Mitigation of Sybil Attack on A Campus Network (CANET) Using Inter-Arrival Time Threshold and Physical Address Comparison

Victor Onomza Waziri
Federal University of Technology Minna
36 PUBLICATIONS **81** CITATIONS
SEE PROFILE

Morufu Olalere
Federal University of Technology Minna
23 PUBLICATIONS **90** CITATIONS
SEE PROFILE

Shafi'i Muhammad Abdulhamid
Federal University of Technology Minna
109 PUBLICATIONS **1,484** CITATIONS
SEE PROFILE

Ismaila Idris
Federal University of Technology Minna
42 PUBLICATIONS **339** CITATIONS
SEE PROFILE

Mitigation of Sybil Attack on A Campus Network (Canet) Using Inter-Arrival Time Threshold and Physical Address Comparison

Onomza Victor Waziri, Balikis Bukola Jimoh, MarufuOlalere, shafi'i Muhammad Abdulhamid ,ismailaidris
Department of Cyber Security, Federal University of Technology, Minna, Nigeria.
onomzavictor@gmail.com, jbalikis8@gmail.com, lerejide@futminna.edu.ng, shafii.abdulhamid@futminna.edu.ng, ismi.idris@futminna.edu.ng

ABSTRACT
A particularly detrimental attack ravaging campus and ad hoc networks is the Sybil attack, where a node illegally claims more than one identity, targeting honest and genuine nodes, thereby weaken or disrupting the system. This research work aimed at designing a mitigation mechanism to combat the attack on a Campus network (CANET). Setting threshold and checking for IP address spoofing by comparing nodes physical addresses is the focus of this work. The success of the algorithm is validated by simulation, and quality of service is guaranteed with regards to the detection rate and packet delivery ratio.

Keywords: *Campus network, Computer security, Inter-arrival time, Sybil Attack*

1 INTRODUCTION

Computer security threats are persistently inventive, master of deception and exploitation, these threats regularly evolve to look for novel means to disturb, steal and destroy. Many attacks exist that hinge on the issue of identity (Tran, 2012). Any decentralized distributed arrangement of network is mostly prone to Sybil attack in which a nefarious node pretend to be numerous dissimilar nodes, known as Sybil nodes, at the same time in an attempt to disrupt the appropriate working of the network (Balachandran & Sanyal, 2012).

In computer security, a Sybil attack is a kind of attack in which a system with reputation is disrupted by creating fake identities in peer-to-peer networks (Patra, 2014). it is a threat on computer system or network where an adversary generates as multiple false identities as possible, launches attacks via these fake identities because they pretends as different entities. Such identities itself often becomes undetectable (Patra, 2014). It is an invasive problem in many areas such as using more than one IP addresses to submit votes resulting to manipulation of Internet opinion poll, is a notable and key problem in real-world elections and to get benefit in any outcome of a chain letter. Some organizations also use it to increase the rating of Google Page Rank of their customers to mention a few (Levine, Shields, & Margolin, 2006).

With the innovation and evolution of IT world, security has still remained as an ever increasing challenge of a campus network. Campus network is a self-sufficient network that university control which is within a local geographical place and sometimes it may exist as a metropolitan area network (MAN). Campus area network is an exclusive local area network (LAN) or set of intertwined LANs serving a government, cooperation, agency, university or similar organization (Ali, Hossain, &Parvez, 2015). Sybil attack is a breach against identity where single entity pretends to have multiple identities at the same time. The Sybil attack is a central problem in many network of which a campus network (CANET) is not an exception and repelled a generally applicable solution so far.

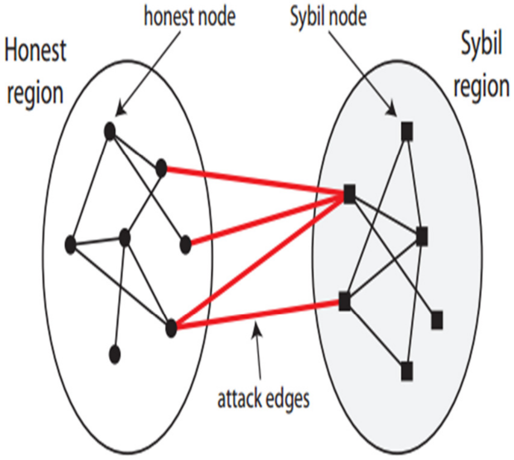


Figure 1: A simple illustration of Sybil nodes been created from Honest nodes (Tran, 2012)

2 RELATED WORK

According to Zanga et al (2013), they tried to detect Sybil nodes in anonymous communication system by trying to find out challengers identity in the network and the proposed two-class undirected mixed membership stochastic block models to discover adversary's Sybil identities in the network and a matrix B to illustrate the communication likelihood of Sybil and genuine nodes that can be used to monitor infected condition of the system. This result in a generative model that is use for resolving the difficulty in Sybil discovery and make it known that Sybil nodes cannot only be part from genuine nodes except that it should also notice the network infected condition.

Trifunovicand and Hossmann (2014) present an anatomy of Sybil attack in opportunistic network by studying the types and efficiency of Sybil attack that are achievable in opportunistic network under a variety of resource restriction on the aggressor. They use two real traces and a mobility model to measure the strong point of Sybil attacks on OppNets, depending on used resources and on how the attack is put into action and they were able to discovered that that OppNets come with additional challenges as well as useful properties

In another research work (Jangir&Hemrajani, 2016) did evaluation of Black hole, Wormhole and Sybil Attacks in Mobile ad-hoc network so as to examine and improve the performance of network This work entails implementing and analyzing three major attacks namely Blackhole, Wormhole and Sybil attack. With the aid of huge number of simulation processes the working methodology of these attacks along with their potential effect on network performance parameters are evaluated. The simulation results has proven that the Sybil attack is more influential one when compared with black hole and wormhole attack because it's method of creating false identities are hard to avoid during the route discovery process. Saranya (2014) conducted a research on the detection of Sybil attack on social network using defender algorithm to spot Sybil node in a distributed platform. The method used was the Sybil defender algorithm which has two techniques, Sybil discovery algorithm and Sybil community recognition algorithm, it was deduced that the technique yield excellent result as it minimizes the time complexity when judge with Sybil detection algorithm before now.He proposed that the method should be used in other decentralized system other than on social network to know if the desired result will be achieved.

Also, Frey, Guerraoui, Kermarrec and Rault (2015) did a collaborative filtering under a Sybil attack of a Privacy threat by analyzing the impact of an active Sybil attack on user-based collaborative filtering recommenders by proposing User-based collaborative-filtering implementing provided by Mahout 0.9, a machine-learning library developed by the apache foundation. The output shows that while the attack is generally effective, some users get natural protection from their inherent similarity with other users in the system. Confirming the results on different datasets and on different variants of the recommenders is to be done in the future.

3 METHODOLOGY

A sufficient implementation of detection and mitigation technique to combat Sybil attack on a CANET is deployed in this section.Though there is no by and large acknowledged way out to the Sybil attack, a number of approaches for various blend of platforms and attacks have been proposed in the literature. This research work focuses on the development of algorithm that set a threshold for all the nodes by getting the inter arrival time and also comparing the physical address of all nodes with the one on the routing table so that we can detect if the IP address is being spoofed using simulation. Inter-arrival time threshold is a localization algorithm and demonstrated to be most efficient used in detecting a node as mean because it is the requirements that knows the genuine time stamp of when a message is transmitted and when it arrive at the anchor node, this reason make it stringent for strict time synchronization of the whole network. If a node is legitimate, it should not take more than certain period of time (threshold) to get to the verification algorithm, if otherwise we will mark such node as Sybil and further check the physical address of such node which always turns out to be illegitimate node.

Security characteristics a CANET should possess include non-repudiation, integrity and confidentiality. Non-repudiation in the sense that a node will not have the ability to deny the fact that he sent a broadcast (message), this scenario can arise when the network is being under Sybil attack and can cause disruption on the network. Also worth mention is integrity, information sent from a node to the other must be genuine and this is not achievable if the Sybil nodes breach the security of the campus network. On a CANET, steps must be taken to ensure that unauthorized users have no access to confidential information especially via masquerading which can be achieved through authorization and authentication. This approach is effective as it will keep all incoming nodes in check.

3.1 PROPOSED METHODOLOGY

Any link or node can initiate the identification of the Sybil node. It is worthy to say in this paper the sender node does the detection. Threshold was set, so if the threshold time is met it will receive reply messages with physical address else it will add the node as fake/ Sybil node. Furthermore, comparison is made if multiple nodes reply with the same physical address but different logical address. If yes add node as Sybil node, if no acknowledge the node as honest node.

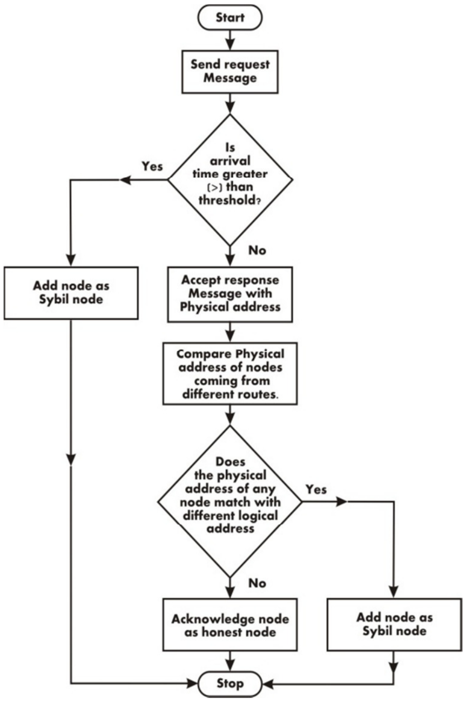

Start
Send request Message
Is arrival time greater (>) than threshold?
Yes
No
Add node as Sybil node
Accept response Message with Physical address
Compare Physical address of nodes coming from different routes.
Does the physical address of any node match with different logical address
Yes
No
Acknowledge node as honest node
Add node as Sybil node
Stop

Figure 2: Flow chart for detection and mitigation of Sybil nodes.

3.2 Tools Used

To implement this research work simulation need to be carried out on OPNET modeler. OPNET gives a detailed development platform supporting the modeling of communication/ interacting networks and distributed systems. Performance and behavior of modeled systems are both modeled and can be analyzed by carrying out discrete event simulations as stated by (LUMS, 2016); it also possess graphical specification which give instinctive mapping from the modeled system.

3.3 Proposed Method Implementation

The implementation of the proposed approach was done based on the simulation parameters summarized in Table 1.

TABLE 1: SIMULATION PARAMETERS

Simulation parameter	Value
Simulation Area	100km X 100km
Simulation Time	200 seconds
Seed value	191
Number of normal nodes	73
Number of Sybil nodes	4
Inter-arrival threshold	Constant (1.0)

SCENARIO 1

This is the CANET Baseline scenario architecture in opnetmodeller showing the different units and departments in the Campus network. The baseline scenario implements the network with the normal traffic without any malicious node such as the Sybil node. This is depicted in Figure 2

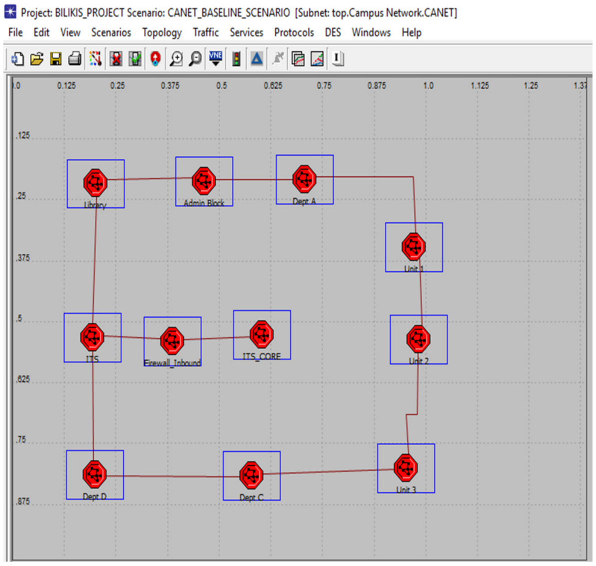

Project: BILIKIS_PROJECT Scenario: CANET_BASELINE_SCENARIO [Subnet: top.Campus Network.CANET]
File Edit View Scenarios Topology Traffic Services Protocols DES Windows Help
Library
Admin Block
Dept A
Unit 1
ITS
Firewall_Inbound
ITS_CORE
Unit 2
Dept D
Dept C
Unit 3

Figure 2: CANET Baseline Scenario

SCENARIO 2

Scenario 2 is implemented by adding 4 malicious (Sybil) nodes to the entire network. Figure 3 and 4 show Sybil nodes 2, 3 and 4 added to the network to transmit malicious packets to the servers.

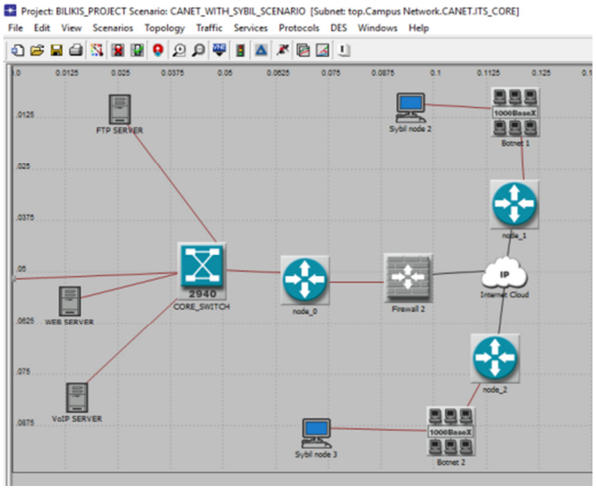

Project: BILIKIS_PROJECT Scenario: CANET_WITH_SYBIL_SCENARIO [Subnet: top.Campus Network.CANET.ITS_CORE]
File Edit View Scenarios Topology Traffic Services Protocols DES Windows Help
FTP SERVER
Sybil node 2
1000BaseX
Botnet 1
node_1
2940
CORE_SWITCH
node_0
Firewall 2
IP
Internet Cloud
WEB SERVER
node_2
VoIP SERVER
Sybil node 3
1000BaseX
Botnet 2

Figure 3: 2 Sybil nodes on the network

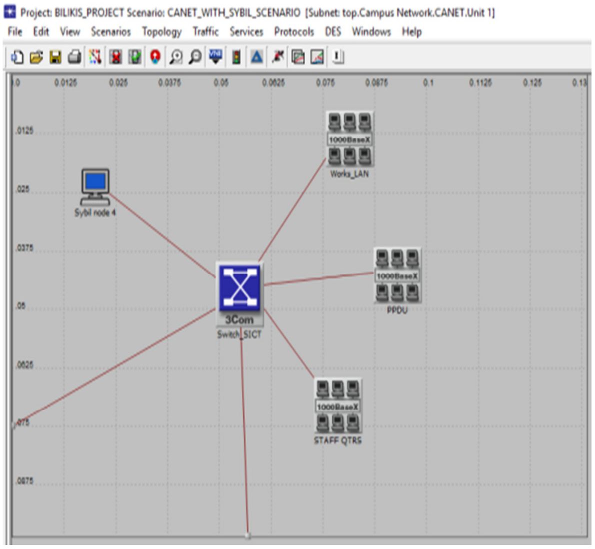
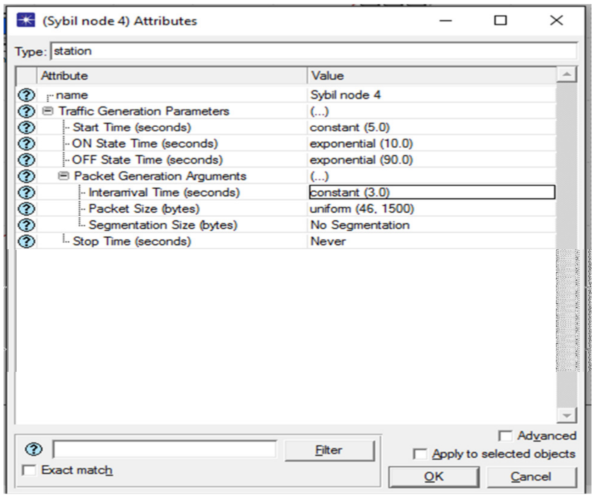

Project: BILIKIS_PROJECT Scenario: CANET_WITH_SYBIL_SCENARIO [Subnet: top.Campus Network.CANET.Unit 1]
File Edit View Scenarios Topology Traffic Services Protocols DES Windows Help
Sybil node 4
1000BaseX
Works_LAN
3Com
Switch_SICT
PPDU
STAFF QTRS

Figure 4: 2 Sybil node 4 on the network

The Sybil nodes are configured to transmit malicious packets which have packet inter-arrival time greater than the set threshold value. The Sybil node configuration setting is shown in Figure 3.10


(Sybil node 4) Attributes

Type: station

Attribute	Value
name	Sybil node 4
⊟ Traffic Generation Parameters	(...)
Start Time (seconds)	constant (5.0)
ON State Time (seconds)	exponential (10.0)
OFF State Time (seconds)	exponential (90.0)
⊟ Packet Generation Arguments	(...)
Interarrival Time (seconds)	constant (3.0)
Packet Size (bytes)	uniform (46, 1500)
Segmentation Size (bytes)	No Segmentation
Stop Time (seconds)	Never

Figure 5: Sybil node configuration

SCENARIO 3

Scenario 3 implements the CANET with the Sybil mitigation IDS. The Packet Discarder acts as a filter that constantly checks the inter-arrival pattern of inbound packets with respect to their MAC signatures. Any source whose packet arrives beyond the threshold inter-arrival time is blacklisted and the packet discarded and the routing table updated for rerouting of packets within the network. Figure 3.11 shows the scenario 3 implementation with the Packet Discarder.

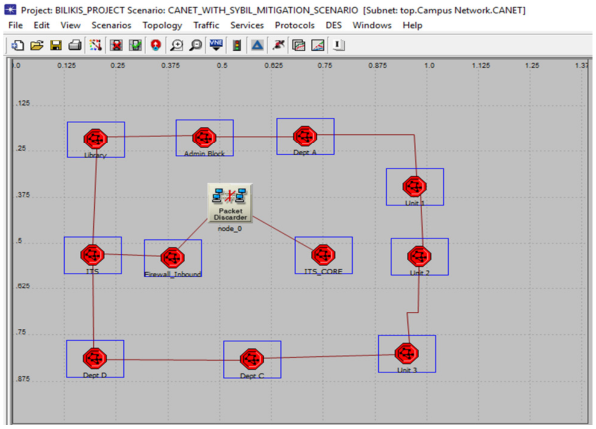
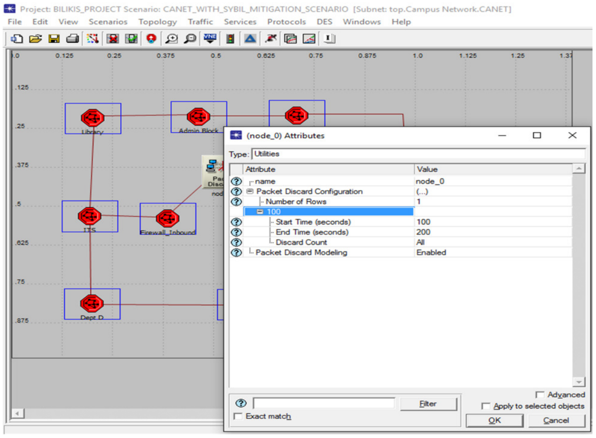

Project: BILIKIS_PROJECT Scenario: CANET_WITH_SYBIL_MITIGATION_SCENARIO [Subnet: top.Campus Network.CANET]
File Edit View Scenarios Topology Traffic Services Protocols DES Windows Help
Library
Admin Block
Dept A
Unit 1
Packet Discarder
node_0
ITS
Firewall_Inbound
ITS_CORE
Unit 2
Dept D
Dept C
Unit 3

Figure 6: Packet Discarder on the network

The configuration of the Discarder node is shown in Figure 7


Project: BILIKIS_PROJECT Scenario: CANET_WITH_SYBIL_MITIGATION_SCENARIO [Subnet: top.Campus Network.CANET]
File Edit View Scenarios Topology Traffic Services Protocols DES Windows Help
Library
Admin Block
ITS
Firewall_Inbound
Dept D

(node_0) Attributes

Type: Utilities

Attribute	Value
name	node_0
⊟ Packet Discard Configuration	(...)
Number of Rows	1
⊟ 100	
Start Time (seconds)	100
End Time (seconds)	200
Discard Count	All
Packet Discard Modeling	Enabled

Filter
□ Exact match
□ Advanced
□ Apply to selected objects
OK
Cancel

Figure 7: Packet discarder configuration settings

The confusion matrix formulae for evaluating Intrusion Detection Systems (IDS) as follows (Abdulhamid *et al*, 2017);

The True Negative Rate (TNR) also called specificity is given by $\frac{TN}{TN+FP}$, True Positive Rate (TPR) also called Sensitivity or Detection Rate (DR) is calculated using $\frac{TP}{TP+FN}$ while, False Positive Rate (FPR) also known as False Alarm Rate (FAR) is given as $1-TNR$, False Negative Rate (FNR) is also given as $1-TPR$ and Accuracy is calculated using $\frac{TN+TP}{TN+TP+FN+FP}$. The values based on our system implementation are given in Table 4.3 in chapter 4.

4 DISCUSSION OF RESULTS

The implemented system comprises of 77 nodes out of which 4 of them are Sybil nodes. As discussed from the previous section, simulation was carried out for the three different scenarios. The raw result obtained is shown in Table 2. The parameters of interest are Total packet transmitted, PKT TX, Total Packet received, PKT TR and Total packet discarded, PKT DS. The derived data, RS PKT TX, RS PKT RX, RS PKT DS and NSP TX represent Real Sybil packets transmitted, Real Sybil packet received, Real Sybil packet discarded and Non-Sybil packet transmitted respectively.

TABLE 2: RAW RESULT DERIVED FROM SIMULATION

Time (s)	PKT TX	PKT RX	PKT DS	RS PKT TX	RS PKT RX	RS PKT DS	NSP TX
0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0
54	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0
74	0.7	0.45	0.09	0.036	0.023	0.013	0.664
76	1.3	0.75	0.19	0.068	0.039	0.029	1.232
78	1.51	1.5	0.3	0.078	0.078	0	1.432
80	2.2	1.6	0.41	0.114	0.083	0.031	2.086
82	2.5	1.87	0.52	0.129	0.097	0.032	2.371
84	3	2.17	0.628	0.156	0.112	0.044	2.844
86	3.6	2.25	0.73	0.186	0.117	0.069	3.414
88	4.1	2.4	0.835	0.213	0.124	0.089	3.887
90	4.5	3.1	0.889	0.234	0.16	0.074	4.266

The performance metrics was then further derived in Table 3, True Negative (TN), True Positive (TP), False Negative (FN) and False Positive (FP) metrics were derived and are given in Table 3.

TABLE 3: PERFORMANCE METRICS

Time (s)	TN	TP	FN	FP
0	0	0	0	0
18	0	0	0	0
36	0	0	0	0
54	0	0	0	0
72	0	0	0	0
74	0.054	0.036	-0.214	0.054
76	0.122	0.068	-0.482	0.122
78	0.222	0.078	0.068	0.222
80	0.296	0.114	-0.486	0.296
82	0.391	0.129	-0.501	0.391
84	0.472	0.156	-0.674	0.472
86	0.544	0.186	-1.164	0.544
88	0.622	0.213	-1.487	0.622
90	0.655	0.234	-1.166	0.655

The negative values validation is given by $FN = Total\ packet\ recieved - number\ of\ sybil\ packets\ sent$. These values are derived from table 2 and it is the total grand truth.

TABLE 4: PERFORMANCE EVALUATION METRICS

Time (s)	Accuracy (%)	TPR	TNR	FPR	FNR
0	0	0	0	0	0
18	0	0	0	0	0
36	0	0	0	0	0
54	0	0	0	0	0
72	0	0	0	0	0
74	25.13966	14.4	0.144	85.6	0.856
76	23.92947	12.36364	0.123636	87.63636	0.876364
78	50.84746	53.42466	0.534247	46.57534	0.465753
80	34.39597	19	0.19	81	0.81
82	36.8272	20.47619	0.204762	79.52381	0.795238
84	35.40023	18.79518	0.187952	81.20482	0.812048
86	29.94258	13.77778	0.137778	86.22222	0.862222
88	28.36277	12.52941	0.125294	87.47059	0.874706
90	32.80443	16.71429	0.167143	83.28571	0.832857

The detection rate (DR) of the implemented system is about 53.42%. It can also be shown that reasonable amount of packets got delivered which account for the high packet delivery ratio (PDR). This can be seen in figure 4.4 and implies that this technique although mitigate against the flow of Sybil packets and still guarantees the quality of service (QOS) of the network with respect to PDR.

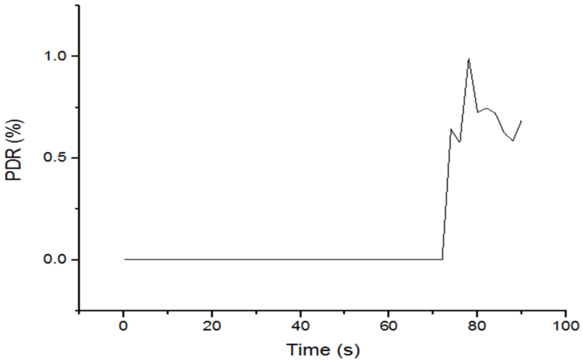


Figure 8: Graph of PDR against Time(s)

5 CONCLUSION

This paper has revealed to us how Sybil attack can be used to breach security on a campus network (CANET). Therefore, a Sybil mitigation technique was proposed which is based on two processes, to detect and to prevent the fake nodes. Both the threshold and physical address comparison is used for detection and prevention of these Sybil nodes. The proposed method was based on simulating inter-arrival time threshold and physical address comparison. The result gotten shows that the system guarantees quality of service (QoS) with respect to detection rate (DR).In the future, other simulator such as NETSIM can be used to carry out the implementation because of the features it possesses so as to know which is more efficient and this technique should be carried out on some social network so as to be able to identify profiles that are being cloned.

ACKNOWLEDGEMENTS

We would like to thank Ahmed Aliyu for his contribution, the Department of Cyber Security Science, FUT Minna and the anonymous reviewers for many helpful comments on this paper.

REFERENCES

Abdulhamid, S. M., Abd Latiff, M. S., Chiroma, H., Osho, O., Abdul-Salaam, G, Abubakar, A. I. and Herawan T. (2017), "A Review on Mobile SMS Spam Filtering Techniques", IEEE Access, DOI: 10.1109/ACCESS.2017.2666785.

Ali, M. N. B., Hossain, M. E., &Parvez, M. M. (2015). Design and Implementation of a Secure Campus Network. International Journal of Emerging Technology and Advanced Engineering, 5(7), 370-374. doi: http://www.ijetae.com/

Balachandran, N., &Sanyal, S. (2012). A review of techniques to mitigate sybil attacks. arXiv preprint arXiv:1207.2617.

Frey, D., Guerraoui, R., Kermarrec, A.-M., &Rault, A. (2015). Collaborative filtering under a sybil attack: analysis of a privacy threat. Paper presented at the Proceedings of the Eighth European Workshop on System Security.

Jangir, S. K., &Hemrajani, N. (2016). Evaluation of Black hole, Wormhole and Sybil Attacks in Mobile Ad-hoc Networks. Paper presented at the Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.

Levine, B. N., Shields, C., &Margolin, N. B. (2006). A survey of solutions to the sybil attack. University of Massachusetts Amherst, Amherst, MA, 7.

LUMS. (2016). Modeling Concepts. Retrieved October 09, 2016, from http://suraj.lums.edu.pk/~te/simandmod/Opnet/01%20Modeling%20Overview.pdf

Patra, P. (2014). A Survey of Sybil Attack Detection Techniques in WSN. (Master), Jadavpur University, India.

Saranya, V. (2014). Detection of Sybil attack on social networks using Sybil defender algorithm. International journal of control theory and applications.

Tran, N. (2012). Combating Sybil attacks in cooperative systems. (Doctor of Philosophy), Courant Institute of Mathematical Sciences New York University.

Trifunovic, S., &Hossmann-Picu, A. (2014). Stalk me if you can: the anatomy of sybil attacks in opportunistic networks. Paper presented at the Proceedings of the 9th ACM MobiCom workshop on Challenged networks.

Zanga, W., Zhangb, P., Wang, X., Shi, J., &Guo, L. (2013). Detecting Sybil Nodes in Anonymous Communication Systems Paper presented at the Information Technology and Quantitative Management Beijing, China.