ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 10(19), DOI: 10.17485/ijst/2017/v10i19/109245, May 2017* ISSN (Online) : 0974-5645

Recognition and Handling of Insider and Outsider DDOS Attacks in WSN

Shivam Dhuria[1*], Monika Sachdeva[2] and Gulshan Kumar[3]

[1]CSE, SBSSTC, Ferozepur – 152004, Punjab, India; sdhuria13@gmail.com
[2]IKGPTU Main Campus, Kapurthala – 144603, Punjab, India; monasach1975@gmail.com
[3]SBSSTC, Ferozepur – 152004, Punjab, India; gulshanahuja@gmail.com

Abstract

Objectives: Recognition and Handling of Insider and Outsider DDoS attacks are very important in WSN. Various schemes have been proposed in the past to fight against DDoS attacks in WSN. But they have either used a complex approach for recognizing the attack or they were not able to handle the attack efficiently after recognizing it. The presented method has followed a simplified and effective approach to recognize and handle the DDoS attack. **Methods:** In this paper two methods have been introduced, Authentication method is based upon a mathematical formula which is only known to legitimate nodes in the network. In data filtration method, each node in the network checks the input data volumes coming from other nodes against a threshold value to find the traffic abnormalities. Both these methods are simple and can be deployed at every node in the network. **Findings:** The results have been verified using the Network Simulator 2 (NS2) on various performance metrics i.e. throughput, delay, lost packets, energy consumption and PDR. It has been observed that fixing the threshold value results in recognition of attack at very early stages and blocking the communication with the attacker results in saving approx 56% energy of the network.. The threshold value can be decided as per the bandwidth usage that may vary in different applications. **Improvements:** The data filtration method can be enhanced in future by using historical methods so as to analyze and mitigate other severe attacks like blackhole and sinkhole attacks.

Keywords: Authentication, Data Filtration, DDoS, NS2, Threshold, WSN

1. Introduction

Wireless Sensor Network (WSN) is a network of spatially distributed autonomous sensors that cooperatively pass their data to the main location called base station. WSNs are emerging at a great pace due to their cost effective solutions for the sensitive and remote applications like military, medical and environmental applications[1]. But, due to limited range, memory, processing and power supply, gathering of important remote data from wireless sensors is really challenging. The use of ad-hoc network and radio waves for data transmission has increased the chance for attackers to attack on such networks[2-4]. Keeping in mind the limited battery power of nodes, implementation of various security methods like authentication, encryption, jamming detection and DDoS attack recognition and handling etc is one of the important concerns in WSN.

Denial of service (DoS) is a type of attack in which attacker launches by overwhelming the legitimate node with continuous route request (RREQ) packets or continuous stream of data so as to make its services unavailable to other legitimate nodes. All the legitimate node's resources become busy in replying to RREQ packets or receiving high volume data packets from attacker thus leading to drainage of its battery very soon[5]. Distributed Denial of Service (DDoS) attack is same as DoS attack but with traffic from multiple directions are involved resulting in more severe attack. Due to battery constraint and limited resources, DDoS attack has become a major threat for WSN nodes. DDoS attacks can drain the whole battery for bunch of nodes which can make a segment of network totally disconnected with base station.

Generally, attackers in WSN can be described in two ways i.e. 1) Outsider Attackers who have little or no secret information about the network. 2) Insider

* *Author for correspondence*

Attackers who have all the secret information of network and are legitimate part of the network. Outsider attackers attack the WSN by a) Passive attack i.e. via connecting to appropriate frequency and getting all important information without causing any harm to data. b) Active attacks like jamming the network[6], collision attacks, replay attack, authentication attacks etc. Insider attackers can attack the networks more severely. As being the legitimate node of the network, insider attacker can directly communicate with other reachable nodes of the network. Insider attacker can also manipulate the data easily before sending it to other nodes of the network. In the research paper we have tackled both inside and outside DDOS attacks. Following are some of the related work and references that have been observed carefully in order to accomplish this research work.

In[7] have followed a probabilistic approach to mitigate the DDOS attack by calculating the receiving rate of intermediate nodes. It slashes the sending rate if receiving rate is found abnormal. Using PPFS mechanism, packet flow rate is reduced which gradually reduces the flooding of packets from attackers. The proposed mechanism however does not eliminate the attack completely but is the first step to handle the attack, buffer mechanism to discard the packets from attackers after certain limit has been proposed for future work.

In[8] has followed a scheme to detect DDOS attacks in early stages in order to prevent the resources from getting wasted. They divide the network into grids and deploy the examiner nodes, if any node sending data at faster rate, then its PDR will be compared with the neighbor node by the examiner node as examiner node has all the information of nodes present in its grid. If PDR is abnormal then that node will be marked as malicious and the network will stop communicating with that node.

In[9] has described the various types of DOS attacks and also various defense mechanisms to tackle them in WSN at different network layers. They concluded that majority of the attacks in WSN can be prevented by authentication and anti replay mechanism, other methods also exists to detect and recover from attacks but they can be defeated by some counter mechanism, so the reason to find some concrete solutions to overcome from DOS attacks in WSN.

In[10] has described a method to tackle a selective jamming attack in TDMA based WSN. Attackers can easily disrupt a particular service of a particular node in TDMA based network. It is also hard to detect this kind of attack as compared to wide based jamming attack. The method described by author is to randomly change the time slots for the nodes based on the local information thus following self adaptive solution and allowing the nodes to join and leave the network without hindering other nodes activities. They force the adversary to attack randomly and reduce its effectiveness to 1/N where N is the total number of slots in the network. Author proposes some future work in case when multiple nodes want to join the network at same time.

2. Methodology

In this paper we have presented authentication method and data filtration method to tackle both outsider and insider DDoS attacks. Authentication is the best way to keep the outsider attackers stay away from the network[11-13]. Route request flooding (outsider attack) is one of the frequent attacks in WSN because attackers attack the legitimate nodes by bombarding the route request or authentication packets in the network; in that case data filtration method plays an important role to prevent this attack. Insider attacks are also frequent in WSN because of their deployment in remote areas with lesser maintenance and thus leading to node capturing. Insider attacks can also be prevented by the data filtration method.

2.1 Two Way Authentication Method

In this paper a method is introduced in which a node will only be able to communicate with other node in the network if they have the shared secret of the network. For this, each node generates hash answer key for some random seed using the shared secret and send it to other node for authentication. Other node verifies this secret information and vice versa. A specific bit pattern is also decided for route requests i.e. REQ(11) and route reply i.e. REP(22).

2.1.1 Authentication Algorithm

1) Node A sends REQ(11) + RREQ to Node B.
2) Node B generates a random seed and send [REP(22) + SEED(B) + HASH(ANSWER(SEED(B)))] to Node A.
3) Node A uses Node B seed to generate hash answer key at its end and match it with the one that came from Node B.

4) If Auth == Success then Node A sends [REP(22) + SEED(A) + HASH(ANSWER(SEED(A)))] to Node B.
5) Node B authenticate Node A same as STEP(3).
6) If Auth == Success then Node B update its routing table and start receiving data from Node A.
7) If TIMER(NODE A) expires, Repeat STEP(2) to STEP(6).
FUNCTION ANSWER(SEED)
1) ANS = SIN(SEED) * COS(SEED) * LOG10(SEED)
2) ANS = - ANS IF ANS < 0
3) ANS = ROUND(ANS*1000)
4) RETURN ANS

2.2 Data Filtration Method

For recognition of insider and outsider DDoS attacks, each node in the network checks the input data stream coming from other nodes of the network. The individual data volumes are then scanned against a threshold value to recognize the attacker(s). As every node in WSN has data communication rate within a limited range, a threshold value can be decided as per the application requirement. If any node is found with data transmission exceeding that threshold value then that node will be considered as attacker node and all the communication from that particular node gets blocked by other nodes in the network. Figure 1 represents the data filtration flowchart.

The explanation of data filtration method is logically divided into following:

- I. Data Filtration Algorithm and Flowchart
- II. NS2 Implementation
- III. Graph Analysis and Results

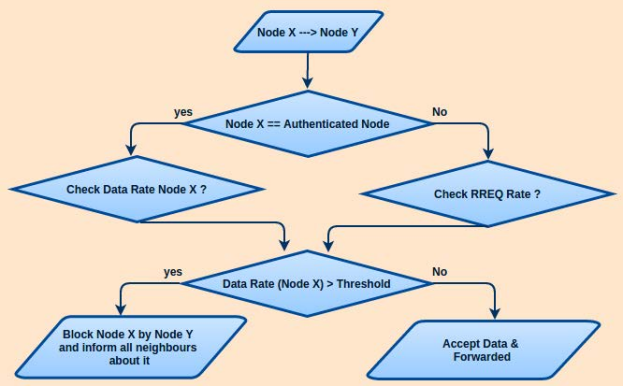

Figure 1. Data Filtration Flowchart.

2.2.1 Data Filtration Algorithm

1) Node X send some data to Node Y.
2) If Node X == Authenticated Node and Node Y == destination node, then Node Y check data rate of Node X.
3) If data rate Node(X) > Threshold Limit, then communication from Node X gets blocked.
4) Node Y informs all the neighbour nodes about this attack.
5) If Node X != Authenticated Node, Node Y checks its requesting rate, if it is exceeding the threshold limit, then Node X also gets blocked in this case.
6) Else Data from Node X is accepted and forwarded to destination or the base station.

2.2.2 Implementation using NS2

Data filtration method for detecting insider and outsider DDoS attacks has been implemented using ns2 simulator[14] with AODV[15,16] as routing protocol for WSN nodes, implementation details as shown in Table 1. Table 2 represents the node communication details under the simulation.

In Table 2, N represents the normal nodes, I-Attackers represent the insider attackers in the network and O-Attackers represent the outsider attackers in the network. Normal nodes send their data to the gateway nodes 10, 20 and 30 respectively. In this simulation both outsider attackers and insider attackers try to bombard the packets either to the normal nodes or to the gateway nodes between 30 to 70 seconds. Nodes which are attacked by the attackers get busy in receiving the packets from the attacker and the normal functioning of the network get degraded. Figure 2 represents the network animator screen-shot.

In the simulation there are two switches one is attack switch and second is control switch. There are two kinds of nodes under simulation, one is normal node and another is attacker node. Following are the three modes of operations:

- Normal Mode: In normal mode, attack switch is off and attackers are inactive, all the normal nodes operate within the threshold limit of the network. The simulation is done under the normal circumstances.
- Attack Mode: In attack mode, attack switch is on, and attacker nodes are active. Attacker nodes attack the normal nodes by sending high volume of data. Here control switch is off hence no filtration of data

is done and attacker has the ability to degrade the performance of the network.

- Control Mode: In the control mode, both attack switch and control switch are on, and hence data filtration is active under the node. In this case node has the ability to recognize the attack and block the attacker node.

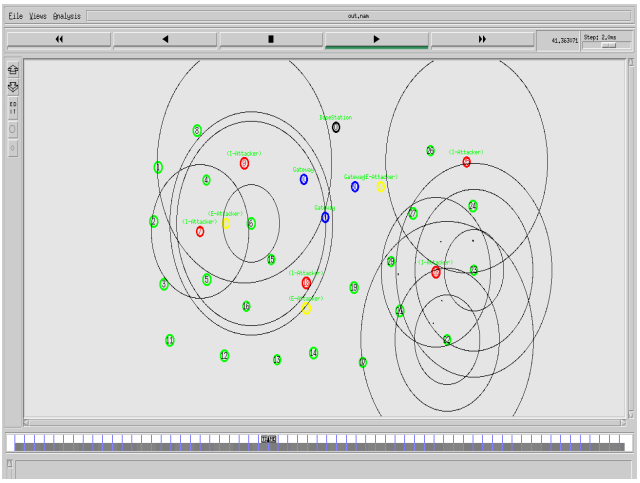

Figure 2. Network Animator Screen-shot.

Table 1. NS2 Implementation Details

NS2 Version	**2.35**	**Transmission Radius**	**250 m**
Energy Model	Energy Model	Initial Energy	1000 J
Ideal Power	0.2	Receiving Power	0.3
Transmission Power	0.4	Sleep Power	.01
Transition Power	0.1	Number of Nodes	33
Simulation Time	100 s	Simulation Modes	Normal, Attack, Control
Gateway Nodes	10,20,30 (Blue)	Attacker Nodes	7,9,18,25, 28,31,32,33
Normal Data Rate / Attack Rate	1 kbps / 40 kbps	Time of Attack	From 30 sec to 70 sec
Routing Protocol	AODV		

Table 2. NS2 Node Communication Details

Sender Node	**Receiver Node**	**Data Rate**
1, 2, 3, 4, 5, 6, 8 (N) (Green)	10 (Blue)	1 KBPS
11, 12, 13, 14, 15, 16, 17, 19 (N) (Green)	20 (Blue)	1 KBPS
21, 22, 23, 24, 26, 27, 29 (N) (Green)	30 (Blue)	1 KBPS
7, 9 (I-Attackers) (Red)	10 (Blue)	40 KBPS
18 (I-Attackers) (Red)	20 (Blue)	40 KBPS
25, 28 (I-Attackers) (Red)	30 (Blue)	40 KBPS
31, 32, 33 (O-Attackers) (Yellow)	6, 19, 30 (respectively)	40 KBPS

2.2.3 Performance Metrics

The network performance has been analyzed based upon following parameters:

- Throughput:: Number of packets sent per unit time. It is measured in kbps.
- PDR (Packet Delivery Ratio): It is defined as the ratio of number of packets sent by sender node to the number of packets successfully received by the receiver node.
- Lost Packets: Number of packets that get lost during the communication between sender and receiver.
- Delay: It is defined as the average time taken by the single data packet between the source and the destination.
- Energy Consumption: The amount of energy in joules that get consumed during the operation of the network.

3. Research Results

When simulation is performed under control mode i.e. when both attack and control switches are on and attack starts at time t = 30 second, attackers are detected one by one and get eliminated from the system very quickly thus preventing the loss of packets in the communication. Figure 3 represents screen-shot of terminal view when simulation is undergoing process. Attacker nodes 18, 31, 32 and 33 are detected at time t=40 seconds, attacker node 9 is detected at time t=45 seconds, attacker nodes

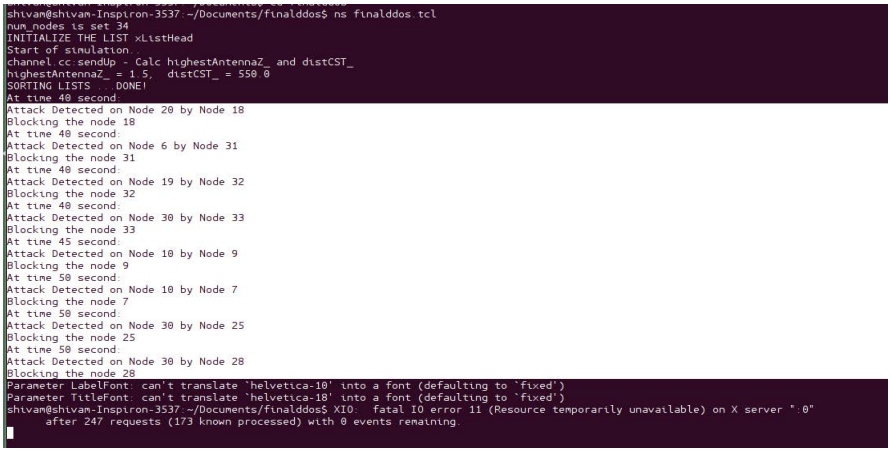

Figure 3. Terminal View Screen-shot.

7, 25 and 28 are detected at time t=50 seconds. So all the attacker nodes get blocked by the time t=50 seconds and results can be seen clearly in the graph deviations at time t=50 seconds.

Figure 4 to Figure 8 represent the different graphs for various performance metrics. All the simulation results under different modes of simulation (Normal mode – Blue Color, Attack mode – Red Color and the Control mode – Orange Color) have been combined for each performance metrics. The deviation of the orange curve from red curve in each graph shows the effectiveness of the data filtration approach.

Table 3 provides the values of various performance metrics under different modes at time t = 80 seconds i.e 20 seconds before the end of simulation.

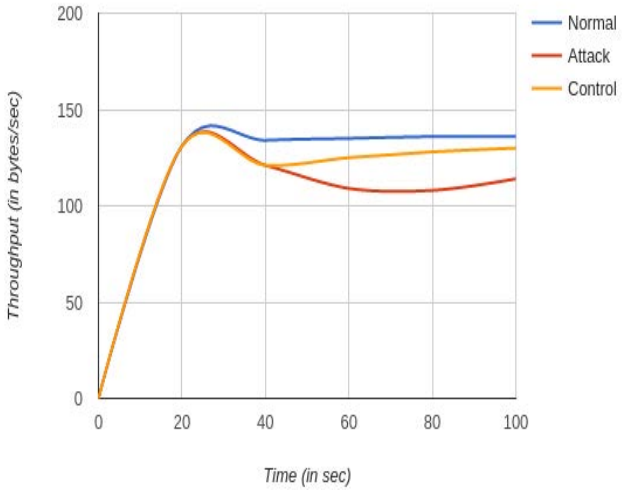

Figure 4. Average Throughput Graph for Normal, Attack and Control Mode.

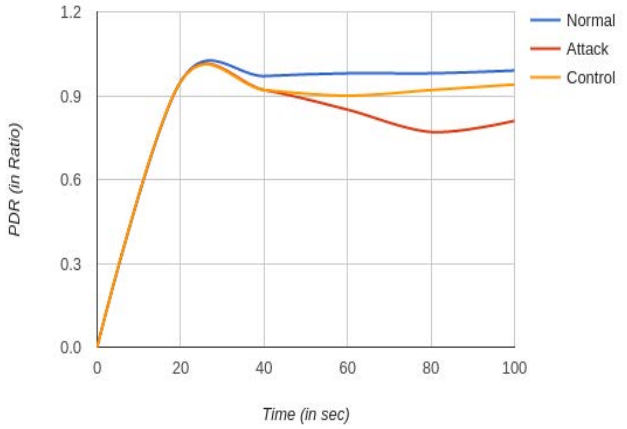

Figure 5. Average PDR Graph combined for Normal, Attack and Control Mode.

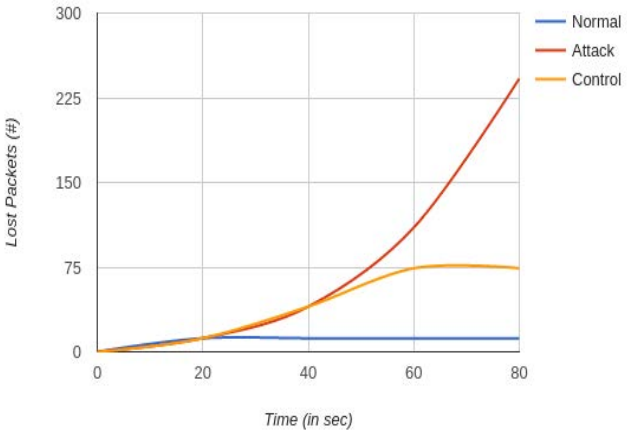

Figure 6. Lost Packets Graph combined for Normal, Attack and Control Mode.

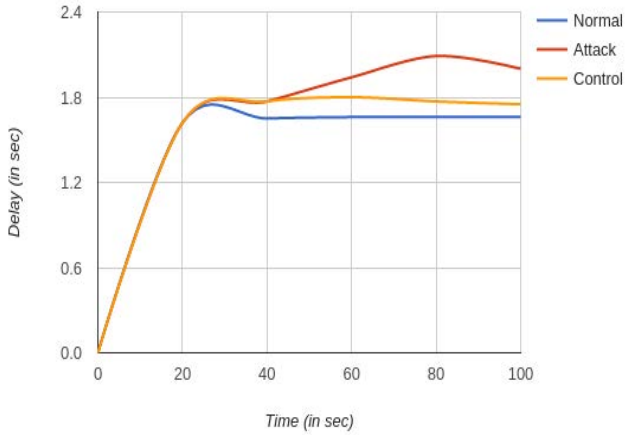

Figure 7. Average Delay Graph combined for Normal, Attack and Control Mode.

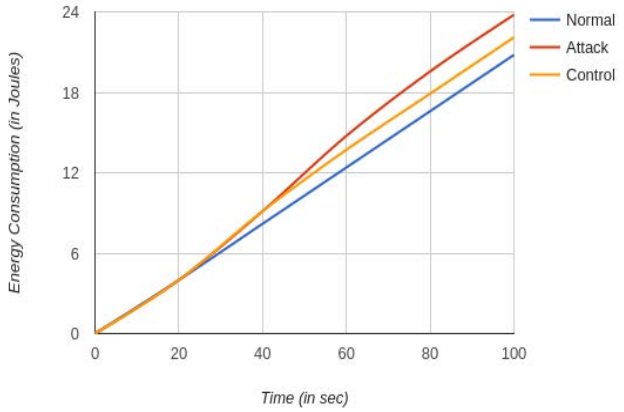

Figure 8. Average Energy Consumption Graph combined for Normal, Attack and Control Mode.

Table 3. Values evaluated for different performance metrics at time t = 80 sec

Simulation Mode	Normal Mode	Attack Mode	Control Mode
Avg. Throughput	135 bytes/ sec	107 bytes/ sec	128 bytes/ sec
Avg. PDR	0.99	0.77	0.93
Lost Packets	15	242	75
Avg. Delay	1.68 sec	2.10 sec	1.77 sec
Avg. Energy	16.40 J	19.80 J	17.90 J

4. Conclusion

The above proposed methods are simple and can be deployed at every node in the network. The DDoS attacks launched in the simulation are detected at very early stages i.e within 20 seconds from the start of the attack. The network performance has improved considerably after blocking the attackers i.e 56% energy is saved while considering 40 seconds of attack time. A little computation and storage resulted from authentication and data filtration methods prevent the whole drainage of node's battery source that can be caused by the DDoS attacks.

5. References

1. Chatterjee A, Pandey M. Practical Applications of Wireless Sensor Network Based on Military, Environmental, Health and Home Applications: A Survey. International Journal of Scientific and Engineering Research. 2014 Jan; 5(1):1–1.
2. Xing K, Srinivasan SSR, Rivera MJM, Li J, Cheng X. Network Security. In: Attacks and Countermeasures in Sensor Networks: A Survey. Springer US. 2010 Jun; 251–72.
3. Sahu SS, Pandey M. Distributed Denial of Service Attacks: A Review. Modern Education and Computer Science. 2014; 1:65–71. Crossref
4. Walters JP, Liang Z, Shi W, Chaudhary V. Security in Distributed, Grid, and Pervasive Computing. In: Xiao Y editor. In: Wireless Sensor Network Security: A Survey. CRC Press: Boca Raton, FL, USA. 2006; 1–50.
5. Palmieri F, Ugo SR, Massimo F, Castiglione FA. Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures. The Journal of Supercomputing. 2015 May; 71(5):1620–41. Crossref
6. Shaikh M, Syed AH. A Survey on Jamming Attacks, Detection and Defending Strategies in Wireless Sensor Networks. International Journal of Research in Engineering and Technology. 2014 Mar; 3(3):1–4.
7. Sahu SS, Pandey M. A Probabilistic Packet Filtering-Based Approach for Distributed Denial of Service Attack in Wireless Sensor Network. In: Jain L, Patnaik S, Ichalkaranje N. editors. Intelligent Computing, Communication and Devices. Advances in Intelligent Systems and Computing. Springer, New Delhi. 2015; 309:65–70. Crossref
8. Kaushal K, Sahni V. Early Detection of DDOS Attack in WSN. International Journal of Computer Applications. 2016 Jan; 134(13):0975–8887.
9. Buch D, Jinwala DC. Denial of Service Attacks in Wireless Sensor Networks. International Conference on Current Trends In Technology. 2010 Dec; 382(481). p. 09–11.
10. Tiloca M, Guglielmo DD, Dini G and Anastasi G. SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks. Emerging Technologies and Factory Automation, IEEE 18th Conference. INSPEC. 2013 Oct. p. 1–8. Crossref
11. Abdallah W, Boudriga N, Kim D, An S. An Efficient and Scalable Key Management Mechanism for Wireless Sensor Networks. Advanced Communication Technology

(ICACT), IEEE 17th International Conference. INSPEC. 2015 Aug. p. 480–93. Crossref
12. Kodali RK. Key Management Technique for WSN. IEEE Region 10 Symposium. INSPEC. 2014 Jul; 540–5. Crossref
13. Morshed M, Islam R. CBSRP: Cluster Based Secure Routing Protocol. Proceedings of Advance Computing Conference (IACC), IEEE 3rd International. INSPEC. 2013 May. p. 571–6.
14. Gautam G, Sen B. Design and Simulation of Wireless Sensor Network in NS2. International Journal of Computer Applications. 2015 Mar; 113(6):1–3. Crossref
15. Karadge PS, Sankpal SV. A Performance Comparision of Energy Efficient AODV Protocols in Mobile Ad hoc Networks. IJARCCE. 2013 Jan; 2(1):1–5.
16. Abdulleh MN, Yussof S, Jassim HS. Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols. Communications and Network. 2015 May; 7:125–37. Crossref