

# Detection and Prevention of Sybil Attack Using Sink Based Detection Mechanism in Wireless Sensor Networks

Mohit Angurala, Manju Bala, Sukhvinder Singh Bamber

1 Research Scholar, IK Gujral Punjab Technical University, Punjab, India, amohitpit@gmail.com

2 Khalsa College of Engineering and Technology, Amritsar, Punjab, India

3 P.U Swami Sarvanand Giri Regional Centre, Hoshiarpur, Punjab, India

**Abstract:** Recent advances in wireless and electronic communications have enabled the deployment of low-cost, low-cost, low-power, multi-function sensors and communicate in a nutshell. Intelligent and economical sensors, connected to the network via wireless links and distributed in large quantities, offer unprecedented opportunities to monitor and control homes, cities and the environment. In addition, sensors connected to the network use a wide range of applications within the defence area, generating new features for recognition and surveillance and various tactical applications. Sybil is one of the most terrible attacks is the cloning attack of the node, where the attacker captures the node and extracts its secret information, create replicas and enter them in the network field other malevolent behaviour. In this paper, to detect and mitigate this attack, sink-based detection schemes have been proposed.

## Introduction

A Wireless device Network (WSN) is formed by many tiny, cheap low memory nodes and less energy, and process capability. In Such specific variety of WSNs, many issues arise to find out every node. Current advancements in wireless transmissions have facilitated to roll-out the cheap, less energy and versatile sensors that are tiny in size and transmit in a miniature distance. Inexpensive and good sensors are associated with the help of wireless channels and positioned in large amount. Moreover, the sensors which are associated or networked use a wide range of applications between the defense area, creating novel potential for intelligence and police work and numerous military science fields. Self-relocation capabilities are often an extremely fascinating sign of wireless device networks. The examples of environmental based applications are water quality checking and agriculture; the measuring data are not at all meaningful. Moreover, location estimation might alter several applications as an example of Intrusion Recognition, Stock Organization, Traffic Monitoring, Health Examination, intelligence and police work.

With all the development inside the reduction and incorporation of the finding and transmission technologies, the system of high level wireless mechanisms uses a considerable amount of economic sensors and low energy consumption previously realized. Within a wireless device system, the nodes of the powered devices are scattered in a physical space. Each device within the sensor network collects information, for example, detection of vibrations, temperature, radiation and various environmental factors.

## 2. Related Work

**R. Upadhyay et.al. [1]** Said that WSNs is a financial as well as problem free answer for a diversity of applications. The open character of wireless sensor networks makes it incapable against a range of security threats. A variety of security attacks like wormhole attack, black hole, distributed denial of service attack. It is likely to work together with the information as well as the sensor node in the network. In this manner, the drainage of the power of the battery unswervingly debases the existence of the node. Moreover, this work considered it a solemn dilemma and planned a resolution to conquer the trouble of power consumption owing to distributed denial of service attack.

**S.Maidhili R et.al.[2]** Said that WSNs are likely to be vulnerable when they select the cluster head between sensor nodes. IDS cannot avoid it or act, but it can only detect it. IDS informs the controller to take the necessary measures when activating the alarms if an attack is detected, which is positive, but also involves a waste of resources and a waste of time in the detection process. Prevention must be carried out in the state of launch of the attack so as to minimize the waste of resources and the consumption of time. Initially, the attacker launches the attack to enter the selection of group heads (CH) that transmit control messages with false information, such as high energy & neighbour counting. The results of the experimental simulation work, to detect attacks at the basic level & improve network performance, to avoid the attack in order to reduce the resource overload and to perform routing & aggregation of data resident in the WSN.

**O,Can et.al. [3]** Proposed that the WSNs is a large-scale network with dozens of hundreds of small devices. The use of WSN fields such as the army, health, the smart home has a large scale and its areas of use are increasing day by day. The WSN safe theme is an important research area & WSN applications have some important security shortcomings. The intrusion detection system is a second line of network security mechanism and is very important for integrity, privacy and availability. Intrusion detection in WSN is something other than wireless networking with no power restrictions, since WSN has some restrictions that affect the types of attacks and cyber security attacks. This paper is a survey that describes the types of attack of WSN intrusion detection approaches that oppose this type of attack.

**S. Rao et. al.[4]** Studied and analyzed the impact of the jam on micaz specks running Tiny OS and explores ways to mitigate the impact. Interference is facilitated by disabling the detection of the carrier on the interference nodes. The interference attack is detected while monitoring RSSI and PDR on the receiver. Varying different parameters in the sender, such as power level, package size, distance with theoretical analysis

**S. Nagar et.al.[5]** Introduced a secure protocol for WSNs, which is capable of overcoming the distributed denial of service attack in the network. In our proposed approach analysis is done on the malicious nodes by means of the methodology and obstructs that node from any other movement in the network. Therefore, in order to defend the network, authors make use of an intrusion prevention scheme in which particular network nodes perform as an intrusion prevention node. Moreover, such nodes run in their radio series for the area of the network and frequently examine nearby nodes. At last, when the intrusion prevention node come across a misbehavior node which engage regular distribution messages apart from user datagram protocol and transmission control messages, the intrusion prevention node lumps the malicious node as well as transmits the information to every original dispatcher nodes to amend its routes.

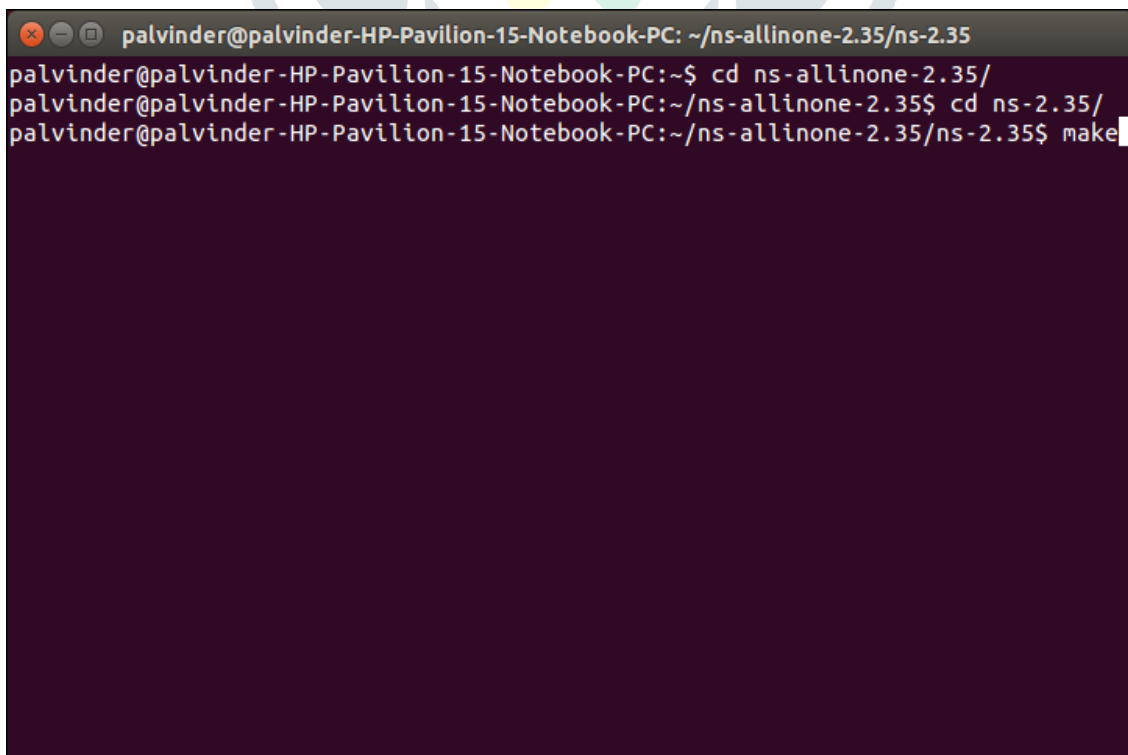
**T.Kaur et. al.[6]** Said that with the advancement and innovation, one of the fundamental concerns nowadays is security. There are a few conceivable assaults on WSN, in DDOS assaults (Distributed Denial of Service), malignant nodes are adjusted to numerous assaults, for example, flood assaults, dark gaps and hot-opening assaults, to stop the general activity of the system. The dangers are considerably more prominent when one talk about military and modern applications. Besides, there are numerous confinements in WSN, for example, constrained battery limit, low bunch limit, and so forth. Showing a security demonstrates that thinks about these confinements and gives security is a noteworthy test nowadays. There are a few instruments proposed by scientists to recognize or shield against this DDOS assault.

**P. Gosavi et. al.[7]** Said that specially appointed wireless systems are dynamic in nature. Ad-Hoc systems don't rely upon any default foundation. At whatever point correspondence is required by then, this system can be executed. In this article they talk about vampire assaults. Vampire assaults are anything but difficult to perform through the system and hard to distinguish. At that point they contrast the new technique and the current convention and Beacon Vector directing. What's more, they reach the resolution that the new convention is better, since it distinguishes and anticipates vampire assaults.

### 3. Implementation Work and Results

There are many techniques which different researchers have proposed in order to attack dos attacks but the major limitation of them is the congestion among those nodes. Due to congestion, the drainage of battery becomes fast and nodes become dead rapidly. So, in this research work, we will distribute the traffic among gateway nodes so as to minimize the traffic load and to enhance the battery depletion problem. Therefore as per the literature survey conducted, the problem is the traffic among every node as every node becomes busy in detection DOS attack.

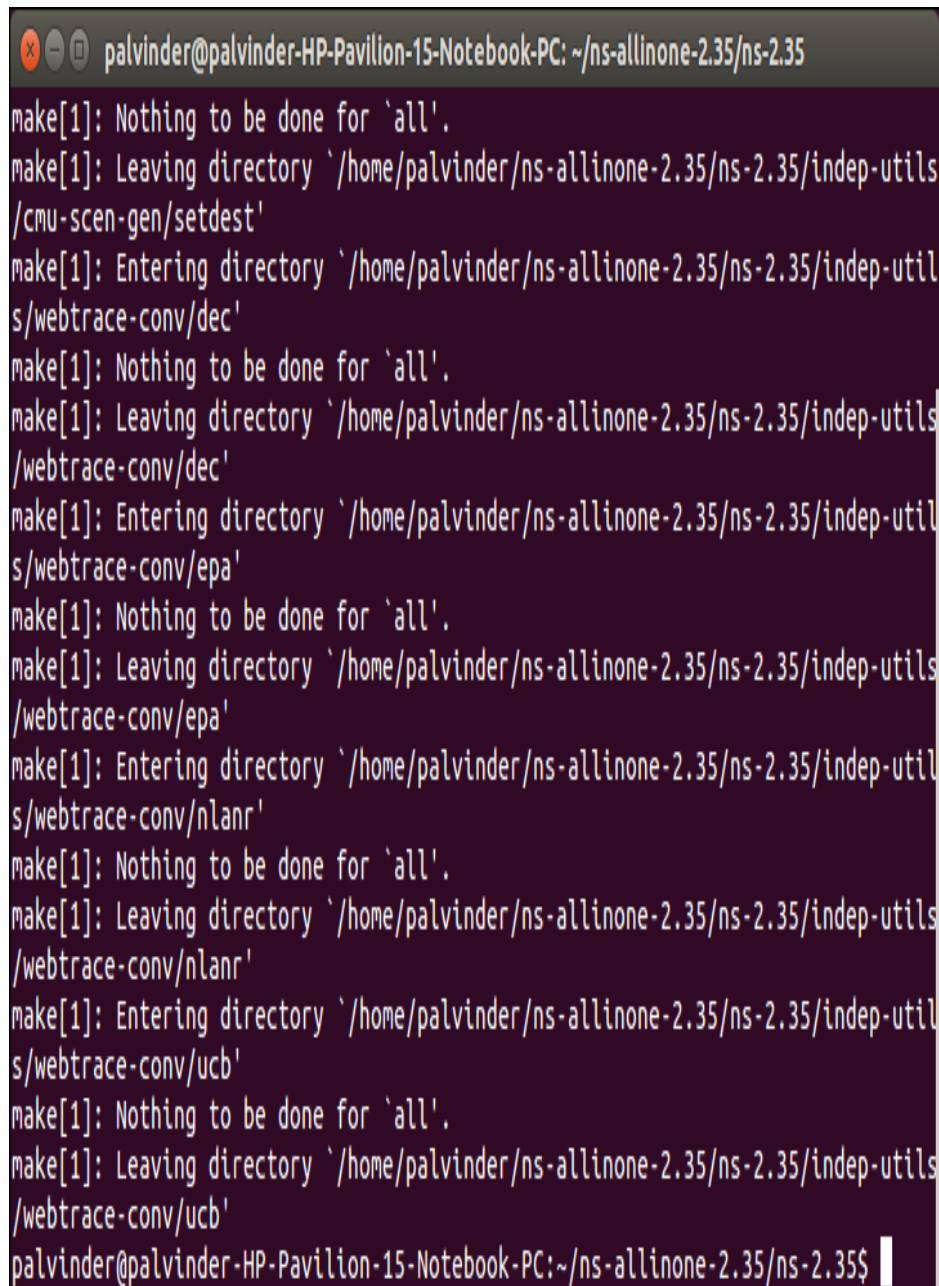
In the implementation work, firstly we diffused area as 1000\*1000 m2, then number of nodes can be taken 50 and traffic type is constant bit rate. Further omni directional antenna type is used. When the simulation is run we have varied number of mobile connectors as 5, 10, 15, 20.



```
palvinder@palvinder-HP-Pavilion-15-Notebook-PC: ~/ns-allinone-2.35/ns-2.35
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~$ cd ns-allinone-2.35/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/ns-allinone-2.35$ cd ns-2.35/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/ns-allinone-2.35/ns-2.35$ make
```

Figure 1. Make Command to Refresh NS2

In the above figure we have used make command to refresh the changes. We have made while doing simulation , this make command is used in the command live as shown in figure above. After this make command , now we are in a position to run our scenario and gathered the results .

A terminal window screenshot showing the output of a 'make' command. The terminal title is 'palvinder@palvinder-HP-Pavilion-15-Notebook-PC: ~/ns-allinone-2.35/ns-2.35'. The output consists of a series of messages: 'make[1]: Nothing to be done for `all`.', 'make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/cmu-scen-gen/setdest`', 'make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/dec`', 'make[1]: Nothing to be done for `all`.', 'make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/dec`', 'make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/epa`', 'make[1]: Nothing to be done for `all`.', 'make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/epa`', 'make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/nlanr`', 'make[1]: Nothing to be done for `all`.', 'make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/nlanr`', 'make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/ucb`', 'make[1]: Nothing to be done for `all`.', 'make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils/webtrace-conv/ucb`', and finally 'palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/ns-allinone-2.35/ns-2.35\$'.

```
palvinder@palvinder-HP-Pavilion-15-Notebook-PC: ~/ns-allinone-2.35/ns-2.35
make[1]: Nothing to be done for `all`.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-utils
/cmu-scen-gen/setdest'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/dec'
make[1]: Nothing to be done for `all`.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/dec'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/epa'
make[1]: Nothing to be done for `all`.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/epa'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/nlanr'
make[1]: Nothing to be done for `all`.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/nlanr'
make[1]: Entering directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/ucb'
make[1]: Nothing to be done for `all`.
make[1]: Leaving directory `/home/palvinder/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/ucb'
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/ns-allinone-2.35/ns-2.35$
```

Figure 2. Scenario with Make Successful

In this figure, the make command success is depicted. After that the ddos.tcl is run as shown below, which is a tcl command. When this tcl command is run, it will first show the number of nodes taken in a scenario. Further simulation is setup and now we are in a position to run our proposed work.

```

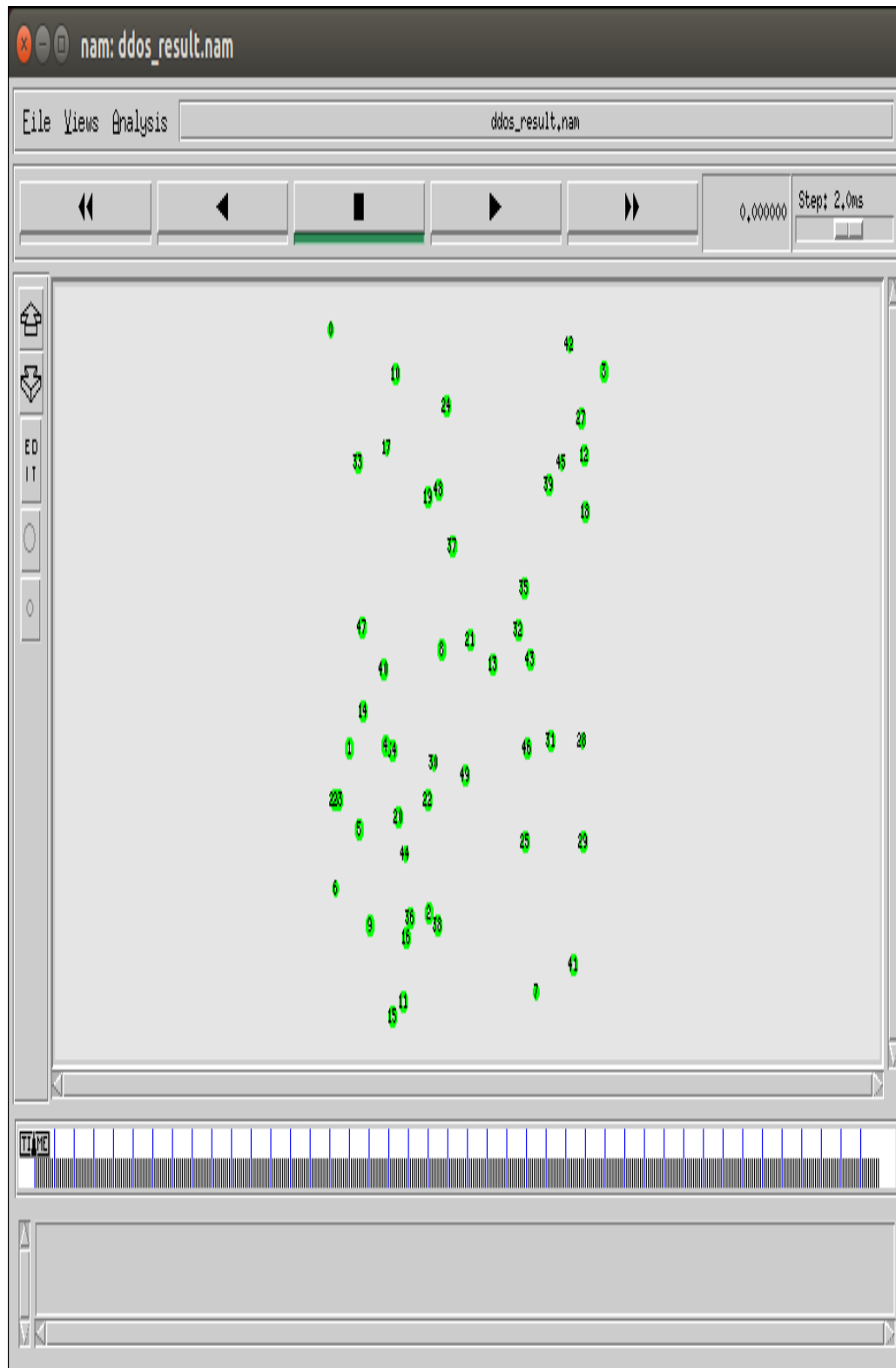
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~$ cd Desktop/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop$ cd simulation/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ ns ddos.tcl
num_nodes is set 50
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
Loading scenario file...
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ...DONE!
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
; Sending pkt up the stack on default.

NS EXITING...
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44i am 44 and dest is @data dropped by 44i am 44 and dest is @palvinder@pa
lvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ nam ddos_result.nam

```

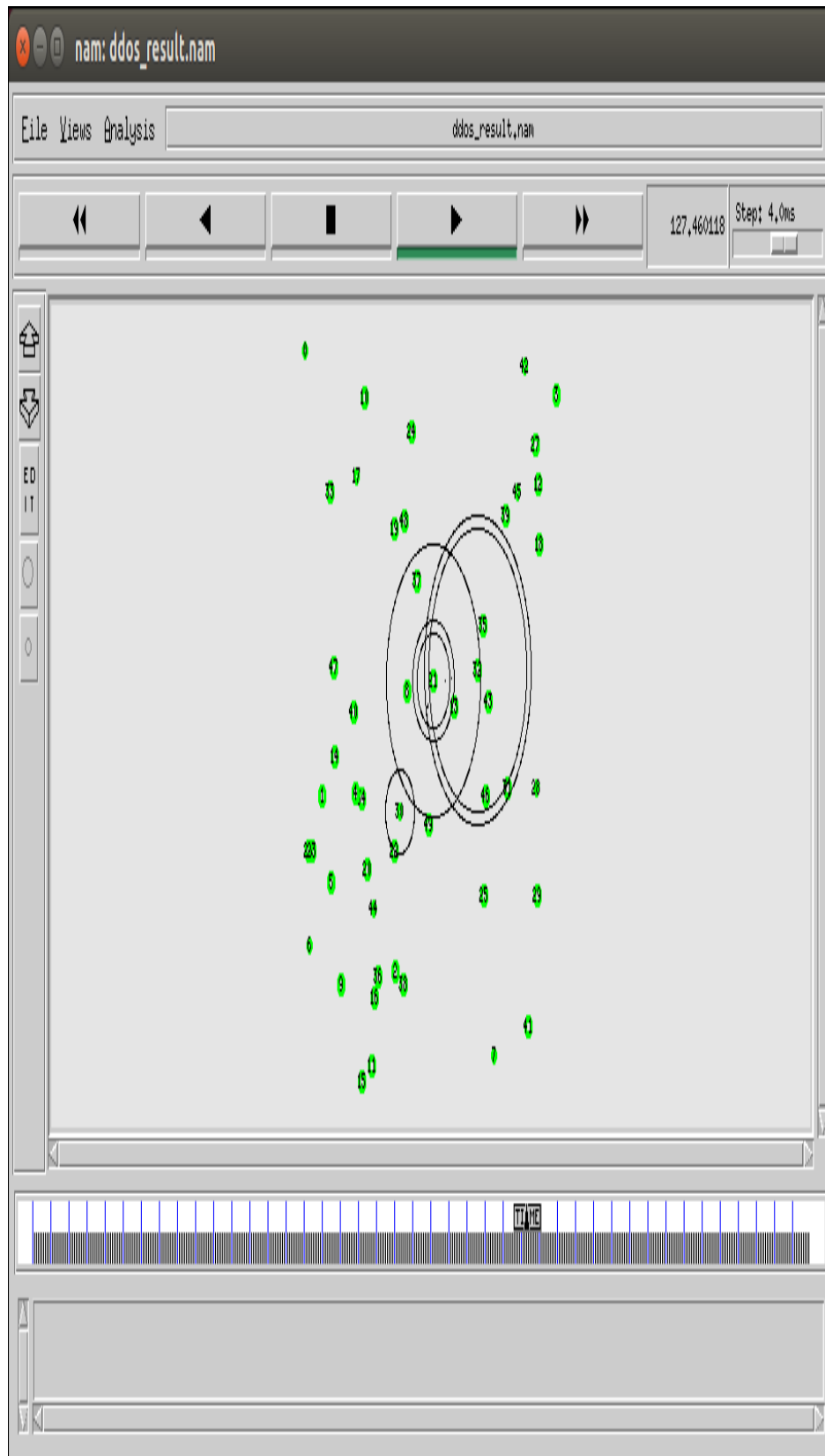
**Figure 3. Simulation Complete**

This diagram indicates that the scenario has successfully been completed and NS is exited. Now, we can use name file for looking into the scenario part and look for simulation.



**Figure 4. Deployment of various nodes in a network**

The above figure shows that the deployment of various nodes in which number of nodes is from 1 to 50. Here the animation file can be run by using play button indicated on the top button and then we can increase the simulation speed using right top scroll button.



**Figure 5. Animation to Show Flooding Attack**

This animation diagram indicates the flooding by various nodes in a circle. The flooding is indicated by the number of circles in a nam file as shown in the above diagram.

This next figure represents the command to calculate various parameters



```

palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~$ cd Desktop/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop$ cd simulation/
palvinder@palvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ ns ddos.tcl
num_nodes is set 50
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
Loading scenario file...
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ...DONE!
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44direction for pkt-flow not specified
; Sending pkt up the stack on default.

NS EXITING...
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44data dropped by 44
data dropped by 44data dropped by 44data dropped by 44data dropped by 44i am 44 and dest is 0data dropped by 44i am 44 and dest is 0palvinder@pa
lvinder-HP-Pavilion-15-Notebook-PC:~/Desktop/simulation$ awk -f packetdeliverratio.awk ddos_result.tr
    
```

Figure 6. Command to calculate various parameters

**Results**

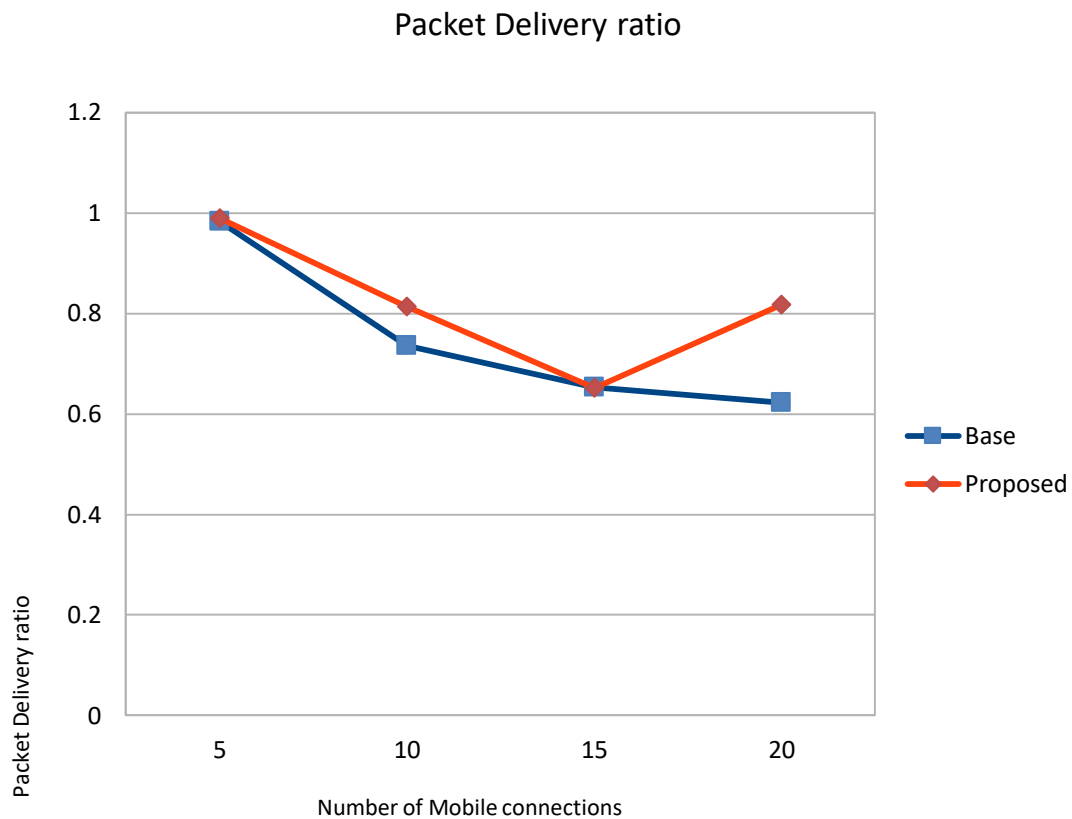
**Performance Metrics**

**1. Packet Delivery ratio**

The package distribution ratio in this simulation is defined as the ratio between the number of packets sent by the constant bit rate sources (CBR, application level) and the number of receiver packets per CBR receives in the destination Table.

**Table 1: Packet delivery ratio**

No of mobile connections	Base work	Proposed work
5	0.9835	0.9896
10	0.7358	0.8132
15	0.6525	0.6519
20	0.6226	0.818



**Figure 7. Packet Delivery Ratio**

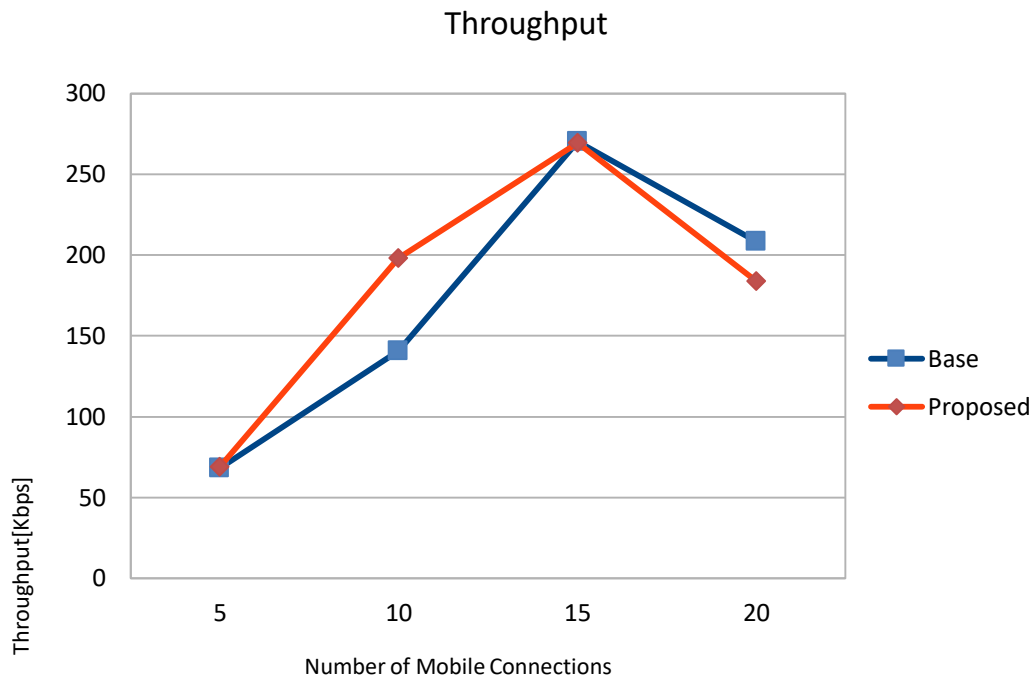
When we set up the number of mobile connections as 5 the packet delivery ratio in case of base work is .9835 while the value in our case appears to be .9896 which is better than our work. Further when the mobile connection is 10 the packet delivery ratio of base work is 0.7358 while value of our work is 0.8132. Again when number of mobile connection is 15 then the packet delivery ratio in base work is 0.6525 and our work value is 0.6519. Again when no of mobile connection is 20 then the packet delivery ratio of base work is 0.6226 but our work value is 0.818. Overall to conclude, our work is better than base work.

**2. Throughput:** Throughput is total packets success fully delivered to individual destinations in excess of total time.

**Table 2. Throughput**

No of mobile connection	Base work	New work
5	68.13	68.82
10	140.78	198.02
15	270.3	269.45
20	208.23	183.97





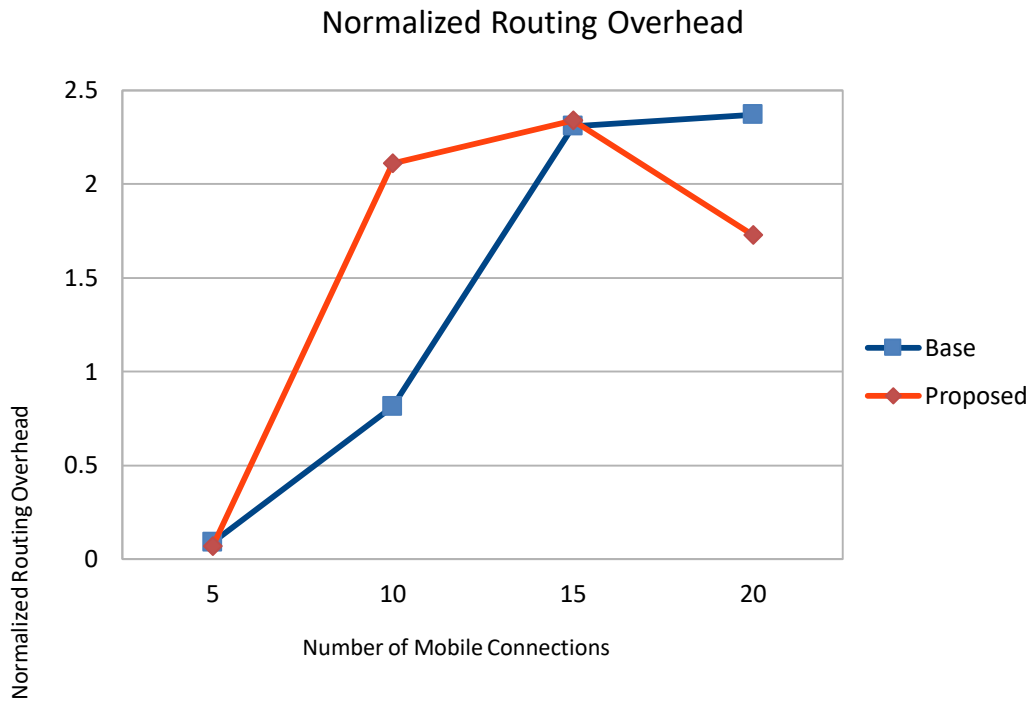
**Figure 8. Throughput Analysis**

When we set up the number of mobile connections as 5 the Throughput in case of base work is 68.13 while the value in our case appears to be 68.82 which is better than our work. Further when the mobile connection is 10 the Throughput of base work is 140.78 while value of our work is 198.02. Again when number of mobile connection is 15 then the Throughput in base work is 270.3 and our work value is 269.45. Again when no of mobile connection is 20 then the Throughput of base work is 208.23 but our work value is 183.97. Overall trend again suggests that our work is better than base work.

**3. Normalized Routing Overhead (NRL):** NRL is defined as Normalized Routing Load Ratio of network control packets to all delivered packets.

**Table 3. Normalized Routing Overhead**

No of mobile connection	Base work	New work
5	0.088	0.068
10	0.814	2.109
15	2.309	2.339
20	2.369	1.727



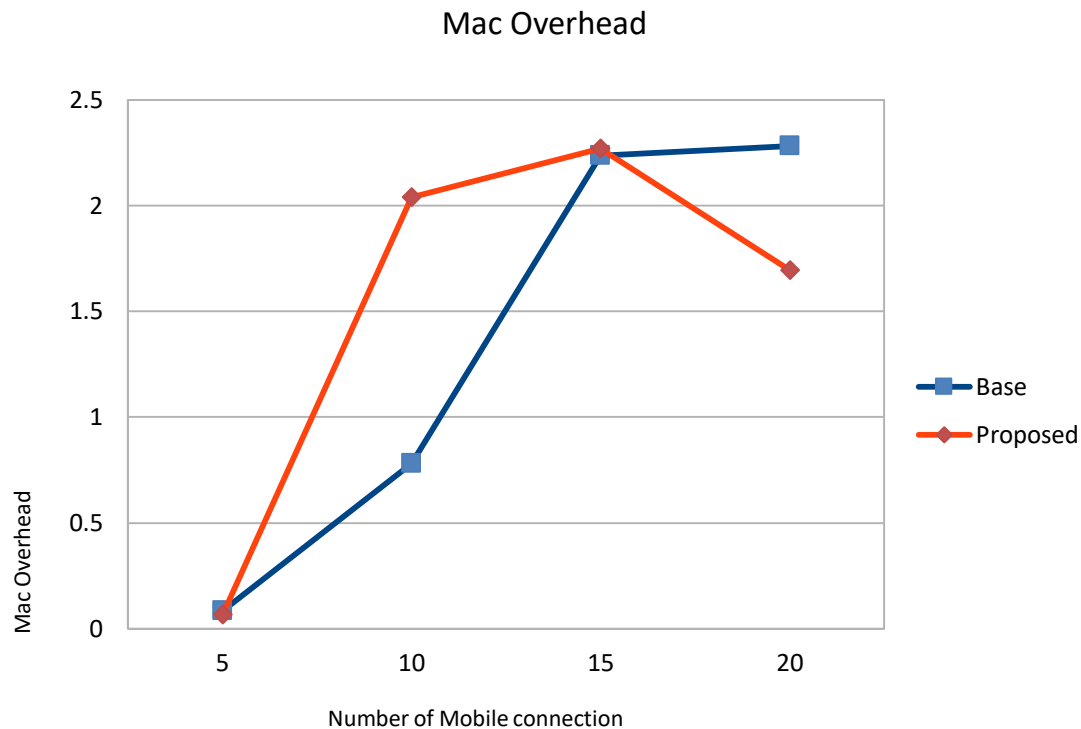
**Figure 9. NRL Analysis**

When we set up the number of mobile connections as 5 the NRL in case of base work is 0.088 while the value in our case appears to be 0.068 which is better than our work. Further when the mobile connection is 10 the NRL of base work is 0.814 while value of our work is 2.109. Again when number of mobile connection is 15 then the NRL in base work is 2.309 and our work value is 2.339. Again when no of mobile connection is 20 then the NRL of base work is 2.369 but our work value is 1.727. Overall trend again suggests that our work is better than base work.

**4. MAC Overhead:** MAC overhead is defined as *ratio of MAC control packets to all delivered packets.*

**Table 4. MAC Overhead**

No of mobile connection	Base work	New work
5	0.085	0.066
10	0.779	2.04
15	2.237	2.269
20	2.283	1.695



**Figure 10. MAC Overhead Analysis**

When we set up the number of mobile connections as 5 the MAC Overhead in case of base work is 0.085 while the value in our case appears to be 0.066 which is better than our work. Further when the mobile connection is 10 the MAC Overhead of base work is 0.779 while value of our work is 2.04. Again when number of mobile connection is 15 then the MAC Overhead in base work is 2.237 and our work value is 2.269. Again when no of mobile connection is 20 then the MAC Overhead of base work is 2.283 but our work value is 1.695. Overall trend again suggests that our work is better than base work.

#### 4. Conclusion

One of the most alarming attacks in the WSN is the cloning attack of the nodes where the attacker takes the details of the node and collects their personal data, duplicates them and inserts them into the network field for further malicious activities. To detect and eliminate this type of attack, different detection techniques have been designed based on both static and mobile WSNs.

The base work is compared with the proposed approach, which further suggests that proposed approach is better in case of Throughput, Packet Delivery ratio and delay.

Future Work can be done by taking large network with thousands of nodes because when the network gets large, the complexity gets increases, and hence maintaining such a large list is a difficult task.

#### References

- [1] R.Upadhyay, S. Khan, H. Tripathi, U. Rathore Bhatt, "Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain," Intl. Conference on Computing and Network Communications (CoCoNet'15), 2015.
- [2] S.Maidhili R, Karthik GM, "Intrusion Detection and Prevention Based on State Context and Hierarchical Trust in WSNs," International Conference on Computer Communication and Informatics, Coimbatore, INDIA, 2018.
- [3] O. Can and O. Sahingoz, "A Survey of Intrusion Detection Systems in WSNs," IEEE, 2015.
- [4] S. Rao, Deepak S and P. Pradeep, "Parametric Analysis of Impact of Jamming in WSNs," IEEE, 2013.
- [5] S.Nagar, S.S Rajput, A.K Gupta and M.C Trivedi, "Secure Routing Against DDoS Attack in WSNs," 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT), 2017.
- [6] T. Kaur , K. Saluja and A. Sharma, " DDOS Attack in WSN: A Survey," IEEE International Conference on Recent Advances and Innovations in Engineering, Jaipur, India, 2016.
- [7] P.. Gosavi and B. Patil, "Draining Life from Wireless Ad-hoc Sensor Networks," International Journal of Computer Applications (0975 – 8887) Volume 144 – No.9, June 2016.

- [8] V.Nigam, S.Jain and K. Burse, "Profile based Scheme against DDoS Attack in WSN," Fourth International Conference on Communication Systems and Network Technologies, 2014.
- [9] A .Abidoeye and I. Obagbuwa, "DDoS attacks in WSNs: detection and countermeasures," IET Wireless Sensor System, 2018, Vol. 8 Iss. 2, pp. 52-59, The Institution of Engineering and Technology 2017.
- [10] N. Shone and Q. Monnet "Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures," IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015.
- [11] C.Kavitha, "Complete Study on Distributed Denial of Service Attacks in the Presence of Clock drift," ICICES2014, Chennai, Tamil Nadu, India, 2014.
- [12] V. Kansal and M. Dave, "Proactive DDoS Attack Detection and Isolation," International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017.
- [13] K. S. Bhosale, M. Nenova and G. Iliev, "The Distributed Denial of Service Attacks (DDoS) Prevention Mechanisms on Application Layer," IEEE, 2017.
- [14] S. Lakshminarasimman , S.Ruswin and K.Sundarakantham, "Detecting DDoS Attacks using Decision Tree Algorithm," 4th International Conference on Signal Processing, Communications and Networking, Chennai, INDIA,IEEE, 2017.
- [15] A. Kaur, D. Kaur and Gagandeep "DDOS Attack Detection on WSNs: A Review" International Journal of Innovative Research in Science, Engineering and Technology (A High Impact Factor & UGC Approved Journal) Vol. 6, Issue 8, August 2017.
- [16] M. Shinde and D. Mehetre, "Black Hole and Selective Forwarding Attack Detection and Prevention in WSN," IEEE, 2017.
- [17] Y. Liu, M. Dong and A. Liu, "Active trust – secure and trustable routing in WSN," IEEE, 2016.
- [18] Z.Zheng, and A. Liu, "Energy and Memory Efficient Clone Detection in WSNs," 32nd Annual IEEE International Conference on Computer Communications, IEEE INFOCOM, 2013.