Grenze International Journal of Engineering and Technology, January 2016

Modeling Different Forms of Sybil Attack in MANET

[1]Aditi Paul and [2]Somnath Sinha
[1] Faculty of Computer Science, Dronacharya College of Engineering, Greater Noida
Email:aditi23.mca@gmail.com
[2]Faculty of Computer Science, Pacific Academy of Higher Education & Research University, Udaipur, India
Email: ssin.mca@gmail.com

***Abstract*—In Mobile Ad-hoc Network (MANET) Sybil attack can be launched in different dimensions. The current study proposes formation of Sybil attack using simulation in three different aspects. These models are designed to show various forms of Sybil attack in different application domains of MANETs and give a transparent view of each category. Comparisons of the post-attack effects are shown graphically according to the simulation results after executing each model. These comparisons are made on different network parameters such as throughput, packet delivery ratio, percentage packet drop and average end-to-end delay. Although these models may not strictly follow the basic taxonomy of Sybil attack but they are relevant with the behaviour of Sybil nodes in different domain.**

***Index Terms*— Sybil attack, Mobile Ad hoc Network, NS2, Sybil attack formation.**

I. INTRODUCTION

The Sybil attack is very severe in MANET due to the absence of any central authority. The central authority is useful to verify the identities of the nodes [1]. In MANET data can be sent from source to destination via multiple hops which are available. Thus the authenticity of the source and destination plays an important role to preserve data integrity. The MANET should be capable of determining the correspondence between an entity and its identity. The mobile nodes in MANET recognize each other by some exchanging message i.e. through message passing (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 nodes) it can be deceived into selecting a single entity multiple times. This falsification of multiple identities is termed as Sybil attack. Thus in Sybil attack a malicious device takes multiple identities (called Sybil nodes) illegally and mislead legitimate nodes. This attack be categorized into three dimensions which are direct or indirect, stolen or fabrication and simultaneous or non-simultaneous. Theoretical definition of theses classification is not sufficient to get a clear idea of this attack in real system or application domain of MANET. Literature shows various form of Sybil attack in varieties of application domain of MANET. However, it is hard to model all these forms in a standard way; in the proposed study we show three different models of Sybil attack using NS2. The paper is organized as follows: section 2 describes taxonomy of Sybil attack, section 3 gives literature review of Sybil attacks in different domains which do not follow the taxonomy strictly, section 4 shows the attack models and three categories of Sybil attack, section 5 shows the comparative analysis of the effect of these attacks and section 6 represents a qualitative comparisons of the three models.

Grenze ID: 01.GIJET.2.1.513

II. SYBIL ATTACK

A. Sybil Attack Taxonomy

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. The fundamental taxonomy [6] of Sybil attack can be proposed based on three dimensions: Direct vs. Indirect attack, Fabricated vs. Stolen identities and Simultaneous vs. Non-simultaneous attack. A brief description of these three dimensions is cited below.

Dimension I: Direct vs. Indirect attack. In direct communication the attacker directly communicates with the true nodes and attracts traffic towards it. In indirect communication the attacker does not communicate directly with the genuine node. Instead it communicates through one or more Sybil nodes. As soon as the data packets arrive at the Sybil node it passes it to the attacker.

Dimension II: Fabricated vs. Stolen Identities. In fabrication the attacker creates arbitrarily new identities with distinguishable identification and executes the attack. The attacker may also steal the identity of a legitimate node. This can be achieved either by negotiating with the existing node or by stealing the identities of the legitimate nodes without their knowledge.

Dimension III: Simultaneous vs. non- simultaneous.

In simultaneous attack all the Sybil identities of the attacker are launched at a time (i.e. simultaneously) in the network. Though it is hard for a single physical device to activate more than one identity at a time, it cycles through all the identities so rapidly that it appears to be presented simultaneously. In non-simultaneous attack the attacker uses huge number of Sybil identities for a certain time interval. 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 equal number of physical devices as the number of identities and represents them one by one with each single physical device.

The theoretical explanation of taxonomy of Sybil attack only gives an overall idea of the attack. However, in reality the prospect of the attack differs in dimension and vastness. The notion of the proposed study is to model some form of Sybil attack which do not follow the taxonomy always but launch the attack in some different ways. Here, we have implemented three models of Sybil attack in NS2 platform and demonstrate the attack scenario graphically.

III. LITERATURE SURVEY

In the literature of Sybil attack and its detection and mitigation technique different forms of Sybil attack have been discussed. In [5] a different form of Sybil attack in MDHT (mainline DHT) has been focused. The authors in this [5] study considered two kinds of attacks on a DHT; the *horizontal* attack in which the Sybils spread widely across the system. The aim is to pollute as many routing tables as possible. The *Vertical* attack attempts to insert as many Sybils as possible in one specific routing table. However none of the attack strictly follows the taxonomy of the attack. In [2, 4] the Sybil attack was described in social network. In [4] the authors assumed that Sybils would find it difficult to become friend (compromise) with real users and hence they use to connect to each other to make a group. According to this paper there is a difference in the goals of Sybils and real users in case of online services. While the real users share several features of the social networking sites, Sybils focus on specific actions such as acquiring friends and disseminating spam in order to maximize resource utilization per time spent. In [3] it is shown that when the Sybil attacker creates new identity, the signal strength of that identity will be high enough to be distinguished from the newly joined neighbor. This paper showed that the fabricated identities of the Sybil nodes differentiate themselves by their transmission power which is again a new form of attack. Another aspect of Sybil node described in this paper is the signal strength based behaviour of the Sybil nodes. Here it is shown experimentally that new legitimate nodes become neighbors as soon as they enter inside the radio range of other nodes; hence their *first* RSS at the receiver node is low enough. In contrast a Sybil attacker, which is already a neighbor, will cause its new identity to appear abruptly in the neighborhood. In all these literature of Sybil attack it is evident that Sybil attacks create new dimension in different field and do not follow the basic taxonomy in most of the cases. The goal of the current study is to demonstrate such behavioral aspects of Sybil nodes (through simulation) which are different from the fundamental types of Sybil attack.

IV. ATTACK MODEL

Category I: In category-I we design a MANET (figure 1) of 7 nodes among which 0 is made attacker which compromises node 1. Node 1 sends wrong routing information of having shortest path towards destination to

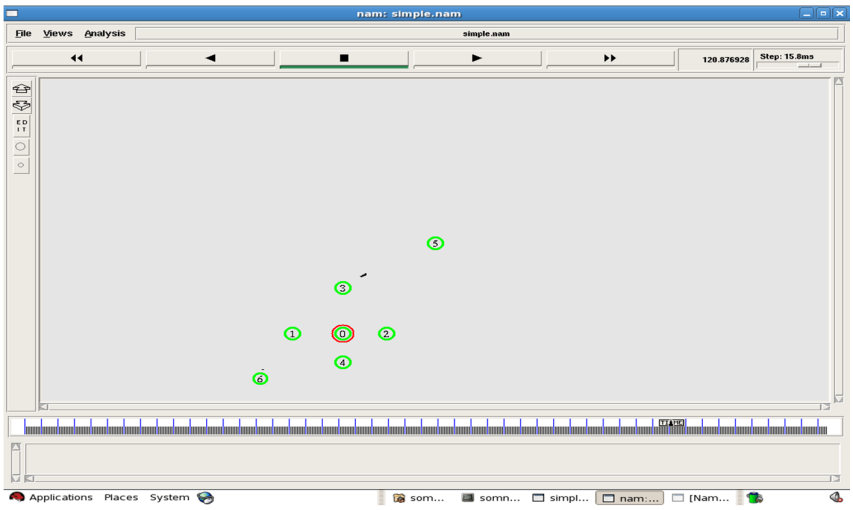

Figure1. Topology of attack model

node 6. Thus node 6 sends data packet to node 1 who forwards incoming packets to node 0. Node 0 consumes the packets when they reach to it. This causes a disruption in the network and hence network performance degrades drastically. Source node 6 broadcasts route request (RREQ) to find a route to destination node 5. Since our algorithm works for MANET we consider that node 6(source) and node 5(sink) are mobile. This assumption makes other nodes in the network relatively mobile with respect to the source and sink. Total simulation time is 150s. Attack starts after 30 sec. Node 1 sends wrong routing information to node 6 by representing it as node 0 over the time interval of 20 sec. and increases its sequence number higher than the most recent value. Thus node 6 sends data packet to node 1 who forwards incoming packets to node 0. Node 0 consumes these packets when they reach to it. In the next interval of 20 sec. the nodes become legitimates.

Category II: Category-II is complementary model of category-I. Here node 0 periodically takes of the identities of node 1 and sends wrong routing information to the source node. When node 0 behaves as node 0 there is no attack and the traffic goes to node 1, the true node. However, when node 0 takes of the identity of node 1 the source node gets two RRP from same node (node 1): one from attacker node 0 and another from node 1 itself. This phenomenon attracts data traffic towards node 1. When data packets reach to node 1 it forwards it to the destination or next hop but when the data traffic reaches to node 0 (behaving as node 1) it consumes these packets instead of forwarding them towards destination or next hop. This phenomenon does not increase packet drop or decrease packet delivery ratio (figure2 to 4) but reduces network throughput.

Category III: The third category is based on the concept of flooding where the attacker (node 0) floods huge request packets with the identity of the other node (node -1). The continuous flooding of RRQ packets exhausts the resources of all communicating nodes and disrupts the routing operation as well.

Table I shows the simulation parameters for the attack model (figure 1). The simulation is run with 7 nodes in an area of 500x500 sq meters among which node 0 are made Sybil attacker. The simulation parameters are shown in table 1. Total simulation time is 150s. Attack starts after 30 sec and at every 20 sec. interval the attacker changes its identity. The attacker misguides the source node by sending wrong routing information or creates congestion in the network over the time interval of 20 sec. In the next interval of 20 sec. the nodes become legitimates. We consider two-ray ground propagation model for communication between the nodes. The speed of the sink node is given 15m/s and that of source is 1m/s. Initial energy of all the nodes is set as 100 joules and transmission power 1.8 w. The authors used AODV protocol to implement all the models and done necessary changes in the coding according to the requirements.

V. Simulation Result

In this section we show the outcome of the three categories of attacks discussed in the previous section. We consider four network parameters which are total throughput, average end-to-end delay, packet delivery ratio

TABLE I. SIMULATION PARAMETERS OF ATTACK MODEL

Parameter	Level
Propagation Model	Two-Ray Ground
Transmission power	1.8w
Frequency	2.472 x 10^{9} Hz
Initial energy	100 J
Collision threshold	100 dB
Carrier sense threshold	5.011872 X 10^{-12} w
Receive power threshold	5.82587 X 10^{-09} w
Idle Power	712 X 10^{-6} w
Rx Power	35.28 X 10^{-3} w
Tx Power	31.23 X 10^{-3} w
Sleep Power	144 X 10^{-9} w
Number of Nodes	44
Protocol	AODV
MAC	802_11
Maximum packet in ifq	50
Topology	Flat Grid
Area covered	(500x500) sq.m.
Node movement (sink)	at 50 towards position 25, 20 at 100 towards position 490,480
Node movement (source)	at 10.0 towards position 20, 18
Simulation time	150s
Speed of the sink node	15m/s
Speed of the source node	1m/s
Starting time of attacker	30.0s
Attacker vary id in each	20.0s

and percentage packet drop and show their variation due to attack in each category. These results evaluate each model (section 3) of Sybil attack and their effect on the network.

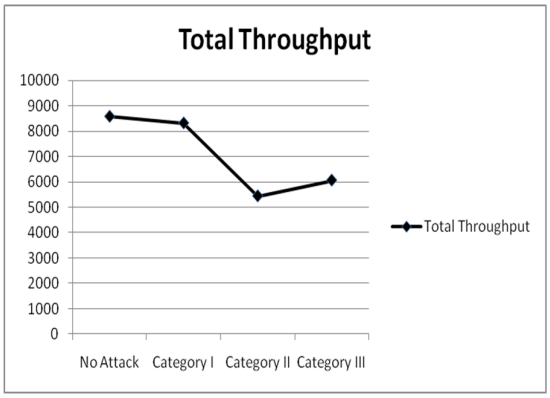

Figure 2. Comparison of network throughput

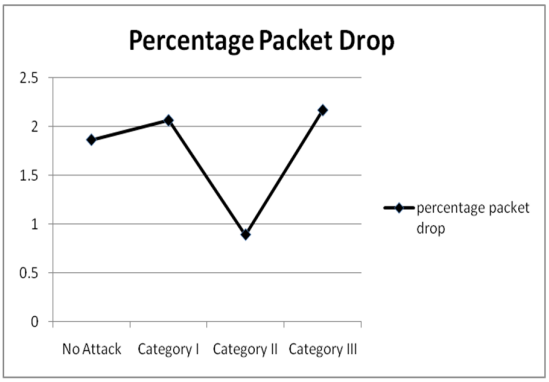

Figure 4.Comparison of Percentage Packet Drop

In Figure 2 we see that Network throughput has decreased drastically during attack which is obvious if the attacker successfully execute the attack. Percentage packet drop and packet delivery ratio are inversely proportional to each other. One important observation here is that category I and category II show complementary effect (figure 3 to 4) on these two parameters. For category I packet delivery ratio is minimum and packet drop is maximum whereas for category II these results are complementary.

During attack the attacker sends wrong routing information which creates confusion to the communicating nodes and packet drops increase. This leads to high end-to-end delay. In figure 4 we see that packet drop is high for category-II and hence end –to-end delay is also high. The comparative analysis of these three categories of Sybil attack is shown in Table I.

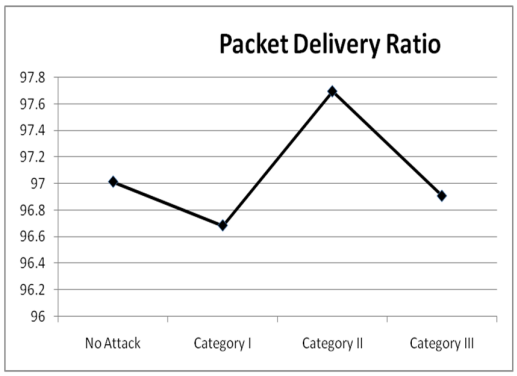

Figure 3. Comparison of Packet Delivery Ratio

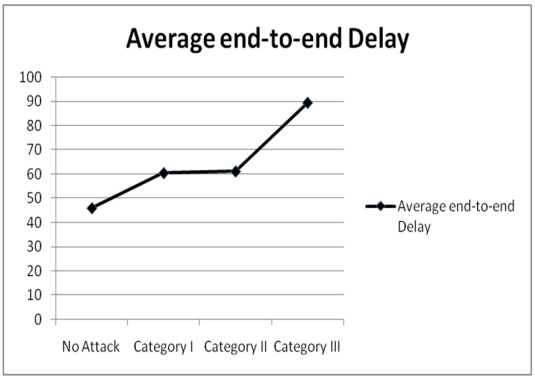

Figure 5. Comparison of Average End-to End Delay

VI. Analysis and Discussion

In this study we model some forms of Sybil attack in MANET. One important aspect of the current study is that it evaluates the notion of attacker in a network. This fact is vital for attack detection various domains. The simulation result for the three categories give a contrasting view of the intention of the attackers. In category I we see that packet drop is very low and packet delivery ratio is highest (higher than no-attack condition) which shows a normal network condition. However, the network throughput decreases by a considerable amount. This indicates an abnormality in the network. On the other hand category III damages the network enormously which we see from figure 4 and figure 5.

Table II. Performance Analysis Of Proposed Sybil Attack Detection Models

Category of Attack	Taxonomy	Total Throughput	Packet Delivery Ratio	Percentage Packet Drop	Average end- to-end Delay	Intensity
Category I	Indirect communication	Low	Lowest	Almost same as category III	Lower	Easy to identify
Category II	Stolen identities	Lowest	highest	lowest	Lower (almost same as category I)	Most severe
Category III	Simultaneous attack	Lower than category I	Higher than category I	Highest	Highest	High intensity

VII. Conclusion

The current study shows the different perspectives of Sybil attack in MANET. The proposed models of Sybil attack and their analysis bring forth a new aspect of the attack for the researcher. Table II gives a brief comparison of the attack scenarios among the three attack models. In future we will incorporate more advanced form of Sybil attack and their effect on network performances.

References

[1] J.R.Douceur, "The Sybil attack", in Proceedings for the First International Workshop on Peer-to-Peer systems (IPTPS'02), ser. LNCS, vol. 2429. Cambridge, MA, USA: Springer, Mar 2002, pp. 251–260.

[2] A.Mohaisen, N.Hopper and Kim.Yongdae, " Keep your friends close: Incorporating trust into social network-based Sybil defenses", Univ. of Minnesota, Minneapolis, MN, USA, INFOCOM 2011, Proceedings IEEE, 10-15 April 2011, pp 1943 – 1951.

[3] S.Abbas, M. Merabti and D.Llewellyn-Jones, "Lightweight Sybil Attack Detection in MANETs", IEEE systems journal, vol. 7, no. 2, June 2013 , pp 236-248.

[4] Gang Wang, Tristan Konolige, Christo Wilson, Xiao Wang, Haitao Zheng and Ben Y. Zhao, "You are How You Click: Clickstream Analysis for Sybil Detection", 22nd USENIX Security Symposium, August, 2013, pp. 241-255.

[5] Liang Wang, Jussi Kangasharju, "Real-World Sybil Attacks BitTorrent Mainline DHT", Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 826-832.

[6] S.Sinha, A.Paul, S.Pal, "The Sybil Attack in Mobile Adhoc Network: Analysis and Detection", proc "International Conference on Recent Trends in Communication and Computer Networks - ComNet 2013", Nov 2013, pp. 95-103.