Analysis of Non Simultaneous Sybil Attack on DSR

Tripti Sharma
M.Tech
Krishna Engineering College, Uttar Pradesh
Technical University, Lucknow

Leenu Singh
Assistant Professor
Krishna Engineering College, Uttar Pradesh
Technical University, Lucknow

ABSTRACT

Security is one of the most challenging issues in Mobile ad-hoc networks (MANETs). Most of the routing protocols in MANETs do not have an inbuilt mechanism to fight security attacks. Sybil attack is one such attack in which a single physical device takes on multiple identities in network thus behaving as multiple independent devices. With the help of these forged identities, the attacker can draw more benefits from the network by asking for more resources with the help of the multiple fake identities. The paper analyses the impact of Non-Simultaneous Sybil Attack on Dynamic Source Routing protocol (DSR). Its effect has been studied on performance metrics - End to End Delay and Throughput.

Keywords

Mobile Ad-hoc Networks, Sybil Attack, DSR, Network Security.

1. INTRODUCTION

In a network where there is no criteria to judge the authenticity of a node, any device can enter and exit the network on its own wish. MANETs in their basic form, do not pose restriction on any mobile device to prevent it from joining the network. They do not have a central authority which can regulate its functioning. In such unrestricted environments, an intruder or an attacker node can easily join the network. Depending on the nature of the attack, the attacker can harm the network in various manners. Douceur, for the first time formally presented an excellent discussion on an Identity based attack [1]. When a single physical device takes on multiple forged identities in a network, it is called a Sybil attack. The attacking node can behave as more than one physical device, thus fooling the other nodes. Since there is no central authority to ensure that one physical entity is bound with only one identifier, an attacker can take as many identities as it wants. An attacker can forge identities in two ways [2]. The First, in which the attacker uses only one forged identity at a time for communication with the rest of the network. This fake identity is discarded periodically and another one is taken. The process is repeated continuously and therefore at a particular time, only one fake identity of the attacker is up in the network. This is called non- simultaneous Sybil attack. In the second type of Sybil attack, the attacker communicates with the network using all its fake identities simultaneously behaving as multiple devices. It sends packets through these fake identities simultaneously by cycling through them frequently. Such an attack is called Simultaneous Sybil Attack.

The paper analyses the impact of Non-Simultaneous Sybil attack on Dynamic Source Routing (DSR) protocol [3]. In the process of switching the identities, the attacker may break the communication path and hence, it degrades the network performance. The rest of the paper is organized as follows. Section 2 highlights the related work. In section 3, the implementation details of the Sybil attack on DSR protocol have been described. Section 4 gives an overview of the simulation environment. Analyses and Results have been discussed in section 5. Finally, section 6 concludes the paper.

2. RELATED WORK

Researchers have mainly worked on detection of Sybil attack. Very little work has been done on analyzing the impact of Sybil attack on routing protocols in MANETs. Mohaisen et al. have discussed the behavior of the Sybil attacker in detail [4]. The defense mechanisms for Sybil attack have also been reviewed in their work. Newsome et al. have discussed the various forms of Sybil attack and its multiple effects on the network, particularly in context of sensor networks [2]. It is summarized as follows. The impact of the Sybil attack depends on whether the attack is simultaneous or non-simultaneous. In simultaneous form, an attacker can affect the voting system among the nodes. The result of voting can be drawn in favor of the Sybil attacker as it can participate in the voting using its multiple identities and hence, it can vote more than once. An attacker of this kind can draw more resources with the help of multiple identities. The attack can also affect the multipath routing protocol where disjoint multipath are used. The attacker can do so by acting as multiple devices. In figure 1, 'S' is the source node and 'D' is the destination node. Source 'S' has established two disjoint paths, S-A-B-D and S-T-R-D. A Sybil attacker participates in the disjoint paths by acting as two or more independent nodes.

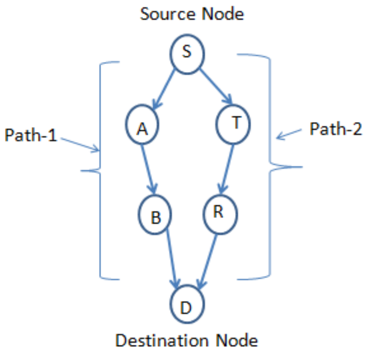

Fig 1: Actual Disjoint Paths

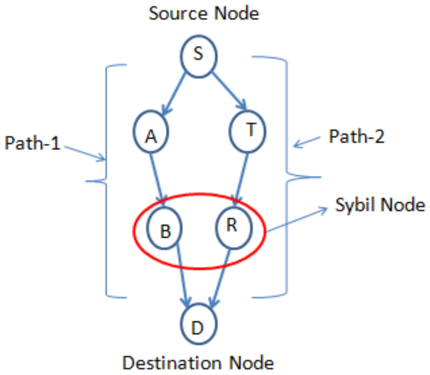

Fig 2: False Disjoint Paths Created by Sybil Attacker

For example, in figure 2, nodes 'B' and 'R' might be the fake identities of a single Sybil node. In this way, the seemingly disjoint paths may actually pass through a single node.

The Non-Simultaneous Sybil attack on the other hand can fool the misbehavior detection system by dropping its previous identity which has done harm to the network and taking another fresh identity.

Vasudev et al. analyzed the effect of the Sybil attack on lowest ID based clustering mechanism in MANETs [5]. In lowest ID based clustering algorithm, the node with lowest ID becomes clusterhead. It has been shown in their work that it is very easy for a Sybil attacker to forge an identity which is minimum among its surrounding nodes. As a result, a Sybil attacker can deliberately take the position of a clusterhead. The base protocol DSR, is one of the very popular routing protocols available in Mobile ad-hoc networks. In DSR, the source node finds a route to the destination only when the route is required. Several researchers have analyzed the impact of various attacks on DSR [6] [7] [8] [9].

3. ATTACK MODEL

When a node frequently changes its IP address (by discarding previous identity and taking a new one), it can potentially affect the working of routing protocol. In DSR, the source node first establishes a route to the destination through RREQ (Route request) and RREP (Route Reply) messages and then forwards the data along that path. As shown in figure 3, let's say, nodes S, A, B, C, D have identity ID-1, ID-2, ID-3, ID-4 and ID-5 respectively. S is the source and wants to send packets to destination node D. The discovered path is S-A-B-C-D. We assume that node C exhibits non-simultaneous Sybil behavior. If node C stops sending the packets by discarding its current identity ID-4 and comes up with a new identity ID-5, then the route from S to D will be disrupted (Figure 4). Due to this, node B will notice a link failure. As a result, a route error will be generated by node B due to which node S has to find a route to the destination D again. Node C on the other hand, will join the network with a new identity ID-5. The attacker Node C, repeats this process by leaving and joining the network with new identities, disrupting the route repeatedly. As a result, the source will be engaged in finding path multiple times due to path breakage. This may result in decreased throughput, increased routing load, and increased end to end delay. Also, the impact will accentuate if there are multiple attackers in the network.

A node keeps on gathering information about new links it has learned in the route cache. When a Sybil attacker continuously keeps on making and breaking the links using new identities, some of the information in route cache becomes useless.

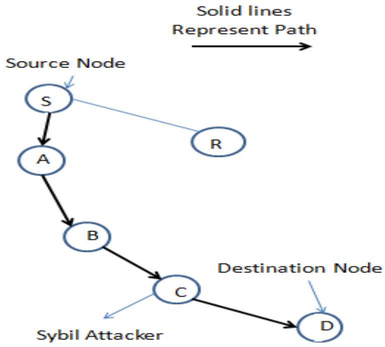

Fig 3: Initial Path

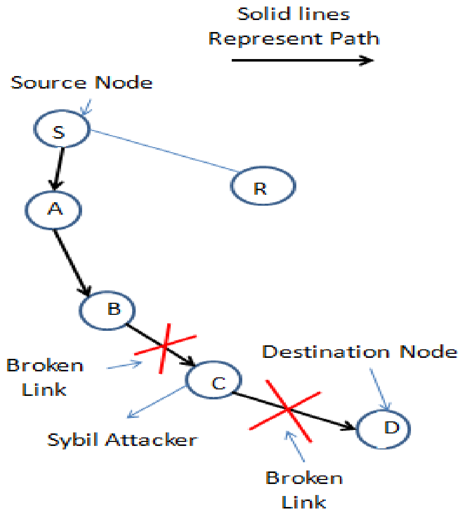

Fig 4: Broken Path

4. SIMULATION

Simulation has been done using Network Simulator (NS2). Two scenarios have been created. In first scenario, DSR without attack has been taken. In second, non-simultaneous Sybil attack has been launched on DSR.

4.1 Network Parameters in NS2

Following are the main simulation parameters and their corresponding values that have been set for this experiment in NS2.

Table 1. Network Parameters

Parameter	Value
Platform	Linux CentOS 5
NS Version	Ns-2.33
Mobility Model	Random Way Point
Traffic Type	CBR
Area of Simulation	500 * 500 m
Packet Size	512 bytes
Protocol	DSR
Packet Size	512 bytes
Pause Time	0, 20, 50, 100, 200, 250, 300, 350, 400

4.2 Performance Metrics

To evaluate the performance of DSR with and without attack, Throughput and End-to-End Delay have been taken as metrics.

4.2.1 Throughput

It is defined as the ratio of data packets received at the destination to those generated by source.

4.2.2 End to End Delay

Latency in a network, usually includes four parts: The transmission delay, queuing delay, propagation delay and processing delay. End to End Delay signifies the total amount of time taken by a packet from source to destination.

5. ANALYSIS & RESULTS

5.1 Throughput

Throughput of DSR, with and without Sybil attack has been plotted against different pause time. Pause time is the time for which all the nodes pause before moving further to next position. It can be seen from the graph (Figure 5) that the throughput of DSR decreases when the attack is launched. Since the attacker is switching its identities frequently, the packet dropping is increased resulting in decreased throughput.

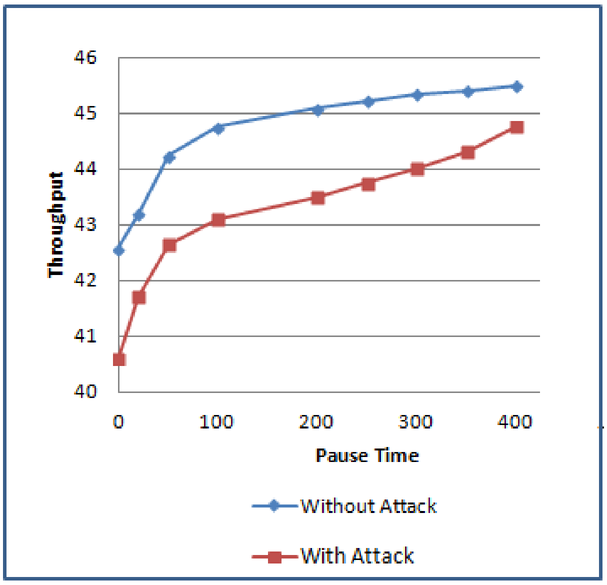

Fig 5: Throughput Graph

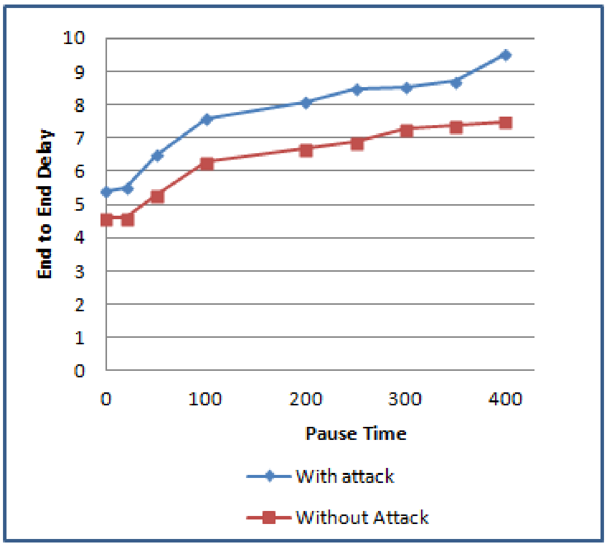

Fig 6: End to End Delay Graph

5.2 End to End Delay

The End-to-End Delay graph (Figure 6) shows that delay has increased in the presence of attack as compared to scenario when the attacker is not present in the network. The reason for the increase is that when an attacker comes between source and destination, it continuously breaks the path of communication. Such a behavior of the attacker forces the source node to find the path to destination repeatedly. Consequently, the packet delivery time increases.

6. CONCLUSION AND FUTURE WORK

It has been observed that Sybil attacker has reduced the Throughput and increased the End to End Delay of the network. It can be seen from the graphs that the Sybil attacker affects the network more when the pause time is low as compared to higher values of pause time. This is due to the fact that when pause time is greater, the network becomes more stable and hence routing disruption caused by Sybil nodes has less effect on the network throughput. The attacker also increases the flow of routing packets in the DSR protocol thus increasing routing load. With the help of this analysis, the properties of the Sybil attacker have been found out. In future, the work will be done on analyzing the impact of Sybil attack on other routing protocols in MANETs. Also, work will be done on finding out a detection mechanism for the non-simultaneous Sybil attack.

7. REFERENCES

[1] Douceur, J. R., “The Sybil Attack,” presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, pp. 251–260, 2002.

[2] Newsome, J., Shi, E., Song, D., Perrig, A., “The Sybil Attack in Sensor Networks: Analysis and Defenses,” presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), pp. 259–268, 2004,.

[3] Johnson, D. B., Maltz, D. A., Hu, Y.C., and Jetcheva, J. G., "The Dynamic Source Routing Protocol For Mobile Ad hoc Networks", IETF Internet draft, draft-ietf-manet-dsr-04.txt, November 2000.

[4] Mohaisen, A., Kim, J., "The Sybil Attack And Defenses: A Survey, Smart Computing Review, vol. 3, no. 6, December 2013.

[5] Vasudevand, A., Sood, M., “Sybil Attack On Lowest id Clustering Algorithm In The Mobile Ad hoc Network”. International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012

[6] Salehi, M., Samavati, H., Dehghan, M., "Evaluation of DSR Protocol Under A New Black Hole Attack", Electrical Engineering (ICEE), 2012 20th Iranian Conference on , vol., no., pp.640,644, 15-17 May 2012 doi: 10.1109/IranianCEE.2012.629243.

[7] Agrawal, R., Tripathi, R., Tiwari, S., "Performance Evaluation and Comparison of AODV and DSR Under Adversarial Environment," Computational Intelligence and Communication Networks (CICN), 2011 International Conference on, vol., no., pp.596,600, 7-9 Oct. 2011

[8] Salehi, M., Samavati, H., "DSR vs OLSR: Simulation Based Comparison of Ad Hoc Reactive and Proactive Algorithms Under the Effect of New Routing Attacks," Next Generation Mobile Applications, Services and Technologies (NGMAST), 2012 6th International Conference on , vol., no., pp.100,105, 12-14 Sept. 2012.

[9] Ahuja, R., Ahuja, A.B., Ahuja, P., "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack," Image Information Processing (ICIIP), 2013 IEEE Second International Conference on , vol., no., pp.699,702, 9-11 Dec. 2013.