International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May - June, 2018)

An Intrusion Detection System to Secure Efficient Clustering Routing in WSN

Ajay Kumar Mishra
M. Tech. Scholar in Dept.of Electronics and Communication
Rewa Institute of Technology Rewa
ajay7872@gmail.com

Swatantra Tiwari
Asst.Prof. in Dept. of electronics and communication
Rewa Institute of Technology Rewa
swatantratiwari84@gmail.com

Abstract*—The sensor nodes in wireless sensor network (WSN) are stationary or may be mobile some times. The sensor nodes are energy dependent and consume energy in every commotion like sending packets to neighbours and receiving. The attacker in network consumes the valuable energy resource by flooding large amount of data packets to all sensors unnecessary. The energy efficient consumption is very essential in those network sensor nodes because replacement and charging batteries in some places is not possible like in flooding possible areas and in expected explosive volcanoes. In this research work the proposed Intrusion Detection System (IDS) is identified the flooding status of nodes and collect the information of attacker on the basis of heavy flooding and unnecessary energy consumption. The attacker information is also broadcast to other nodes to not communicate with attacker after blocking communication capability of nodes. The base station is only collecting the information sending to BS. The BS is not much intelligent to take action against malicious information. The CH identifies the sink in network and after finding the sink the information of sink is sent back to sender. The sink exists in next Cluster head area and sender utilizes energy by selecting the node having enough residual energy for communication. The attacker's aim is to consume the resources at most of the time because of that the routing performance is affected. The proposed work provides the reliable routing scheme to improve network performance in minimum energy cost. The minimum energy consumption enhances the possibility of communication, which enhance network lifetime. The behaviour of attacker in existing scheme and proposed IDS is evaluated through performance metrics like PDR, Dead nodes evaluation and Average energy consumption.*

Keywords: - Flooding, IDS, Clustering, Energy, Routing, Security, WSN.

I. INTRODUCTION

The Wireless Network is the network in which the communication between the sender and receiver host is possible without any cable connection. The wired network is advanced to wireless network because it reduces the cost of extra link connected to particular host in the network. The different devices in wireless network are performing their role efficiently to maintain the reliable connection in between source to destination. The WSN (Wireless Sensor Network) is the wireless network in which each and every sensor device works as both router and host [1]. The no centralized authority is present in this network for supervision of proper communication, if without base station sensors are communicating with each other. In WSN mobile node can move while communicating and base stations are fixed as node goes out of the range of base station, which gets into the range of another base station [2]. The sensor networks are also considered as static and dynamic [3]. In static network Base Station (BS) collects the information from sensors. It comes under the category of infrastructure based network. In dynamic also, BS collects information and it is possible for nodes that they communicate with other without any presence of BS and supervision system. But wireless link has very high error proneness and fewer infrastructures. That's why attackers or malicious nodes easily degrade the network performance. Most of the energy consumption in WSNs is spent on three main activities: sensing, data processing and communication. All these factors are important and should be considered when developing protocols for WSNs. The communication of the sensor nodes is the major component of the energy consumption. The potential task of the proposed approach is not only to find the reliable path from a source to a destination, but also to provide the most efficient way to extend the network's lifetime. The example of infrastructure based WSN are mentioned in figure 1, where the sender node wants to communicate with receiver or base station through intermediate nodes and all network nodes forward the collective information to Base Station D.

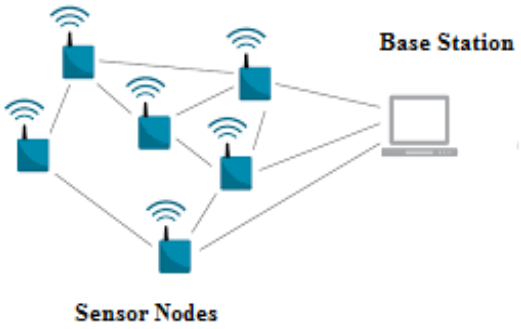

Fig. 1. WSN Example

The node S and base station D are not further communicated with the other nodes because they are not in range of other nodes or destination. Each mobile sensor device is able to communicate with each other if they are under the communication range. The nodes in range are the neighbor nodes and each node also moves in network with random mobility speed in meters second. Due to movement of sensor nodes the string connection establishment is also the major concern for successful data delivery [4]. The attackers or malicious nodes are easily disturbing the original routing performance [5]. The attacker node is always the intermediate node/s and this node/s are not instantly attacking in network but these anodes first analyze the routing information and exactly behaves like the normal node. If the sender has started the data sending at that instant attacker is activated and started dropping or corrupting all valuable information [6]. Some of the malicious nodes are also flooding unwanted information in huge amount. The attackers are also categorized in different categories and these categories mention the attacker type in network. The attacker aim is only to drop the packets, consume network bandwidth or link capacity between the mobile sensor nodes and communicate with fake identity in network. In this survey the different attacks classification in WSN and types of

routing protocols is in detailed manner discussed with different routing strategy in WSN. Al-Karaki in [7], Thus, the routing protocols can be classified into four main schemes: Network Structure Scheme, Communication Model Scheme, Topology Based Scheme and Reliable Routing Scheme

II. Types of Attack in WSN

An Attackers or Malicious nodes are performing different types of malicious activities that have damaged basic aspects of security like integrity, confidentiality, and privacy [8]. Here there are different types of attacks [9] and they are mentioned in detail.

A. Active Attacks

It is like as passive attack that monitors and listens by unauthorized communication channel and it also modifies data stream in communication channel. These attackers are actively participating in network in malicious performance. There are different types of active attacks a shown here.

1) Black hole Attack

Black hole attack is the packet consumption attack. In this attack the attacker nodes is identified the sender that want to send data to receiver and reply fake route information to sender. Sender is sends the data from the path where the attacker is exist in network. Then in that case the attacker is making loss of whole data and network performance id degrades.

2) Sybil Attack

Malicious node can duplicate itself and it presence affects at multiple places. It targets fault tolerance scheme as distributed storage, multipath identities for another node, multipath routing and topology in the networks. These attackers are changing their original identity and grasp the neighbour node identity in network.

3) HELLO Flood Attack

An attacker with high radio transmission range and process on power sends “HELLO” packets to number of sensor nodes which are isolated in wireless sensor network. So sensor nodes prejudice adversary is their neighbour. While information is sent to the base station, then at that time, the victim nodes are trying to go via attacker resulting neighbour in higher spoofed.

4) Denial of Service

When unintentional failure of nodes or malicious nodes attack any event that diminishes network’s capability of services and also affect on destroying network, this can be affected on different layers like Physical layer and DoS attacker in jamming and tampering. While collision, unfairness and exhaustion will occur in Link Layer confirm the presence of DoS attack.

5) Wormhole attack

Wormhole attack is most severe attack in WSN in which using private high speed networking, pair of colluding attackers can record packet information at one location and replay then on other location. So this can be launched against all communications for providing authenticity and confidentiality.

B. Passive Attacks

It does not affect any communication works but unauthorized person can just monitor and listen communication channel and it is hard to find these types of attacks due to its passiveness behaviour. The passive attackers are not continuously and actively injects malicious actions in network because of that their reorganization is difficult.

1) Attacks against privacy

In sensor network there are large numbers of information available by remote access, so any malicious node can easily gather information. Here some attacks against privacy are defined:

2) Monitor and Eavesdropping

It is very common attack, in which, by snooping data adversary it can easily discover communication control information for sensor network configuration that contains information and affects against privacy protection.

3) Traffic Analysis

Though messages are transferred by encrypted, it leaves high possibility communication patterns, because of sensor activities and it can potentially affect on enable information and cause harm to sensor network.

III. Overview of Clustering

In clustering method of communication network nodes are organized in similar groups called clusters in which a node with higher residual energy, for example, assumes the role of a cluster head [4]. The cluster head is responsible for coordinating activities within the cluster and forwarding information between clusters. Clustering has the potential to reduce energy consumption and extend the lifetime of the network. They have high delivery ratio and scalability and can balance the energy consumption. The nodes around the base station or cluster head will deplete their energy sources faster than the other nodes. Network dis-connectivity is a problem where certain sections of the network can become unreachable. If there is only one node connecting a part of the network to the rest and fails, then this section would cut off from the rest of the network. Clustering may be extended to more than just two levels having the same concepts of communication in every level. The use of routing hierarchy has a lot of advantages. It reduces the size of routing tables providing better scalability. Low-Energy Adaptive Clustering Hierarchy (LEACH) [10] is one of the most popular cluster-based routing protocols in wireless sensor networks. The operation of LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are organized, followed by a steady-state phase, when data transfers to the base station occur. In order to minimize overhead, the steady-state phase is long compared to the set-up phase. To reduce management consumption, the steady-state phase is much longer compared to the set-up phase. The head of the cluster collects the data that's been composed by the sensor nodes and this facilitates in to assure high quantity of traffic generated within the network. With this, a large-scalable network with no traffic surplus is organized and by this additionally improved energy efficient constellation is attained as compared to the flat-topology. Single-hop routing is probable from device node to go of cluster, and by this implies able to able to accumulate the energy of the network. Property of distribute within the cluster, where it assigns the role of CH to the opposite cluster within the cluster

IV. Literature Survey

In this section, description of the previous works proposed by different authors in field of security in WSN is given.

In this system [11], they additionally added attack detection when any attack is done over cluster members or cluster head.

This system is also able to prevent the false information sending over network aggregation node. If any attack is detected over cluster head we aggregate all information of the cluster members of information of data collection node. This novel developed system probably gives reliable information delivery as well as secure information sending methodologies. Also they achieved solution for the problem of the data loss and enhanced the performance of network.

Energy Efficient Clustering Algorithm for data aggregation in WSN [12] is one of the examples of clustering algorithm. It includes two phases of clustering. One is the formation of cluster heads. In this phase every node broadcast their radius, residual energy and co-ordinates to the neighbour nodes. Then the nodes will calculate competition bids to select the cluster head. The other phase is data aggregation and tree construction, which includes calculation of weight values for cluster heads depending on the distance from the base station and remaining residual energy. These weight values help to select the leader node among the cluster heads. The aggregated data will be sent to base station only by leader node which leads to uniform energy dissipation and long network longevity.

Energy Efficient Clustering under the joint Routing and coverage constraint [13] addresses optimal planning of the different states of sensors, providing energy efficient scheduling of the states, energy efficient routing, clustering and data aggregation. The algorithm formulates the problem as an ILP model and implementation of TABU search algorithm to manage exponentially increasing computation times. It mentions four different states of sensor node such as Transmit, Receive, Idle and Sleep. A subset of the total number of nodes will remain active at a time to save energy and reduce redundancy. The cluster heads are chosen dynamically on the basis of residual energy and distance from the neighbours and a spanning tree connects all cluster heads which are only capable of routing and thus send data to the sink. It is stated that all nodes have same sensing range and transmission range and the cluster heads are dynamically selected from the nodes.

Another algorithm Energy Efficient Heterogeneous Clustered scheme for Wireless Sensor Network [14] has assumed that a percentage of sensor nodes are equipped with more energy and are immobile with known geographical locations. The introduction of computational heterogeneity includes more powerful microprocessor, more energy, complex data processing ability, which adds a lot of advantages to this model. The Link heterogeneity is introduced with the inclusion of high bandwidth and long distance network transceiver to prolong the lifetime of the network together with reliable data transmission. The Energy heterogeneity brought about the energy efficiency to the network, however increasing the implementation cost.

V. Proposed IDS Algorithm

This section is about how the implementation can be performed to detect and prevent attacker from network. Proposed algorithm shows the step by step process and group into common platform to protect flooding node under cluster based approach. Here the P prevention node create the two different table such as normal and suspicious profile table, it is useful to detect the flooding node and after that protect from flooding behavior using blocking method. In the below it is described how the algorithm work.

Input:
m_n: Mobile Nodes
S: Source Node
R: Receiver Node
CH: cluster head
M_b: Member nodes
F: flooding nodes
P: Preventer node //IDS
Protocol: AODV
Output:
Procedure:
m_k generates cluster head election procedure
If m_n in radio range **then**
m_n receive election message
Compare (speed, no of covered nodes, location)
m_i elected as CH based on low speed, max node covered and center location
m_i broadcast CH message to all m_n node whose in range
all m_n set as m_b ready for communication
Else
Nodes are out of range
End if
S generates routing packets
Broadcast (AODV, S, R)
If CH & m_b belong in range & R not found **then**
m_b receives route packets
m_b forward route packets
CH monitor the entry of all m_b nodes
Else if CH & m_b belong in range & R found **then**
CH synchronize all m_b nodes who participate in route
R sends the reply message through CH coordination
S receives reply by CH or m_b nodes
Call Send (data, S, R)
Else
R not found
End if
Send (data, S, R)
S generate (data, S, R) packet
If route found **then**
P watch the m_b node
If P found m_b node generate unwanted data in higher rate **then**
P send report to suspicious table
P compare suspicious profile & behavior
If behavior == abnormal & profile != normal & rate > normal **then**
Mb node set as F
Block the F node
CH node eliminate m_b from cluster
CH broadcast m_b elimination message to another CH_n & m_k
Re-generate route message
Select route without participation of m_b
Else
Filter unwanted data from network
Send notification to m_b node

End if

Else

m_b send data to R node

P monitor every time to all m_b nodes those participate in route

CH handle all m_b node

End if

Else

Re-route generate

End if

The proposed IDS scheme provides the complete security from attacker by stopping the flooding. The proposed security improves the network lifetime.

VI. Simulator Overview and Performance Metrics

Network Simulator (Version 2), wide called NS-2 [15], is solely an occasion driven simulation tool that has tried helpful in finding out the dynamic nature of communication networks. Simulation of wired similarly as wireless network functions and protocols (e.g., routing algorithms, layer protocols implementation) can be possible in NS2. In general, NS2 provides users with how of specifying such network protocols and simulating their corresponding behaviours. Since 1995 the Defence Advanced analysis comes Agency (DARPA) [15] supported development of NS through the Virtual inhume Network work (VINT) project. Presently the National Science Foundation (NSF) has joined the ride in development. Last however not the smallest amount, the cluster of researchers and developers within the community are perpetually operating to stay NS2 robust and versatile.

A. Performance Parameters

The detail of all the parameters is mentioned below in table 1. The performance of all three modules is based on these parameters. The simulator tool version is used NS-2.34, because this version is support the clustering based communication and also upgraded version of network simulator.

TABLE I. Performance Parameters

Simulator	NS-2.34
Number of nodes	30, 40, 50, 60 ,70
Propagation	Two-Ray Ground
Antenna	Omi-directional
Dimension of simulated area	800×600
Routing Protocol	AODV
Simulation time (seconds)	200
Transmission Range (meters)	550
Transport Layer	TCP,UDP
Traffic type	FTP, CBR
Packet size (bytes)	1024
Maximum Speed (m/s)	25

VII. Results Description

In this section the results of three modules are compared. The performance of attacker presence in network, existing routing scheme [11] and proposed IDS is compared. The proposed IDS are used to improve and prevent network from attacker and to provide better performance than existing scheme.

A. Remaining Energy Analysis

The number of dead nodes in network shows the energy of nodes is fully utilized in communication and nodes goes to sleep mode. The sensor nodes are again wake up after charging or replacing battery (if possible). In most of the areas sensors battery replacement and charging is not possible. In this graph network life time in proposed IDS scheme is more that shows the nodes are ready to work for more time in same network. On the other hand performance of attacker shows the minimum life time in all node density scenarios and after that the life time of existing scheme is more. The minimum lifetime performance is showing less live nodes in given simulation time of 200 seconds. The energy is utilized for communication that means the performance is improved and the overhead and dropping is minimum in WSN.

B. Energy Consumption Analysis

The number of nodes energy consumption shows the activity of nodes in network. The group of clusters is created and shattered in every communication that means the sender wants to communicate with receiver then for each sender the LEACH protocol is forming the different topology when the CH energy reaches to low level than the CM. In this graph the average energy consumption of nodes are evaluated in given simulation time. The number of nodes live in network is more in proposed IDS security as compared to existing scheme and the expectations from attacker is opposite, as usually it shows the more and more energy consumption as compared to rest of two modules. The energy consumption in proposed IDS is less, that's why energy consumption is less because nodes are not cheated by attacker and also chooses the better Cluster Head and Cluster Members.

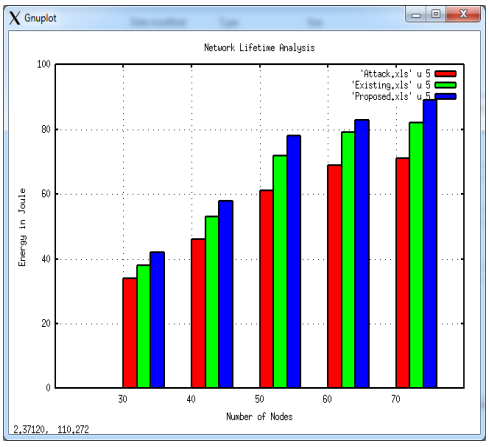

Fig. 2. Lifetime Analysis

C. Normal Routing Load (NRL) Analysis

The senders are establishing connection with sink through routing packets. These routing packets are continuously forwarded by intermediate nodes till the sink node is not found. If the link get break in network then again the whole procedure is repeated. In this graph the routing packets flooding is completely blocked by IDS security that's why energy consumption is also reduced. The routing packets are also consuming energy and if the flooding is minimum, then in that case the energy is saved. The routing overhead of proposed IDS security is less than existing security scheme that shows the better energy utilization. The attacker quantity of flooding enhances the routing packets quantity that also

affects the packets receiving and energy consumption. The proposed approach maintains strong link that's why flooding is minimizes and improves energy utilization.

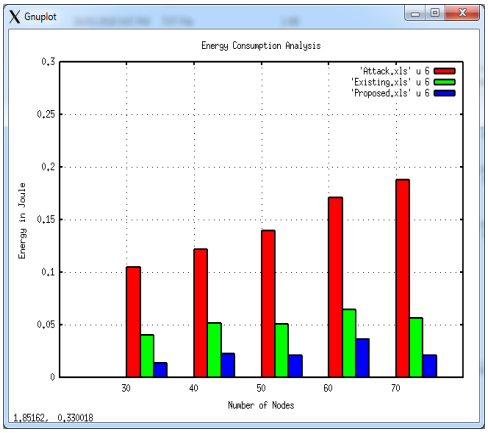

Fig. 3. Energy Consumption Analysis

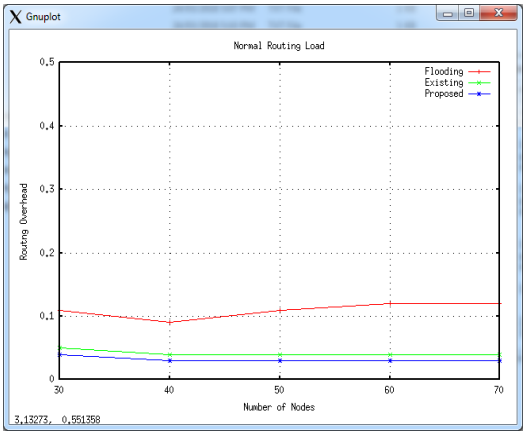

Fig. 4. NRL Analysis

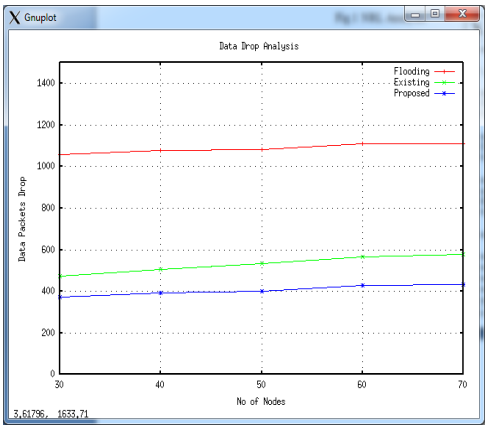

Fig. 5. Data Drop Analysis

D. Data Dropping Analysis

The number of packets successful received at destination shows the better performance because the better quantity of packets receiving in network represents the better energy utilization and minimum data dropping. In this graph the packet dropping performance of module of Flooding attacker, existing security scheme and proposed IDS is measured. Here the packets dropping in presence of proposed IDS is minimum due to better security and reliable path in between source and destination. The proposed scheme is also applied in clustering based routing and detects the attacker by its flooding behavior of unwanted packets that consume limited link bandwidth and energy. The attacker is dropping almost two times more packets as compared to proposed IDS based communication in WSN.

VIII. Conclusion and Future Work

The energy of sensor nodes depletes in every communication and due to limited capacity of battery lifetime it is necessary to utilize the battery power efficiently in WSN. The all nodes are containing the different energy value and also in communication like sending data packets, receiving data packets and in sensing neighbour energy of nodes are consumed. The aim of attackers is to consume limited energy of sensors and because of attackers presence the performance of network degrades continuously. In this research three modules are simulated like flooding attack, existing scheme and proposed IDS. The IDS detects the attacker and improves the clustering based routing performance. For clustering LEACH protocol is used. The LEACH protocol creates the cluster and communication is started between the sender and the sink. The cluster head and cluster members are changed according to residual energy. The attacker is actually only flooding the huge amount of data in network and the number of nodes in network receives it but on the basis of that the cluster communication is secure to detect the attacker malicious behaviour. The IDS blocks the communication capability of attacker. The number of packet dropping in proposed IDS is minimum, as compared to rest of the modules that shows the link stability is more in proposed IDS approach as compared to pro attacker module. The quantity of dead nodes is also less because the energy is utilized in between the source and the sink. The packet receiving is network is also improving the PDR and reduces the packets drooping. The energy consumption in proposed scheme is less that shows the better network lifetime. The improved lifetime shows extra benefit and this benefit is utilized for further communication.

In future we will propose the security scheme against packet dropping attack and energy efficient approach to select the node having sufficient energy and reduce the flooding packets for reducing energy consumption by forming a new mathematical equation. In this equation the energy consumption of node selected having more degree for routing is considered for communication and this equation is also helpful for identifying attacker. We can also apply this scheme in dense and light network by using multipath approach.

References.

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Network : A Survey,” Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA, Computer Networks 38, Elsevier, pp. 393–422, 2002.

[2] S. E. Roslin, C. Gomathy, and P. Bhuvaneshwari, “A Survey on Neighborhood Dependant Topology Control in Wireless Sensor Networks,” International Journal of Computer Science & Communication, Vol. 1, No. 1, pp. 185–188, 2010.

[3] Liping Liu, Feng Xia, Zhi Wang, Jiming Chen, Youxian Sun, “Deployment Issues In Wireless Sensor Networks”, Mobile Ad-hoc and Sensor Networks, Volume 3794 of the series Lecture Notes in Computer Science pp 239-248, Springer 2005.

[4] Neelir Prasad and Mahbubul Alam, "Security Framework for Wireless Sensor Networks. Wireless Personal Communications", 37: 455–469, 2006.

[5] S. Batra, P. Goyal, and A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, 11-15, 2010.

[6] Adrian Perrig, john Stankovic, David Wanger, "Security in Wireless Sensor Networks " Communications of the ACM, Page 53-57, year 2004.

[7] Al-Karaki, A. Kamal, "Routing Techniques in Wireless Sensor networks: A Survey," Security and Networks, Vol. 11, Issue 6, pp.6-28, 2004.

[8] Shio Kumar Singh, M P Singh, and D K Singh"A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks" International Journal of Computer Trends and Technology (IJCTT) pp. 1-9, May to June 2011.

[9] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" Journal of Theoretical and Applied Information Technology, pp. 14-27, 2010.

[10] Xuxun Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks", Sensors, pp. 11113-11153, 2012.

[11] Sneha Kamble, Tanuja Dhope, "Reliable Routing Data Aggregation using Efficient Clustering in WSN", International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp. 246-240, 2016.

[12] Sha, C., Wang, R., Huang, H., Sun, L., "Energy Efficient Clustering Algorithm for data aggregation in WSN", Elsevier Journal, the Journal of China Universities of Posts and Telecommunications, December 2010.

[13] Chamam, A., Pierre, S., "On planning of WSNs: Energy Efficient Clustering under the joint Routing and coverage constraint", IEEE Transactions on Mobile Computing 8(8), August 2009.

[14] Kumar, D., Aseri, T.C., Patel, R.B., "Energy Efficient Heterogeneous Clustered scheme for Wireless Sensor Network", Computer Communication 32(4), pp. 662–667, 2008.

[15] NS2 simulation package, http://www.isi.edu/nsnam/ns/ (Last visited, March, 2018).