International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 6108-6114


# Energy Enhancement Techniques for Wireless Sensor Networks Using Car Algorithm

**M. Jagadheeswari[1] and Dr. M. Anand kumar[2]**

*[1]Ph.D Research Scholar, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.*

*[1]0000-0002-8121-7337*

*[2]Associate professor, Karpagam Academy of Higher, Coimbatore, Tamil Nadu, India.*

**Abstract**

The data transmitted in the network may not be alike. Some of them have high priority to deliver data in the network. Some of them have low priority and all of them have different delivery policy. Congestion occurred due to deployment size and data rates. That congested data will be dropped from that network. Sometimes high important data will be dropped rather than low priority data. It leads to decrease the performance of network. To overcome this problem, Congestion Aware Routing protocol (CAR) is used. CAR algorithm randomly finds out the conzone. This work proposes energy efficient and mitigation on wireless control system. In wireless network, deception attack will damage the network data and produce more damage to the data and its integrity. The main problem of host which is in wireless network is energy consumption. Host will take more energy while its data transmission. It unnecessarily wastes its resources due to its delay of packet transmission and packets lose. If the system always monitors the network, its resource will be waste. These problems will be overcome through TAM and Congestion Aware Routing algorithm.

**Keywords:** Intrusion detection System, Networking, CAR Algorithm, Intruder.

## INTRODUCTION

Now-a-days authentication is very mantory one to protect data and resources from unauthorized person. Intrusion is a set of activity that compromise integrity, confidentiality, or availability, of a computing and networking resource. Intrusion Detection System is a software or hardware device that monitors the network activity and analyzes the activities for signs of possible violations of computer security policies. Intrusion detection provide three main types of security services i) Monitor the network activity ii) detect unauthorized access iii) Respond to any unauthorized access[4].

Deception attack is one of the major cyber attack convey false information in any communication channel. Attacker misuses the information which is carrying out between sender and receiver. Deception attack represented in both deceiver and target. This attack successfully done while the deceiver successfully misuses the target information. It can occur in any financial or economic interaction [1].

This deception attack represents in factory automation where the Network Control System works in dangerous environment. The main problem of NCS is reduction of bandwidth required to each subsystem. To overcome this problem, Network Control System minimizes the overhead of data transfer [11]. Plant and controller connected with packet based network. Plant carry out the command **c** to controller and controller carry out output **o** to plant through packet based network. Deception attack affects the data integrity of packet to modify their payload. Deception represents the interaction between deceiver and target. Deceiver successfully modifies the target data to specify the incorrect version of reality. Deception can be represented in any financially or economical interaction [3].

The packet will be encrypted during the transmission over the network to protect the packet from the unauthorized persons. The digital signature techniques add its signature along with the message for protection. Encryption of packet will take more energy consumption due to increased size of packet. Digital signature will increase the battery consumption due to increased size of transmission packet. Energy overhead will be increased when the attack exists. If monitoring networks all the time, it leads the unnecessary resource waste. Intrusion detection system is used to optimize the system. It will monitor the network traffic and compare with predefined baseline threshold. If attack exists, it will activate the security check [5].

Attack mitigation is another problem in this system. It will measure the performance when an attack is present. If the performance of current network load is higher than the predefined threshold value, then it will send more data, otherwise it will decrease the network load [5].

## LITERATURE SURVEY

Zahra Rezaei, Shima Mobininejad [1] performed a work on energy saving in wireless sensor networks and identified two main approaches that are duty-cycling and data-driven approaches to maximize the life time of node's battery by minimizing consumption of energy. In duty-cycling method, sensor operates on four modes: transmission state, reception state, idle state and sleep state. Transceiver will be in the idle state if no more data to send or receive. It leads to reduce the energy consumption. The sensor should be resumed if new packet becomes ready to send or receive. Alternatively the nodes will be active or sleep depending on the network activity. In data-driven method, mainly it aims to reduce the energy spent by sensing subsystem. This technique follows two processes: in-network processing and data prediction. In-network processing, performs data aggregation at intermediate nodes from source to sink. Data rate will be reduced while traversing the network towards the sink. Data prediction predicts the values sensed by the sensor. If needed accuracy is satisfied, queries can be evaluated at sink to reduce the power consumption [9].

Gurpreet Singh Sodhi and Sarabjit Singh [2] performed a work on Increasing the Performance of Wireless Sensor Networks using IM-LEACH. In this work using the clustering techniques to decrease the battery consumption and to expand the scalability of wireless network. IM-LEACH clustering algorithm is used in this work to reduce the power consumption of battery. It has two phases: a) Cluster formation b) deciding schedule for cluster head. In LEACH, every node has selected a random number that is compared with threshold value. Every node in the network acts as a cluster head whether it has a high energy or low energy. Low energy cluster head will end its life before forwarding the data to the base station. To solve this problem, each and every node will send their energy value to the initiator node. Initiator node will decide which node is eligible to elect the cluster head node. Initiator discards the low energy node and select high energy node as the cluster head. It will forward the data to base station without compromising the performance [3].

Amit Sharma[3] performed a work on Energy Management for Wireless Sensor Network Nodes. This work represents the energy management and saving techniques in WSN. Data transmission takes much more energy consumption to transfer the data. This energy management technique reduced the data transmission rate by minimizing the amount of redundant data. It leads to minimize the cost of data transmission. LEACH is a cluster based algorithm used to reduce the data sensed by the sensor before forwarding this data to the central base node. This technique helps to reduce the memory consumption.

D.Suresh and K.Selvakumar[4] performed a work on Network Lifetime and Reducing Energy Consumption in Wireless Sensor Networks. CAR algorithm helps to reduce the energy consumption and increase the life span of the network. This technique reduces the data transmission distance of sensor node in WSN. CAFEE algorithm helps the base station to receive the information of location and residual energy of sensor node and energy of every node which is in the network. Residual energy of sensor node should be higher than the residual energy of average cluster head. CAFEE follows two phases: setup phase and steady state model. In setup phase, algorithm creates the cluster and find cluster head nodes. In this phase, base station collects information of location and energy level of each node. In steady state model, TDMA schedule is created and begin the data transmission process. Cluster head node will collect the data from non-cluster head node during their transmission slot. After receiving all the data, cluster head compress the data into single signal and send to base station. It helps to reduce the amount of data and reduced to decrease the energy consumption and used to increase the life time of the network.

Subhash Dhar Dwivedi and Praveen Kaushik[5] performed a work on Energy Efficient Routing Algorithm with sleep scheduling in Wireless Sensor Network. This work used sleep scheduling algorithm to save the energy of sensor network and increase the lifetime of the network. Cluster based routing protocol is used to achieve the energy efficiency. In this technique, all the nodes are collected as cluster and one node is selected as cluster head. Cluster head receives data from other node and forward to data sink. Each node in the network may be in sleep state in the probability of p or active state in the probability of 1-p. Sleep state node should not able to send or receive any packet until it get wake up. Sleeping node will be wake up after a period of time. This technique decides which node should be put into the sleep node to save energy consumed by the sensor node. It decides the active node list and sleep node list and constructs the tree structure using Breadth-First Search (BFS). Entire process will be processed to certain period of time. If any node takes long time or get down before time up, it affect the entire routing structure and leads to energy consumption takes much than as usual. So this technique should be considered mantory that the entire node should take equal consumption of energy and sharing of network load by the entire node. It leads the network to work long time without power intervention.

Dhanunjayudu.K and Mahesh.B[6] performed a work on Trust-Based Secure And Energy Efficient Routing Framework For WSNS. This work found out deception and confirms the secure communication over the wireless sensor network. WSN should have a secure communication with the base station. The deception attacks are not allowed over the network. Before sending data to the base station, sensor checks the trust value. If the trust value is higher than the threshold value, means the data will forward to base station. Otherwise data will be rejected. It obtains the greater throughput and used to protect the network from various

deception attacks.

Nidhi Chhajed and Mayank Sharma[7] represents the concept on Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN's): A Review. It represents the concept of detection and prevention technique of black hole attack i.e. ALARM control packet. In ALARM control packet, RREP sequence number is checked whether its value is higher than the entrance value or not. If its value is higher, then sender is considering as an attacker and inserts this information into the black list. Informed this information to the entire neighborhood node that the RREP is a malicious node.

Ira Nath and Dr. Rituparna Chaki[8] performed a work on BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET. This work identified the stranger and friend to cluster head. Before route the data packet, source cluster head send the RREQ to its own cluster member and its neighborhood cluster head and wait for the reply. After some time it collects reply and stores it into the buffer. If more than one cluster head claims as its destination cluster head, it calculates the trust value of the stranger and sender sends the false packer to that stranger. If that stranger is not a black hole, then it will return the reply to the sender. If it is malicious node, it will drop that false packet. This process helps the sender to identify the malicious node and prevent black hole attack in the network.

P. Samundiswary and P. Dananjayan[9] performed a work on Detection of Sinkhole Attacks for Mobile Nodes in Heterogeneous Sensor Networks with Mobile Sinks. This work improves the performance of heterogeneous sensor network in their energy consumption, delay and delivery ratio. According to energy consumption in heterogeneous sensor network, increasing the number of nodes will decrease the energy consumption for certain percentage. According to delay, less number of hop counts will decrease the delay and improve the performance of heterogeneous sensor network. According delivery ratio, network will minimize the data loss and it leads to increase the performance of network. Small amount of broken path, minimum hop count and minimum packet loss all are the characteristics in heterogeneous sensor network helps to increase the performance of network.

Edith C. H. Ngai and Michael R. Lyu[10] performed a work on "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks". This current work confirms that the network data is more than threshold value, and then data received from the node is inconsistent node. That node is considering it as a suspected node. After finding out the suspected node list, base station locate whether sink hole attack occurred or not. Attacked area is circled by the entire suspected node. After finding out the suspected nodes, base station sends a request message to the network. Request message has the list of ID of all the affected nodes and it find out the intruder from the list through analyzing network flow information. Performance of network represented through the simulations and numerical analysis.

## PROBLEM DEFINITION

NCS network faces deception attack problems; it will affect the network performance and leads to data damage. To increase the performance and to provide data integrity, NCS network uses digital signature to encrypt the data. It adds its digest with the message itself, and used to verify the data integrity whether the data is attacked by the attacker or not. Digital signature techniques will increase the size of the data and consume more energy to send the data. Data delay or data lose also affect the network performance, take unnecessary energy consumption. Two techniques are used to reduce the energy consumption and improve the network performance.

1) Protection will be done after the attack is on-going through finding statistical approach.
2) Transmission rate will be adjusted according to the current performance of the network.

## PROBLEM STATEMENT

### Network control system:

In NCS, plant pl(x) and controller cr(x) are connected with the packet based network. Here controller send the command **c** to plant and plant send the corresponding output **o** to controller. Wireless network used to communicate between machines without additional cost for wiring. For the mobile environment, wireless medium is the only one solution. But it had more transmission issues like packet delay and packet loss. These transmission issues take more battery consumption. An energy efficient technique is used to increase the battery life for long time. Energy efficient technique follows two main tasks to increase life span of battery.

1) Minimize the overhead of encrypted packet transmission.
2) Energy consumption will be reduced if control performance is the above threshold value.

### Deception attack and protection:

Man-in-the-middle attack approach is tampered the network medium and make changes in transmission packet. It leads severe damage in the NCS network. To attack countermeasure, digital signature is used for message integrity. In digital signature, message signature is created by sender using sender's private key and inserted into message. Encrypted packet transmitted over the network. At receiver side, receiver decrypts the message by using sender's public

key and compare it with locally computed digest. If both are same, message is not corrupted and receiver accepts the message. Otherwise receiver decides that attack is detected in that message.

Attacker strategy should be well known to handle the deception attack against the network. Attacker control system should work based on some strategy. i) damage system control ii) degrade performance of the network iii) undetected attacks in network for long time. These aspects of attacker will affect the network performance and leads to increase the attack activity in the network system.

An encryption technique consumes more extra energy to transmit the data than sending ordinary data. Digital signature increases the packet size and it requires more energy to be transmitted. Consumption of more energy leads to consume more computational and communication resources. Decreasing this resource overhead is not enough to increase the energy efficiency. It requires achieving two objectives to increase the energy efficiency.

i) Activate protection strategy only if the attack present in the network.

ii) Adjust the transmission rate according to the network performance.

Proposed energy efficient control architecture used to i) detect the attacks ii) find out the end of the attack interval iii) save the transmission energy without compromising performance.

## TAM ALGORITHM

Energy overhead will be high when attack persists on the network. Always Monitoring network leads unnecessary consumption of resources.

To reduce the energy consumption, TAM algorithm is used to check whether the attack occurred on network or not. If attack persists in the network, immediately take the security check action. To achieve this, TAM is used with Multivariate Correlation Analysis.

Multivariate Correlation Analysis (MCA) is used with triangular area map to detect the attack. TAM is created and triangle attributes arranged and compared to find the attack. Mahalanobis Distance is used to find the dissimilarities between network traffic records to identify the normal profile generation. Threshold value is calculated and checked with statistical property to find the intrusion attacks. Multivariate Correlation Analysis follows two steps feature normalization and TAM generation. Feature normalization selects the normal attribute values and these features normally distributed to achieve the better detection rate and desired results. In normal distribution, mean and standard deviation is calculated for every attributes.

Euclidian Distance is calculated in each and every packets and it evaluates the normal threshold range. If it falls in the normal threshold range, then it is considered as normal traffic packet, otherwise it will be considered as an attack [4].

## CAR ALGORITHM

If the number of packets increases than the actual transmit capacity of network, it affects the performance of network. Performance degradation leads to the energy waste. Sometimes high important data will be dropped due to network congestion and low important data will be delivered. This leads to degrade the performance of the network. To overcome this problem by Congestion Aware Routing protocol. It creates a conzone and enforces a differentiated routing based on the data priority. High priority nodes routed inside the conzone and low priority nodes routed outside conzone. Congestion Aware routing algorithm routes high priority data delivery and decrease data delay and data loss. So Congestion Aware Routing reduces the energy consumption and increases the node's lifetime.

To achieve this goal, Congestion Aware Routing protocol divides the network into two areas: congestion area and remaining part of the area. High priority data travels within the congestion zone to increase the performance and low priority data travels outside the congestion zone. After sensor node deployment, base station initiates to create high priority sensor network to carry high priority data.

## NETWORK FORMATION

Base station deploys the nodes and constructs the routing network for routing the high priority data. But initially it have no information about the data, it can change its routing location periodically. Base station finds out the shortest path to route the data.

For network formation, base station send the Build Mesh message to its neighbors to known its network ID and organize the network and set its node's depth as zero. Once the neighboring node received this message, it will check whether it has added that node in the routing network or not. If it is not added in the network, that node will be added into the network, and set its depth as one plus also the depth is added in the network and set the parent as its source. Each and every node rebroadcast the incoming message to its neighbor node by sending its own ID and depth to their neighbors. If the node already added into the network, it will check its depth, if the depth is less than its own, then that message source is pointed as its parent and that message should not be rebroadcasted to others. This Build Mesh message rebroadcast for all the nodes until it reaches to the end of the network. This Build Mesh message periodically rebroadcast the message to maintain its network topology and

adapt to the network changes due to network failure or mobility of node.

## CONZONE DISCOVERY AND DESTRUCTION:

After construction of dynamic network, base station dynamically finds out the conzone. Collection of high priority data forms a conzone. This conzone area is also called critical area. Critical area will not be fixed; it will change dynamically during the lifetime of the deployment. So conzone discovery will be dynamic. It cannot be change its lifetime of deployment. It can be constructed and destructed either from sink to base station. If edge node on the network finds out the high priority event, they initiate conzone discovery to provide the better service quality to provide the high priority data flood. At the same time, conzone destruction will be occurred by critical area node or occurred by the sink. The node will be determined if they are congested path between critical area and high priority data. If that path is too congested means that will be mark as on-conzone area.

### Conzone discovery from edge:

Critical area finds out the trigger discovery. Conzone will be finding out from base station to sink to deliver the high priority data. Critical area broadcast the message to discover the conzone, this message includes its ID and its depth. Depth ensures that the node don't respond to message heard from other direction. When a node hears more than a threshold, that node represented as a D-Edge message and marks it as on-conzone threshold.

### Discovery from sink:

This will be considered conzone discovery from the sink. This technique is useful if the sink will be represented in advance and represent the pre-configure conzone. After discover the network formation, each and every node represent the node and represented in rectangular area. Each and every node send the area coverage message through represent its ID of the area and area covered by the node. This will be continuing until the node reached to the sink. To initiate conzone discovery, it broadcast the discovery conzone and broadcast down from the network. This message contains ID of the node and its depth along with the x and y co-ordinates. When D-sink message comes to the rectangular region and mark it as rectangular region. If the coverage rectangle intersects with the received rectangle, it marks it as on-conzone rectangle. Then it will propagate the message down the network and others can be added to the conzone. Conzone discovery can be split into on-conzone called it as parent and off-conzone called it as sibling. Initially both parent and sibling mark it as off-conzone. If node becomes on-conzone, it will send the D-Sink message

**Local variables:**

Set off-conzone parent POff = {P1, P2, P3, …. Pn}
Set off-conzone sibling SOff={S1,S2,S3,…Sm}
Set children = {C1, C2, C3, … , Ck}
Node on-conzone status: On-conzone=false
D-Edge threshold $\alpha_x = \beta d_x * d_x * n_x$
Set on-conzone parent POn = { }
Set on-conzone sibling SOn = { }
D-Edge msg received = ()

**Conzone discovery from Edge:**

If node x receives D-Edge from child $C_i$ then
If on-conzone == False then
If D-Edge-msg > $\alpha_x$
On-conzone = True
If X <> Sink then
Broadcast D-Edge with $d_x$
End if
Else
D-Edge-msg ++
End if
End if
Else if node x receives D-Edge from Parent $P_j$ then
POff -= {$P_j$}
POff += {$P_j$}
Else if node x receives D-Edge from sibling $S_j$ then
SOff -= {$S_j$}
SOn += {$S_j$}
End if

**Conzone discovery from sink**

If node x receives D-Sink from parent pi then
POff -= {$P_i$}
POn += {$P_i$}
If on-conzone == False then
If x has an edge child Cj ϵ criticalarea then
On-conzone = True
if x is not edge node then
Broadcast D-Sink with $depth_x$
End if
End if
End if

Else if node x receives D-Edge from sibling s1 then
S-Off -= {Sl}
S-On += {Sl}
End if

**Destruction:**

The suboptimal routing of data in low priority data is used to serve the high priority data. If the conzone will be used no longer, than that will be destroyed from the network. That conzone will be destroyed if the network receives "destroy-conzone" message from the critical area. This message will be send to avoid the problem of broadcast flood. While the conzone destruction, if the node hears the "Destroy conzone" message, the network mark that conzone as off-conzone. This process restores the regular routing data in the network.

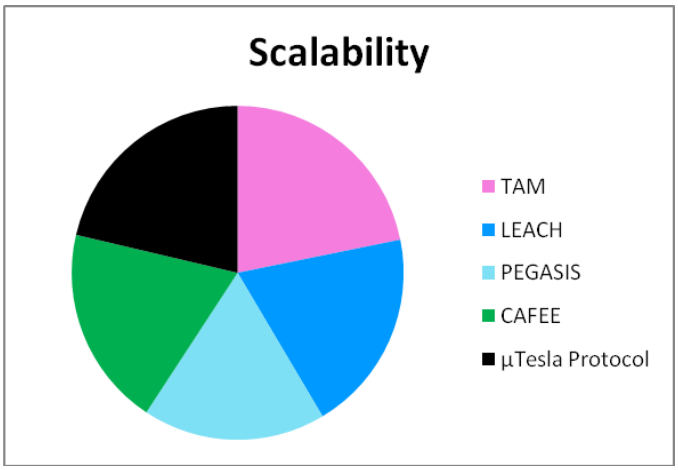
**Differentiated routing:**

Once the conzone discovered, the high priority data will be on-conzone and the low priority data will be off-conzone. Critical area will be the part of the conzone in the network and all high priority data will be generated as part of the network. High priority data will be routed very simple and the data will be forwarded to its parent. Parent node will be chosen randomly to balance the network load and this process will be continued until it reaches to sink. In certain case, if the parent node will goes to shut down, the data will be forwarded to sibling within that conzone. Otherwise that data will be forwarded to neighbor node.

Low priority data will be routed within the conzone in two modes. In first method, the on-conzone node will be generate or receives the low priority data that will be forwarded to on-conzone parent. In the second method, node should not send or receive the data that will be called as off-conzone. After construction of conzone, the node sends message to destination that will split the conzone into two. This node directly connects with the center of the conzone. All low priority data will be sending out efficiently over the shortest path.

Decision made by low priority data will be static. A node will use the node which is going to route the low priority data, that node will also determine which neighbor is going to forward that low priority data. If that parent goes to fail, the alternative node must be used for the same rule to forward data.

| Algorithm | Scalability | Transmission Delay | Energy Efficiency |
|---|---|---|---|
| TAM | 92% | 80% | 98% |
| LEACH | 83% | 82% | 95% |
| PEGASIS | 75% | 95% | 92% |
| CAFEE | 82% | 91% | 95% |
| µTesla Protocol | 90% | 89% | 90% |




## CONCLUSION

Network carries both high priority and low priority data in the network. Both of them have different policy rate to deliver the data in the network. Colliding high priority data will damage the network performance than colliding low priority data. Unnecessarily waste the resource due to network collision. It will affect the data integrity of the network. If the system always monitors the network, resource will be wasted unnecessarily. Energy efficient technique uses two algorithms: TAM and CAR. Energy overhead will be high, if the network always monitoring the network. Always monitoring the network increases the energy consumption. So TAM algorithm is used to decrease the energy consumption. If attack persists, then only it will take security check action. It helps to decrease energy consumption. Another algorithm used in this network is CAR. If the network carries more data than their capacity, it leads to deliver low priority data and rejects the high priority data. This will be degrading the network performance. CAR algorithm is used to overcome this problem. It insists the differentiated routing based on the data priority. It decrease the data lose and data delay and helps to increase the performance.

## ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g." Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

## REFERENCES

[1] M. Anand Kumar and Dr. S. Karthikeyan (2012)," Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" International Journal of Computer Network and Information Security", 4[2] : 22-28.

[2] Zahra Rezaei , Shima Mobininejad, "Energy Saving in Wireless Sensor Networks", IJCSES, Vol . 3 No. 1, Feb 2012, DOI: 10.5121/ijcses.2012.3103. 23

[3] Dr. M. Anand Kumar.and Dr. S. Karthikeyan (2013)," An Enhanced Security for TCP/IP Protocol Suite", International. Journal of Computer Science and Mobile Computing, 2[11]:331-338.

[4] Gurpreet Singh Sodhi, Sarabjit Singh, "Increasing the performance of wireless sensor networks using IM-LEACH", IJESC, March 2015, DOI: 10.4010/2015.311

[5] M. Anand Kumar and Dr. S. Karthikeyan 2012)," A New 512 Bit Cipher - SF Block Cipher" International. Journal of Computer Network and Information Security", 4[11]:55-61.

[6] Amit Sharma, Kshitij Shinghal, Neelam Srivastava, Raghuvir Singh, "Energy Management for Wireless Sensor Network Nodes", IJAET, Vol. 1, Mar 2011.

[7] D.Suresh , K.Selvakumar, "Improving Network Lifetime and Reducing Energy Consumption in Wireless Sensor Networks", IJCSIT, Vol. 5 (2) , 2014.

[8] Subhash Dhar Dwivedi, Praveen Kaushik, "Energy Efficient Routing Algorithm with sleep scheduling in Wireless Sensor Network", IJCSIT, Vol. 3 (3), 2012.

[9] Dhanunjayudu.K, Mahesh.B, "Trust-Based Secure and Energy Efficient Routing Framework For WSNS", IJCTT, volume 5, number 1, Nov 2013, DOI: 10.14445/22312803/IJCTT-V5N1P101.

[10] Nidhi Chhajed and Mayank Sharma, "Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN's): A Review", IJARCSSE, Volume 4, Issue 11, November 2014, DOI: 10.1002/wcm.v8:6. [14].

[11] M. Anand Kumar, Dr. S. Karthikeyan (2011), "Security Model for TCP/IP Protocol Suite", Journal of Advances in Information Technology, 2[2], 87-91.

[12] Ira Nath and Dr. Rituparna Chaki, "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", IJARCSSE, Volume 2, Issue 8, August 2012, DOI: 10.1002/sec.144. 11.

[13] P. Samundiswary,Padma Priyadarshini and P. Dananjayan, "Detection of Sinkhole Attacks for Mobile Nodes in Heterogeneous Sensor Networks with Mobile Sinks", IJCEE, Vol. 2, No. 1, February, 2010.

[14] Edith C.H. Ngai, Jiangchuan Liu, Michael R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks", Elsevier journal, 2014, DOI: 10.1016/j.comcom.2007.04.025.