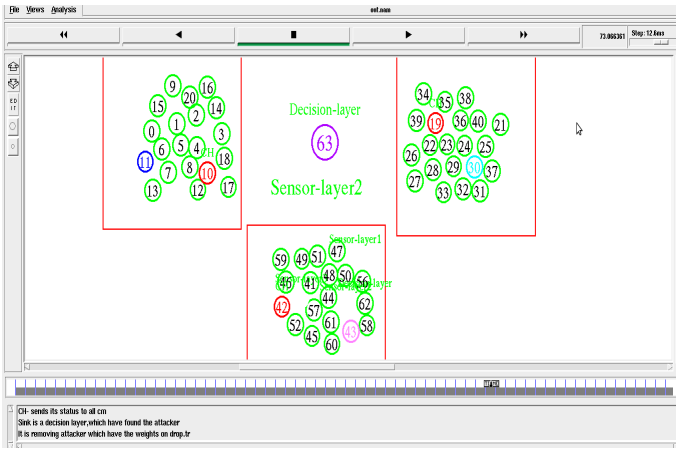



Figure 7: Selection of MLP node and detection of attack

Figure 6, 7 shows the formation of clusters, selection of CH in each cluster. MLP node is selected and the same will calculate the probability of Rr and Rc.

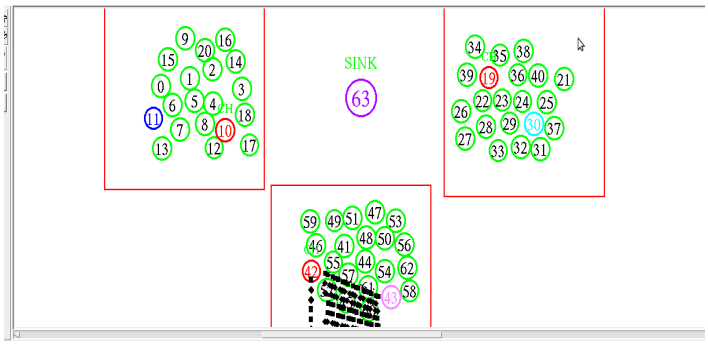



Figure 8: Packet loss during transmission due to attack.

Figure 8 shows the packet loss during transmission. The DoS attack induced in the system will be detected and CH is directed to remove the attacker until the transmission.

## V. PERFORMANCE EVALUATION

The system is evaluated in terms of performance parameters such as Throughput, Packet delivery ratio and Drop rate.


Figure 9: Throughput performance comparison

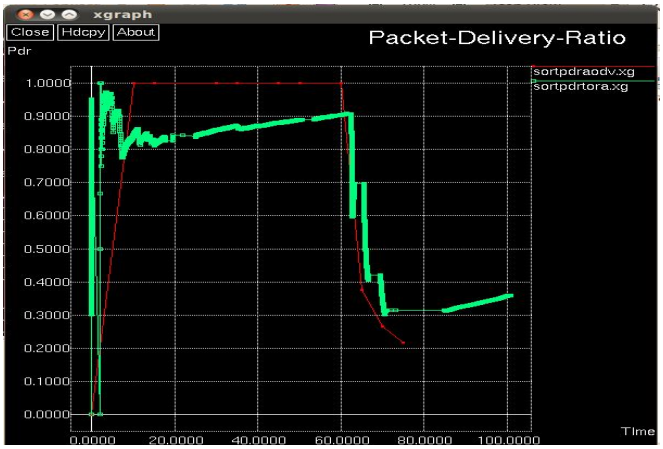



Figure 10: Packet Delivery Ratio

1) *Throughput:* Throughput comparison performances are shown in Figure 9. Throughput is the number of packets sent and received per unit of time. It is expressed in terms of kbps. TORA has more throughput compared to AODV.
2) *Packet Delivery Ratio:* The packet delivery ratio is shown in Figure 10. It is the measure of proportion of number of parcels transmitted by source and the quantity of bundles recognized by goal. Compared to AODV the packet delivery ratio is more in TORA.

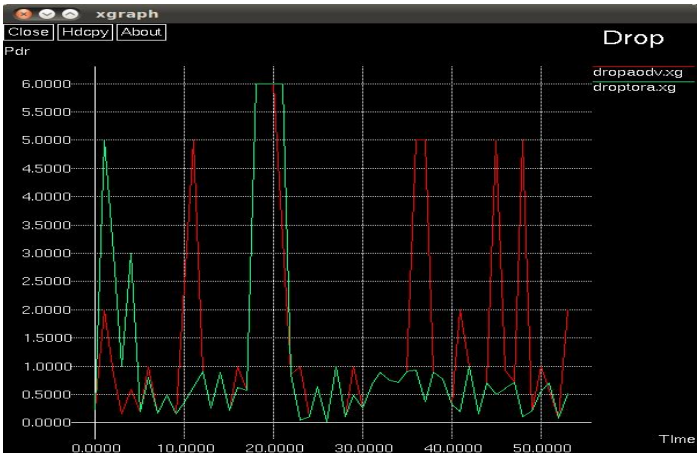



Figure 11: Number of Packet drop rate

*3) Drop Rate:* It is the number of packets dropped or lost during the transmission from source to hub. Comparison of packet drop in AODV and TORA is shown in Figure 11. AODV shows more drop than TORA

Table 1: Comparison table of protocols

| Parameters | Time(ms) | AODV | TORA |
|---|---|---|---|
| Throughput | 5 | 1830045.75 | 1995197.12 |
| | 10 | 2342296.14 | 2234411.96 |
| | 25 | 1818430.68 | 2362731.90 |
| | 50 | 1629060.15 | 2420927.86 |
| Drop | 10 | 0.491736 | 0.366957 |
| | 20 | 0.502931 | 0.332155 |
| | 45 | 0.501519 | 0.50019 |
| | 50 | 0.559397 | 0.209205 |
| PDR | 10 | 1 | 0.8 |
| | 30 | 1 | 0.85 |
| | 65 | 0.375 | 0.7 |
| | 75 | 0.217 | 0.31 |

Table 1 shows the comparison of two protocols. Compared to AODV, TORAs performance is good. Throughput of TORA is better compared to AODV as well as Drop rate is also less in TORA.

## VI. CONCLUSION

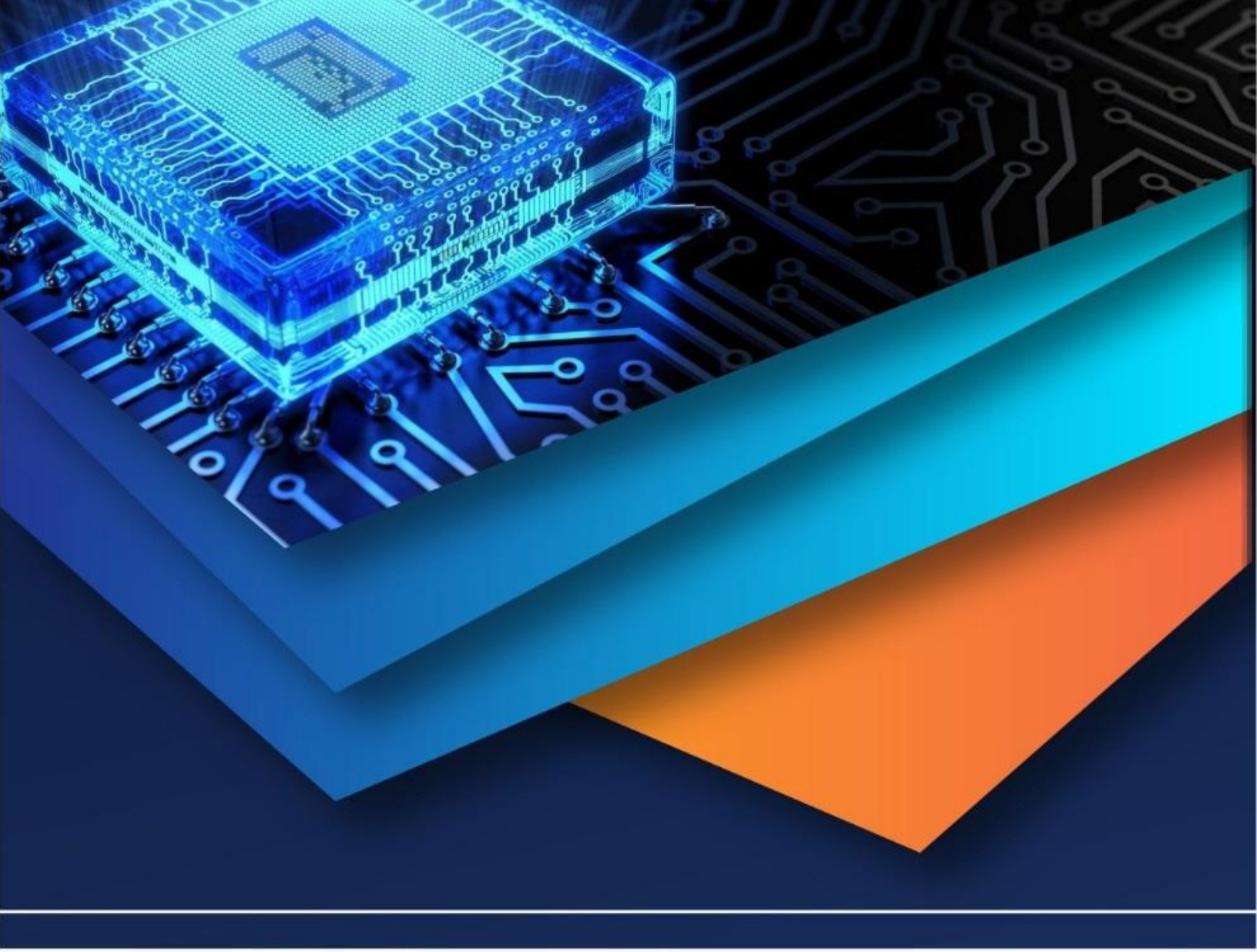
In this approach advancement of Wireless sensor networks by introducing Mobile Sink Node in a Wireless Sensor Network are concentrated. Main application of this sort of sink mobility is in home automation. In home automation sink node may be deployed in humans, some devices, moving objects etc. Mobile Sink node is more advantageous in order to save energy, loss of information, reduction of distance.

Ant Colony Optimization based Clustering algorithm is proposed to discover an optimal mobile trajectory for a mobile sink. Here for Cyber security we proposed MLP ( Multi Layer Perceptron) , a non specific bio-propelled demonstrate. This uses a machine learning based approach. MLP is a Neural Network (NN) system prepared by Swarm Knowledge Enhancement to naturally decide the ideal basic parameters used to identify cyber attacks. Routing protocol comparison performance is analyzed. TORA performs better than AODV in dense network. Number of mobile sink nodes can be increased for better performance of home automation network in future.

## REFERENCES

[1] J. Byun, B. Jeon, and J. Noh, “An intelligent self-adjusting sensor for smart home services based on ZigBee communications”, IEEE Trans Consum. Electron., vol. 58, no. 3, Aug. 2012.
[2] Shahjahan Ali and Parma Nand, “Comparative Performance Analysis of AODV and DSR Routing Protocols under Wormhole Attack in Mobile Ad Hoc Network on Different Node’s Speeds”, IEEE International Conference on Computing, Communication and Automation 2016
[3] Harpreet Kaur, “Attacks in Wireless Sensor Networks(WSN)”, An International Journal of Engineering Sciences, Inaugural Issue 2010.
[4] Salim Bitam, Sherali Zeadally, and Abdelhamid Mellouk, “Bio-Inspired Cybersecurity for Wireless Sensor Networks”, IEEE Communications Magazine June 2016
[5] H. Nakayama and Z. M. Fadlullah, and N. Ansari, “A Novel Scheme for WSAN Sink Mobility Based on Clustering and Set Packing Techniques”, IEEE Trans. Autom. Control, vol. 56, no. 10, pp. 2381-2389, Aug. 2011.
[6] H.S Annapurna and M.Siddappa, ”Secure Data Aggregation with Fault Tolerance for Wireless Sensor Network. IEEE International Conference on Emerging Research in Electronics 2015
[7] Anuj K Gupta and Dr. Harsh Sadawarti, “Performance Analysis of AODV, DSR and TORA Routing Protocols”, IACSIT International Journal of Engineering and Technology, Vol.2, April 2010
[8] J. W. Lee and J. J. Lee, “Ant-Colony-Based Scheduling Algorithm for Energy-Efficient Coverage of WSN”, IEEE Sensors J., vol. 12, no. 10, pp. 3036-3046, Jul. 2012.
[9] Manjeet Gupta and Sonam Kaushik, “Performance Comparison Study of AODV,OLSR and TORA Routing Protocols for MANETS”, International Journal Of Computational Engineering Research IJCER | May-June 2012 | Vol. 2 | Issue No.3
[10] Rajendra Singh Bisht, ”Performance Analysis Of Hierarchical And Non-Hierarchical Routing Techniques In Wireless Sensor Networks”, IEEE International Conference on Soft Computing Techniques and Implementations 2015
[11] Kavitha, T & Sridharan, D 2010 'Security vulnerabilities in Wireless Sensor Networks: A survey', Journal of Information Assurance and Security, vol. 5, pp. 31-44.

[12] Alcaraz, C, Lopez, J & Roman, R 2012, 'Selecting Key Management Schemes for Wireless Sensor Networks application', Journal of Computers and Security (Elsevier), vol. 31, no. 8, pp. 956-966.
[13] Azarderskhsh, R & Reyhani, A 2011, 'Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks', Eurasip Journal on Wireless Communications and Networking, Article ID: 893592, pp. 1-12
[14] Chan, AC & Castelluccia, C 2011, 'A security framework for privacy preserving data aggregation in wireless sensor networks', ACM Transactions on Sensor Networks (TOSN), vol. 7,no. 4, p. 29
[15] Dietrich and F. Dressler, "On the Lifetime of Wireless Sensor Networks," ACM Transactions on Sensor Networks, Vol. 5, No. 1, 2009, pp. 1-38.
[16] K. Kalpakis, K. Dasgupta and P. Namjoshi, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks," Computer Networks, vol. 42, no. 6, August 2003, pp.697-716.
[17] Chatterjea, S. and Havinga, P. "A Dynamic data aggregation scheme for Wireless Sensor Networks," in Proc. ProRISC, pp. 56-60, 2003. Y. Xue, Y. Cui and K. Nahrstedt, "Maximizing lifetime for data aggregation in wireless sensor networks," ACM/Kluwer Mobile Networks and Applications (MONET) Special Issue on Energy Constraints and Lifetime Performance in Wireless Sensor Networks, Dec. 2005, pp. 853- 64.
[18] B. Hong, V.K. Prasanna, "Optimizing system lifetime for data gathering in networked sensor systems," Workshop on Algorithms for Wireless and Ad-hoc Networks (A-SWAN), August 2004, Boston.
[19] Padmaja P,Marutheswar ,G.V ,2016,'Secured Data Aggregation In Wireless Sensor Networks',International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 7 (2016) pp 4740-4745.
[20] Padmaja P,Marutheswar ,G. V ,'Optimization Of Wireless Sensor Networks In Secured Data Aggregation 'International Journal of Electrical and Electronis Engineering Research ISSN 2321- 2055Volume 7, Number 2 (2016) pp 94-100.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY