American Journal of Modeling and Optimization, 2019, Vol. 7, No. 1, 1-7
Available online at http://pubs.sciepub.com/ajmo/7/1/1
Published by Science and Education Publishing
DOI:10.12691/ajmo-7-1-1

Performance and Analysis of Sybil Attack and Its Effect in MANET

Chaman Kumar[1,*], Anil Kumar[2,*]

[1]Department of Computer Science Engineering, Echelon Institute of Technology Faridabad, India
[2]Department Mathematics, Echelon Institute of Technology Faridabad, India
*Corresponding author: chamankumar31@gmail.com, dranilkumar73@rediffmail.com

Received November 11, 2018; Revised December 25, 2018; Accepted January 05, 2019

Abstract Detection of Sybil attack in mobile ad hoc network (MANET) has been a challenging issue in the context of network scalability, limited resource and complexity of the proposed methods. Literature review shows that most of the detection algorithms suffer from the above constraints and could not exhibit their proper efficiency and performance. This paper introduces the technique of formation of Sybil attack using simulation and study the impact of this attack on the major parameters on network. We also propose some unique detection technique on the basis of the analysis of this parameter.

Keywords: *Sybil attack, MANET, NS2, network, node, computer model*

Cite This Article: Chaman Kumar, and Anil Kumar, "Performance and Analysis of Sybil Attack and Its Effect in MANET." *American Journal of Modeling and Optimization*, vol. 7, no. 1 (2019): 1-7. doi: 10.12691/ajmo-7-1-1.

1. Introduction

The Sybil attack is one of the most severe attacks in MANET and WSN. When a malicious node illegitimately declares multiple identities or phony IDs, the network suffers from an attack called Sybil attack. The attack is named after the book Sybil by Flora Schreiber [1], in which there is a case study of a woman with multiple personality disorder that had 16 different "alters". In Sybil attack the malicious node replicates itself to make many copies to confuse and collapse the network. Sybil attack may happen in a system internally or externally. External attacks can be prevented by authentication mechanism but it cannot countermeasure internal attacks. For this there should be one to one mapping between identity and entity in the network which is the essential requirement for each node to prove itself not being compromised. But this attack violates this one-to-one mapping by generating multiple falsified identities of a malicious node. Sybil attack has spread excessive hazard to wireless sensor network as well as MANET in routing, voting system, fair resource allocation, data aggregation and misbehavior detection system. Large-scale peer-to-peer systems also face security threats from faulty or antagonistic remote systems. To defend against these threats, many such systems use redundancy.

Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities which can replicate computational or storage tasks (to preserve integrity of data) or fragment tasks among them (to protect against data leakage). This type of system must ensure that each entity has distinct identity otherwise, when an entity selects a subset of identities to redundantly perform a remote operation, it can be tricked into selecting actually a single remote entity multiple times, thereby defeating the redundancy [2]. The security threat of the Sybil attack vary from out-voting honest users in online settings [3], to the corruption of routing tables in peer-to-peer systems [4]. In the Sybil attack, the adversary joins the targeted system using his Sybil identities and then mounts many follow-up attacks in order to disrupt the targeted system. For example, a rival can pollute the voting scheme of a reputation system [3], undermine the routing and data replication services in DHTs [4], or cripple many critical functions of a wireless sensor network such as routing, resource allocation, and misbehavior detection [5]. A reputation system's vulnerability to a Sybil attack depends on how slackly identities can be generated. If the reputation system accepts inputs from entities that are not trustworthy then linking them to a trusted entity cause threat for the system. Due to presence of duplicate identities the outcome of voting process may vary. Moreover Sybil attacks prevent fair resource allocation among the nodes in network. This threat is particularly keen in decentralized systems, where it may be unreasonable or impossible to rely on a single authority to certify genuine nodes [6]. Though one important result shown in [7] is that without a logically centralized authority, Sybil attacks are always possible (i.e. may remain undetected) except under extreme and unrealistic assumption of resource parity and coordination among entities. Since the Sybil attacker can create many fake identities, it thus can increase the probability that the malevolent node is selected by other nodes as part of their routing paths. Besides, the Sybil attack can significantly reduce the effectiveness of fault-tolerance schemes such as multi-path routing [8,9]

because other nodes will treat the forged nodes generated by the spiteful node as different nodes and establish different routes through the malicious node. A Sybil attacker cans also satire nodes using a geographic routing protocol, such as the GRID routing protocol [10]. A Sybil attacker destabilizes the network by creating a large number of pseudonymous entities to gain a suspiciously large authority. In the presence of Sybil nodes in network, it becomes difficult to identify a misbehaving node.

2. Sybil Attack

To introduce unique detection mechanism for Sybil attacks in MANET it is important to gather an overall idea about Sybil attack and its characteristics. In this section we are going to discuss about Sybil attack taxonomy, its impact and different detection techniques revealed till date in order to mitigate it.

Since MANET is a distributed system data can be sent via one of the multiple nodes which are available. In this case the identity of the source and destination plays an important role in order to maintain data integrity. The network should have the ability to determine whether two apparently different entities are actually different. In MANET nodes do not have any physical knowledge about other nodes. The only way to recognize each other is by some informational abstraction (through request/ response message). This type of system must ensure that distinct identities refer to distinct entities; otherwise, when an entity (or node) sends data to multiple identities (or node) it can be deceived into selecting a single entity multiple times. This falsification of multiple identities is termed as Sybil attack. Thus Sybil attack can be defined as an attack by a malicious device taking multiple identities (called Sybil nodes) illegally misleading legitimate nodes in a MANET.

The Sybil attack can occur in a MANET since it operates without a central authority which can verify the identities of each communicating entity. Because each entity is only aware of others through messages over a communication channel, a Sybil attacker may take different identities during transmission of message to the legitimate node. To defend against Sybil attack it is required to have the knowledge of its different forms.

Sybil attack [7] is a serious threat for today's wireless ad hoc networks. In this attack a single node impersonates several other nodes using various malicious means. A mobile ad hoc network is a collection of wireless mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. This particular nature of the network makes it vulnerable to various, Sybil attack being one of them. With no logically central, trusted authority to vouch for a one-to-one correspondence between entity and identity, it is always possible for an unfamiliar entity to present more than one identity, except under conditions that are not practically realizable for large-scale distributed systems. Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities to mitigate the threat of hostile peers. Many systems replicate computational or storage tasks among several remote sites to protect against integrity violations (e.g. data loss). Others fragment tasks among several remote sites to protect against privacy violations (data leakage).In either case, exploiting the redundancy in the system requires the ability to determine whether two ostensibly different remote entities are actually different. Firstly all the messages in the network are of broadcast nature; secondly the network has no fixed infrastructure. If a good number of nodes are compromised then the network may totally collapse.

Sybil attack is defined as an attack by a malicious device adopting multiple identities illegitimately and the additional identities to the Sybil node are known as Sybil nodes. There are many ways in which the Sybil attack can be launched. These are direct and indirect attack, simultaneous and non-simultaneous attack, stolen and fabricated identity attack.

In direct communication a genuine node sends a radio message directly to a Sybil node from which the message reaches to the malicious device without the concern of the sender. Symmetrically, when any of the Sybil nodes sends a message, the messages are actually sent from the malicious node device. In indirect communication the legitimate node does not communicate directly with the Sybil node. Instead there are one or more malicious nodes in between through which the message has to be passed. When the message reaches to the malicious device it pretends to pass it to the Sybil node but actually consumes it.

In fabrication the attacker creates arbitrarily new identities with distinguishable identification. This identification should be compatible with the identification of the existing legitimate nodes of the network. Fabrication can be defended by introducing some mechanisms like authentication to identify legitimate nodes identity. Sybil attacker may steal the identity of a legitimate node and assign it to a Sybil node. The attacker may temporarily make the Sybil node inactive so that it remains undetected.

Attacker may use all the Sybil identities at a time i.e. simultaneously in the network. Though it is not possible for a single physical device to represent more than one identity at a time it can cycle through all the identities so rapidly that it appears to be presented simultaneously. In non-simultaneous situation an attacker represents large number of identities over a period of time. This can be done in two ways. Either the attacker can represent each identity one after another for a period of time or it can use same number of physical devices as the number of identities to represent them individually by each single physical device.

3. Attack Model

A Sybil node can vary its transmission power during transmissions to create a number of virtual illegitimate nodes. We define a category of Sybil attack in which a malicious node periodically varies its identity with different transmission power. The attacker compromises some legitimate nodes and represents itself through them during communication. The compromise nodes deliver wrong routing information to the source node through send reply routing packet that it has the shortest routing path towards destination through the attacker. Whenever

traffic passes through the attacker it completely drops all the data packets. During the attack the attacker exhibits a higher transmission power than that of the legitimate nodes in order to act as a new legitimate neighbor in the network. Thus during attack the transmission power of the Sybil nodes becomes higher than the other nodes. In our assumption the source and the destination node is moving. The destination node comes towards the source and goes away from the source node in order to create relative motion between all the nodes. We have studied the effect of this attack on the network performance and represented them graphically. The attacker with four neighbors, one source node and one destination is considered as an attack model for our experiment and the topology is represented in the NAM file (Figure 1) when implemented in NS2.35 platform.

In AODV protocol the source node broadcasts request messages to its neighbors for finding paths to the destination. A Sybil attacker compromises one or more legitimate nodes that provide wrong routing information to the source in order to attract data traffic towards itself. While data packet is passed through the Sybil node, it consumes the data packet. Thus by representing same identity at multiple locations simultaneously the attacker creates a scenario which forces to stop the simulation before actual time of end simulation. The dropping packets by the attacker reduce the throughput considerably during communication. The four neighboring nodes are used for measuring the RSP values obtain from the Sybil node during communication.

According to the attack model (Figure 1) nodes 6 is the source and node 5 is the sink (destination). Node 0 is made Sybil which compromises node 1. Node 0 changes its transmission power periodically between 1.8 watt and 2watt after specific time interval of 5s. The sink node moves with a speed of 15m/s towards the source. This assumption makes other nodes in the network relatively mobile with respect to the source and sink. We conduct the simulation over the time period 150s .The maximum transmission occurs in the time period 100s to 125s when source node and the destination nodes are within the transmission range. The attack gets executed during the time period 100s to 150s. We demonstrate the typical simulation parameter values in Table 1 and the scenario of the network performances before and after attack in the Figure 2 to Figure 8 given below.

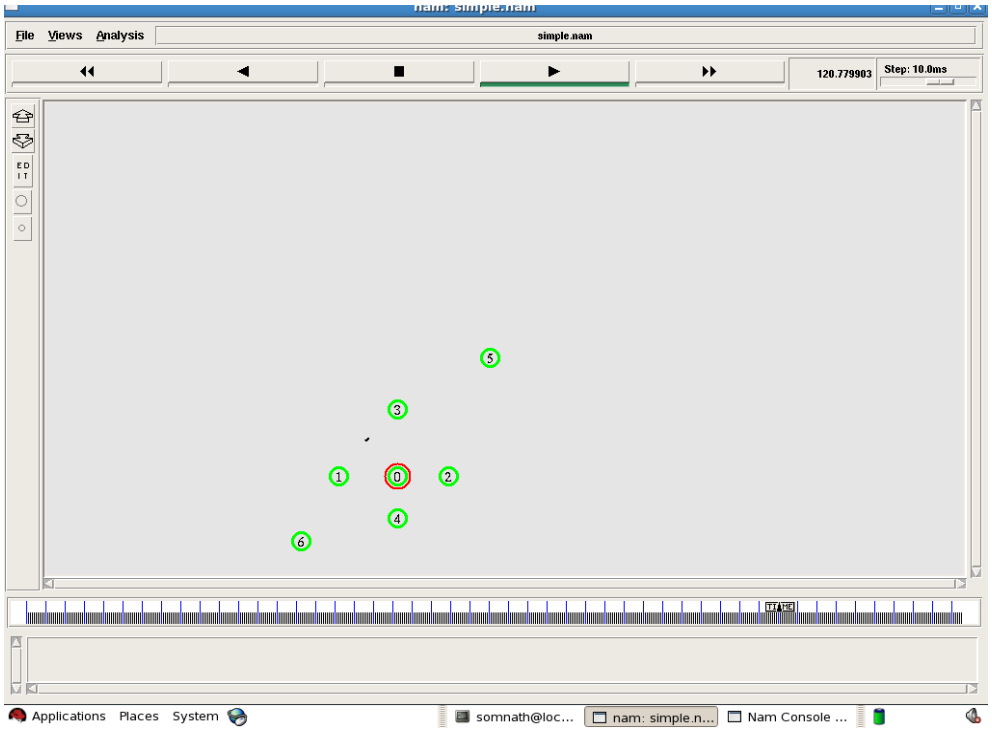

Figure 1. Topology of Attack Model

Table 1. NS-2.35 typical simulation parameter values using AODV routing protocol

Parameter	Value
Transmission power (watt)	1.8/2
Frequency (Hz)	2.472×10^{9}
Initial energy (Jules)	100
Collision threshold (dB)	100
Carrier sense threshold (watt)	5.011872×10^{-12}
Receive power threshold (watt)	5.82587×10^{-09}
Idle Power (watt)	712×10^{-6}
RxPower (watt)	35.28×10^{-3}
TxPower (watt)	31.23×10^{-3}
Sleep Power (watt)	144×10^{-9}
Simulation time (sec.)	150
Speed of the sink node (m/sec)	15

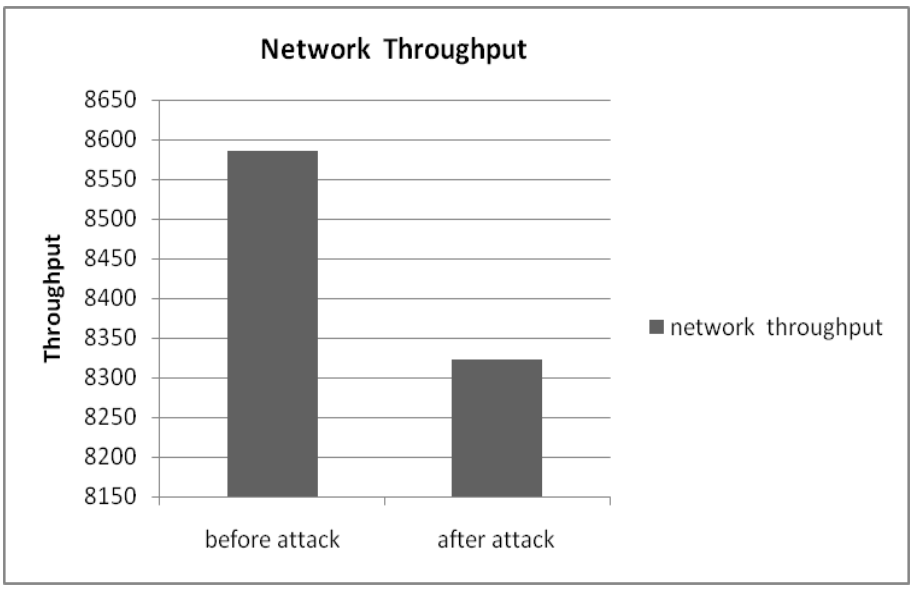

Figure 2. Effect of Sybil Attack on Network Throughput

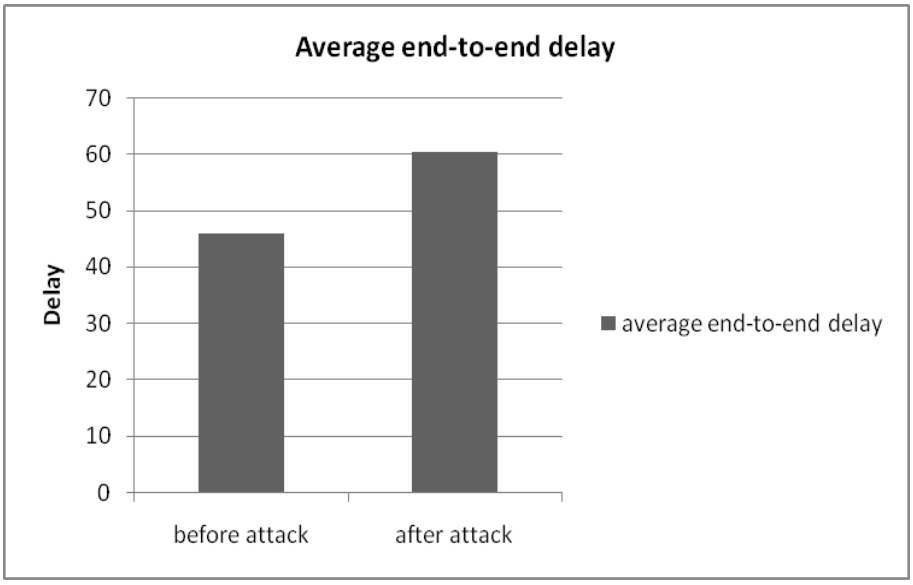

Figure 3. Impact of Sybil Attack on Average Delay

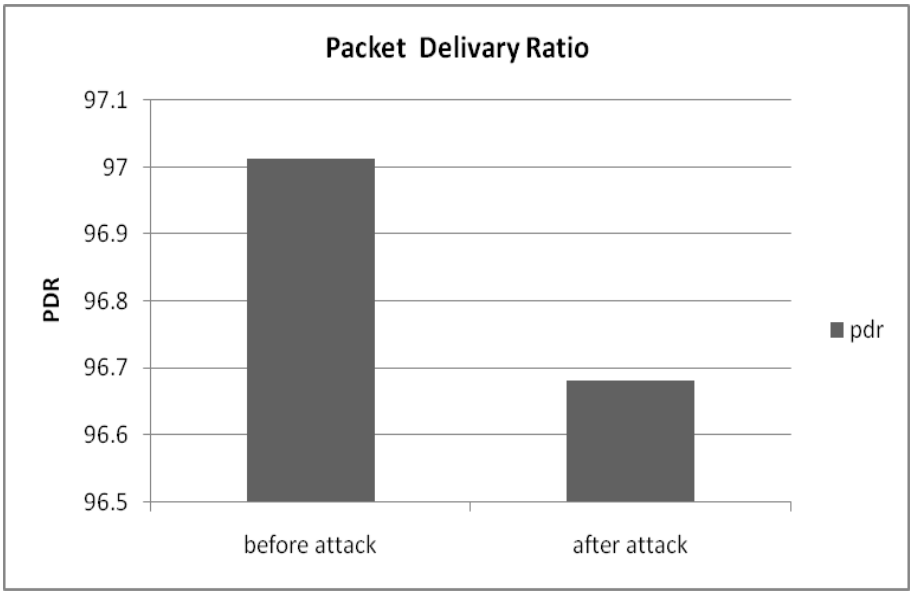

Figure 4. Variation of Packet Delivery Ratio due to Attack

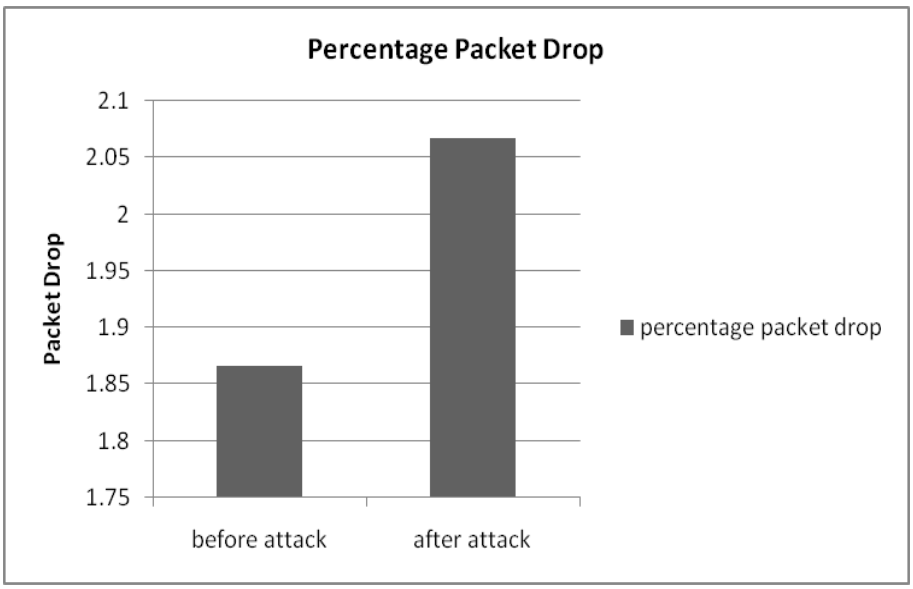

Figure 5. Effect of Sybil Attack on Percentage Packet Drop

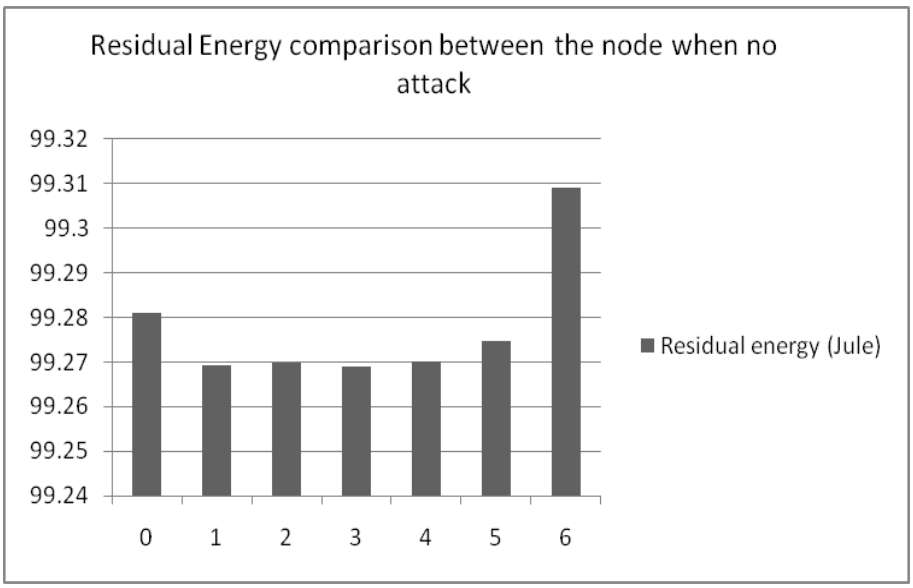

Figure 6. Residual energy comparison

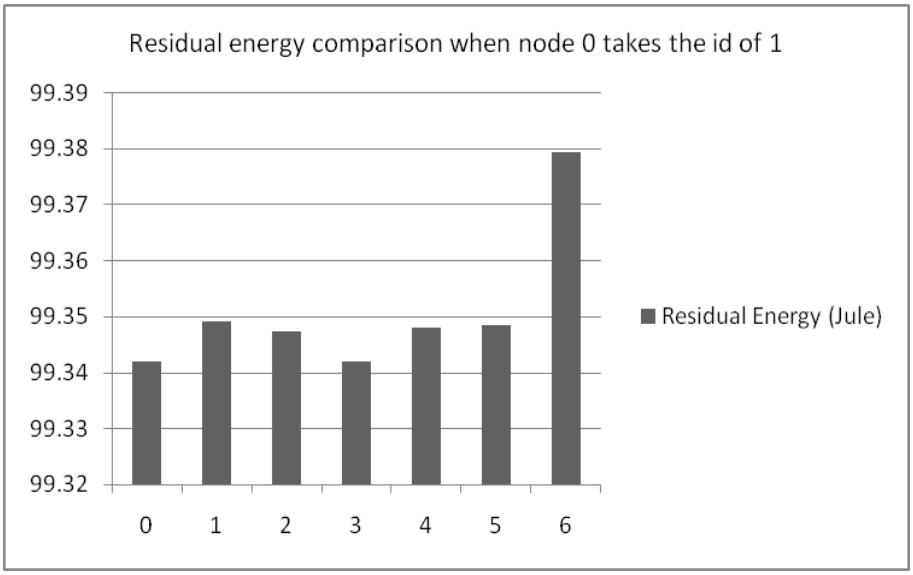

Figure 7. Residual energy comparison

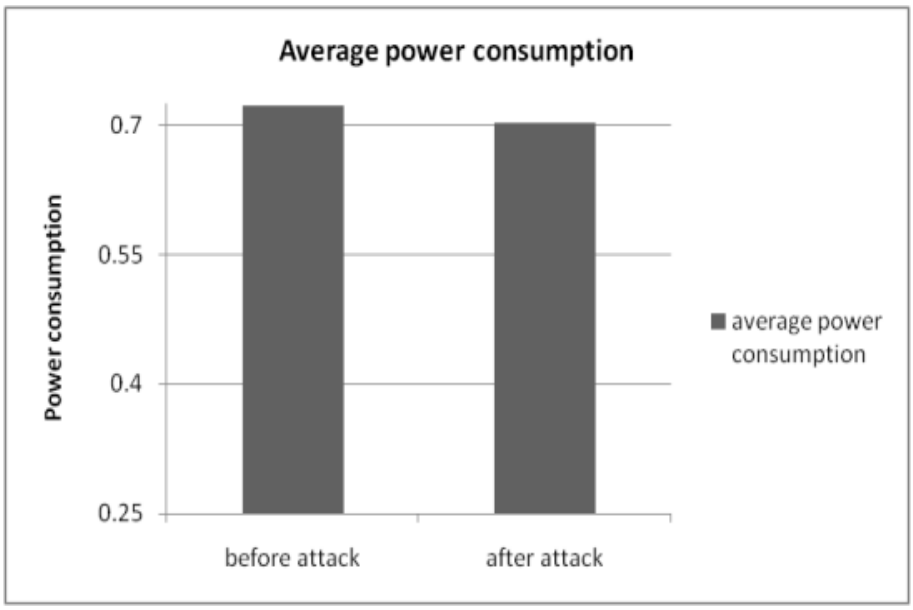

Figure 8. Variation of Average Power Consumption Due to Attack

4. Analysis and Discussion

Figure 2 to Figure 8 shows the impact of Sybil attack on network performance. We see that network throughput and PDR decrease after attack. This is due to the fact that Sybil node consumes more number of packets instead of forwarding them to the proper destination. Another reason is same node having multiple location create network jamming condition .This fact is more prominent in Figure 5 which shows a considerable amount of packet drop after attack. Average delay increases (Figure 3) due to increase in propagation delay.

Another important variation is average power consumption. From Figure 8 we observe that average power consumption is lower after attack. This is due to the fact that Sybil nodes disrupt the whole network by providing wrong routing information and dropping data packets. Hence communication gets stopped earlier than the expected time. This causes more residual energy of the nodes in the network. Whereas, one node with multiple IDs and varying transmission power causes the attacker and compromise node to consume more power than without attacking condition. However, most interesting result comes through the graphs of Figure 6 and Figure 7, where we compare the residual energy of the nodes. It is interesting to be noted that the residual energy of the attacker is lowest as it uses the multiple ids and uses its maximum power to communicate with the other node on behalf of multiple nodes.

5. Conclusion and Future Work

This paper has aimed to rendering the Sybil attack in ad-hoc network. It approaches towards exploring the area of ad hoc network where this attack can occur. We have discussed its severity in those fields such as p2p system, MANET, WSN, reputation system and so on. Along with a brief taxonomy of the Sybil attack we have sketched a clear and distinct classification of the countermeasure of this attack. This categorization is done on the basis of Sybil attack prevention, detection and recovery methods and is useful to select the proper domain for future research on Sybil attack defence. Moreover, this arrangement will help the readers and researches to get an idea of Sybil attack detection on the basis of residual energy. However the residual energy of the attacker and the compromise node depends on the dimension of the attack. In future we will incorporate our idea of detecting the Sybil attack in MANET.

References

[1] F. Schreiber, S. Mart´ınez, and L. Vigil. Sybil. 1981.

[2] John R. Douceur, The Sybil Attack, Microsoft Researchjohndo@microsoft.com.

[3] A. Jøsang and J. Golbeck. ”Challenges for robust of trust and reputation systems”, Sept. 2009.

[4] G. Urdaneta, G. Pierre, and M. van Steen. “A survey of DHT security techniques”. ACM Computing Surveys,43(2), Jan. 2011. http://www.globule.org/publi/ SDST_acmcs2009.html.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig. “The sybil attack in sensor networks: analysis defenses.” In Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on, pages 259-268, april 2004.

[6] N. Margolin and B.N. Levine.Quantifying and discouraging sybilattacks. Technical report, UMass Amherst, 2005.

[7] J. R. Douceur. The sybil attack. In IPTPS ’01: Revised Papers from the First InternationalWorkshop on Peer-to-Peer Systems, pages 251-260, London, UK, 2002. Springer- Verlag.

[8] J. Chen, P. Druschel, and D. Subramanian, “An efficient multipath forwarding method,” *Proc. IEEE INFOCOM*, pp. 1418-1425, 1998.

[9] K. Ishida, Y. Kakuda, and T. Kikuno, “A routing protocol for finding two node-disjoint paths in computer networks,” *Proc. IEEE Int’l Conf.Network Protocols*, pp. 340-347, 1995.

[10] W. H. Liao, Y. C. Tseng, and J.P. Sheu, “GRID: A fully location-aware routing protocol for mobile ad hoc networks,” *Telecomm. Systems*, vol. 18, no. 1, pp. 37-60, 2001.

[11] G. Wurster, P. v. Oorschot, A. Somayaji, "A generic attack on checksumming-based software tamper resistance", IEEE Symposium on Security and Privacy, 2005.

[12] Trifaa Z., Khemakhemb M., “Sybil Nodes as a Mitigation Strategy against Sybil Attack”, International Workshop on Secure Peer-to-Peer Intelligent Networks & Systems (SPINS-2014), Procedia Computer Science 32 (2014)pp 1135 – 1140, June 2014.

[13] Alvisi L., Clement A., Epasto A., Lattanzi S., Panconesi A.,SoK: "The Evolution of Sybil Defense via Social Networks, Security and Privacy (SP)", 2013 IEEE Symposium on Security and Privacy (SP), pp 382-396, 19-22 May 2013.

[14] Demirbas M., Song Y., "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", in Proceedings of WoWMoM 2006, pp. 570.