Indian Journal of Science and Technology, Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/100217, August 2016

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Vampire Act of Sybil Attack on the Highest Node Degree Clustering in Mobile Ad Hoc Networks

Amol Vasudeva*, **Manu Sood and Prem Prakash**

Department of Computer Science and Engineering & Information Technology, Jaypee University of Information Technology, Waknaghat, Solan Himachal Pradesh, India; amol.vasudeva123@gmail.com

Abstract

Objective: This paper aims at analyzing the devastating effect of Sybil attack in Mobile Ad hoc NETworks (MANETs) that use the Highest Node Degree based Clustering scheme for routing. **Method/Analysis:** A Sybil attack can disrupt the highest node degree based clustering scheme in MANETs by impersonating the identity of a legitimate node. An attacker will put all its efforts in forcibly electing its prey node as the leader of a cluster. In making its mission successful, an attacker uses a number of ghost identities to interact with the prey node, and hence increasing the connectivity of that prey node. It can achieve this by allowing its multiple Sybil nodes to communicate directly with a legitimate prey node. In other words, all the Sybil nodes contribute to increase the node degree of a particular prey node, so as to make it a cluster head. The Sybil attack can play the same trick on the same prey node in every cluster formation process by following the direction and movement the prey node. After making this prey node as a cluster head the multiple Sybil nodes can start sucking its battery by communicating with the bogus messages. Once the battery of the prey node is drained completely, the Sybil attacker can impersonate its identity to further disrupt the network system. **Findings:** We have used Java language to simulate the vampire act of Sybil attack in MANETs. All the results obtained from the experiments prove that a Sybil attack succeeded with high probability, in forcibly re-electing the same prey node as a leader of the cluster. **Novelty:** The vampire act of Sybil attack on the maximum connectivity based clustering is shown for the first time in this paper.

Keywords: Highest Node Degree Clustering, Malicious Device, Mobile Ad Hoc Network, Sybil Attack, Sybil Node

1. Introduction

A MANET consists of a number of heterogeneous moving devices that communicate on a wireless media, in a peer to peer manner. These networks totally discard the need of any infrastructure or the central management system[1]. The devices can move randomly with different velocities leading to dynamic topology of these networks[2]. The nodes within the vicinity of each other can establish a direct communication between them. On the other hand, the nodes that are not within the vicinity of each other can send and receive messages, through the intermediate nodes between them. This may lead to large propagation delays, in the case of a large scale network. To resolve this problem, the whole network can be partitioned into groups or clusters, on the basis of certain properties[3]. Clustering in MANETs can lead to significant improvement in resource management, such as bandwidth consumption, and network performance in terms of route delays and throughput etc[4]. Each cluster is managed by a cluster head, which is elected on the basis of node characteristics such as minimum and maximum identity, node degree or mobility etc. All the one-hop neighbors of a cluster head are called the member of the cluster. It is also possible for some nodes to be within the vicinity of more than one cluster; these are called the gateway nodes and are used for inter-cluster communication. Because of the mobile environment, battery power constraints, and independency on the central management system, MANETs are vulnerable to various kinds of attacks[5], such as wormhole attack[6], black hole attack[7], rushing attack[8], and Sybil attack[9] etc.

*Author for correspondence

A single physical device sending messages with multiple ghost identities or Sybil identities is known as the Sybil attack[9,10]. A legitimate node receiving the messages from multiple ghost identities (that belong to the single physical device) will assume them as different nodes. There are three different forms of a Sybil attack depending on the behavior of its Sybil nodes[10].

The first one is the way of exchanging the information between Sybil nodes and other nodes in the network. A malicious device can use two methods to provide the communication between its Sybil nodes and neighbors. In the first method, all the Sybil nodes directly send their messages to the one-hop neighbors of the malicious node. For example, if *i* represents one-hop neighbor of a malicious node, then all the Sybil nodes will also act as one-hop neighbor of the node *i*. These Sybil nodes are called direct Sybil nodes[10]. In the second method, all the Sybil nodes exchange their information with node *i*, through the malicious device, i.e. the node *i* will assume all the Sybil nodes as its two-hop neighbors. This is called indirect communication of Sybil nodes[10]. The second form of the Sybil attack is concerned with the appearance of Sybil nodes in the network. All the Sybil nodes can appear into the network concurrently or one-by-one in different intervals of time. The third form is concerned with assigning unique identification numbers to the Sybil nodes. There are two possible ways to allocate identification numbers to the Sybil nodes. One way is to assign fake identification numbers, so that they are different from the identification numbers of the legitimate nodes in entire network. The other way is to get the identification number of already existing nodes in the network, after their impersonation.

According to authors[10,11], a Sybil attack can affect various mechanisms of an ad hoc network, including zone based and multipath routing, vote based schemes, fair allocation of resources and aggregation of data etc. In this paper we explore the vampire behavior of the Sybil attack in the sense that it sucks the batteries of legitimate nodes in a MANET, for stealing their identities. A MANET using the highest node degree clustering scheme for routing are vulnerable to this kind of attack. In a highest degree clustering algorithm, a node with maximum one-hop connectivity among its neighbors is elected as the cluster head[12]. If two or more nodes have the same node degree within the same cluster, then the node with minimum identity is elected as the cluster head. A Sybil attacker can disrupt the highest connectivity based clustering by using a number of ghost identities or Sybil nodes. It can do so by using its multiple Sybil nodes to increase the node degree of its prey node and thereby increasing the chances of this prey node in becoming a cluster head. The Sybil nodes will put all their efforts to elect the same node as a cluster head, during each election process. Moreover, in order to drain the battery of its prey node, a malicious device will allow all its ghost identities to repeatedly communicate with the prey node. The malicious device can steal the identity of the prey node, after sucking its power completely.

In the rest of this paper, section 2 explains the vampire behavior of the Sybil attack, on the highest connectivity clustering scheme. In section 3, we show the success rate of Sybil attack in achieving its goal, through experiments. Section 4 ends the paper with concluding remarks.

2. Vampire Act of the Sybil Attack

A vital issue in MANETs is to avoid the unnecessary communication and computational overhead that leads to the battery consumption of its nodes. The complete drainage of a node's battery simply means the death of this node, i.e. the node is unable to provide its services to the network. Taking advantage of the battery constraint in MANETs, a Sybil attack can also be launched to impersonate the legitimate nodes in a MANET, by sucking their batteries. The MANETs using the highest degree clustering scheme for routing are victim of this kind of attack. A cluster head is the busiest member of a cluster in terms of processing and communication overheads. It is actively involved in exchange of the information within its own cluster, as well as with other clusters[13]. In order to achieve this, a cluster head has to keep extra information in its memory, such as details of its member and gateway nodes, details of other cluster heads, and routing information etc. Due to these extra responsibilities, the consumption of the battery is more in a cluster head than the ordinary nodes. A Sybil attacker can damage the highest connectivity clustering scheme by sending messages through its multiple ghost identities to a legitimate prey node. The idea is to increase the node degree of the prey legitimate node and hence increase the chances of making it a cluster head.

Let a malicious device has entered into the network with the intention of launching a Sybil attack. A malicious device continuously starts wandering into the network, so as to attain the needful details about the network. If the network is large, multiple malicious devices may take their positions in various areas of the network. After a fixed interval of time, all of these devices can move out of the range of the network to share their information. The process of spying can be stopped immediately after gaining the required information. Thereafter, all the malicious devices can re-enter into the network for launching the Sybil attack. Multiple malicious devices can choose their individual prey nodes, (i.e. the legitimate nodes whose batteries have to be drained). Generally, the weaker nodes in terms of energy can be chosen as the prey nodes. This will help the Sybil nodes to drain the battery in comparatively lesser time. The energy level of the nodes can be estimated by the strength of the signal received from each node, i.e. the Received Signal Strength Indicator (RSSI) value. A weaker node in terms of energy will have a weaker RSSI value.

During the cluster head election process, all the malicious devices can use their respective Sybil or ghost nodes to send the hello messages to their respective prey nodes. Here, the idea is to forcibly make the prey nodes as leaders of their respective clusters, by increasing their neighbors. But, on the other hand, all the Sybil nodes will also be involved to increase the node degree of the other legitimate neighbors of the malicious device. To resolve this problem, the malicious device can introduce its Sybil nodes by gradually reducing their respective transmission powers. In addition to this, the malicious device must be very close to its prey node. If Sybil nodes are communicated directly by gradually reducing their ranges, the chances for all the Sybil nodes to be within the vicinity of the malicious device's one-hop neighbors are very low. It depends on the distance between malicious device and malicious device's one-hop neighbors. If the transmission range of a Sybil node is less than the distance between a legitimate node and malicious device, then this Sybil node cannot be within the vicinity of that legitimate node. Greater the distance between malicious device and its one-hop neighbors, lesser are the chances of these neighbors to be within the vicinity of the Sybil nodes. Therefore, only a few Sybil nodes with comparatively higher ranges can be within their vicinity of the legitimate node. On the other hand, the malicious device is kept at such a distance from the prey node, so that this distance is less than or equal to the minimum transmission range in the Sybil node group. Therefore, all the Sybil nodes will be within the vicinity of their prey node. This will result in increase in the probability of forcibly making the prey node as a leader of the cluster. For example, consider the Figure 1 where *A*, *B* and *C* are the legitimate nodes and *M* is a malicious device. The malicious device *M* is targeting the node *C* to drain its battery by introducing five Sybil nodes S_1, S_2, S_3, S_4, and S_5, with their transmission ranges as $R(S_1)$=30, $R(S_2)$=25, $R(S_3)$=20, $R(S_4)$=15 and $R(S_5)$=10, respectively. Let the distance of malicious device *M* from its legitimate nodes *A*, *B* and *C* is given as $|MA| = 28$, $|MB| = 22$ and $|MC| = 9$, respectively. As $R(S_1) > R(S_2) > R(S_3) > R(S_4) > R(S_5)$, we can observe that

$R(S_1) \geq |MA| > R(S_2)$, i.e. only S_1 is within the communication range of *A*;

$R(S_2) \geq |MB| > R(S_3)$, i.e. S_1 and S_2 are within the communication range of *B*;

$R(S_5) \geq |MC|$, i.e. all the five Sybil nodes are within the communication range of *C*.

The other advantage of gradually decreasing the transmission ranges of the Sybil attack is that its detection becomes very difficult; which has been discussed later in the subsection 2.3.

It is also required for all the Sybil nodes to follow the movement of their prey node. The relative direction of movement of the prey node can be identified if the malicious devices are enabled with directional antennas. The next problem is how to identify the speed of the node and whether the node is moving away from the malicious device or approaching towards it. According to the Frii's free space propagation model[14], $P_r / P_t \propto 1/d^2$, where P_t is the transmitted power and P_r is the received power at a distance *d*. On the basis of the Frii's free space model, a malicious device can also estimate the relative mobility of the prey node by computing the ratio of two consecutive RSSI signals received from this prey node[15]. If the prey

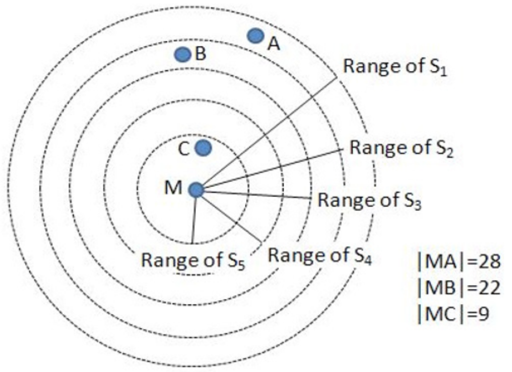


Figure 1. Effect of gradually decreasing the transmission ranges of the Sybil nodes

node is moving away from the malicious device, then the RSSI value of second signal will be less than the RSSI value of the first signal. On the other hand, if the RSSI value of the second signal is greater than the RSSI value of the first signal, then the legitimate node is approaching towards the malicious device.

The malicious device is continuously involved in communicating through its multiple Sybil nodes, with the prey node. Although the device is enabled with more battery, memory and processing capabilities, its battery is likely to get drained completely, after some time. For this, an attacker can replace the currently active malicious device with a new device, after reaching a certain threshold level of the battery. The whole information of the previous device can also be transferred to the new device. The step by step procedure of the vampire act of the Sybil attack has been explained in the following subsection and Figure 2.

2.1 Assumptions and Notations Used

1. Consider that a MANET consists of N number of mobile nodes. Any node can disappear from the network due to the drainage of its battery or some other reason. In addition to this, new nodes may also arrive to join the network.
2. The identity of each node is represented by a set $X = \{x_i\}$, where $i = 0, 2, \ldots, N{-}1$.

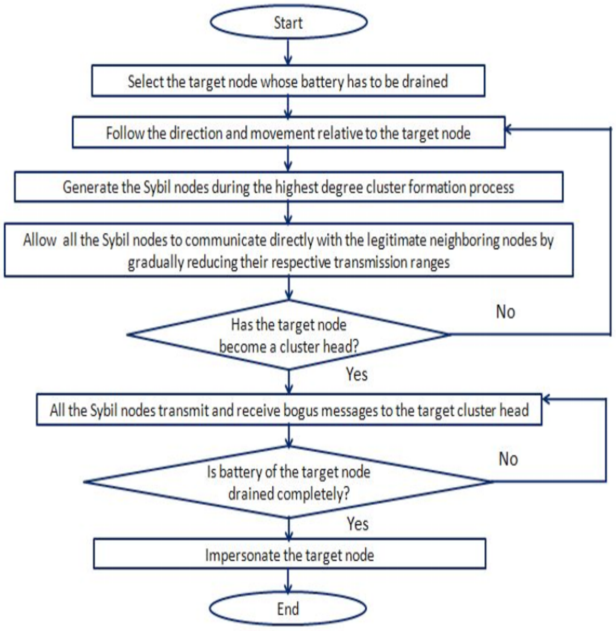

Start
Select the target node whose battery has to be drained
Follow the direction and movement relative to the target node
Generate the Sybil nodes during the highest degree cluster formation process
Allow all the Sybil nodes to communicate directly with the legitimate neighboring nodes by gradually reducing their respective transmission ranges
Has the target node become a cluster head?
No
Yes
All the Sybil nodes transmit and receive bogus messages to the target cluster head
Is battery of the target node drained completely?
No
Yes
Impersonate the target node
End

Figure 2. Steps involved in impersonating its prey node, by the malicious node

3. m_j ($j = 0, 1, \ldots, n{-}1$) represents n number of malicious devices, such that $n << N$. These malicious devices have occupied different positions in the network for spying purposes.
4. Each malicious device introduces its Sybil nodes by gradually reducing their respective transmission powers.
5. The identities of the Sybil nodes are changed periodically.
6. All the malicious devices are equipped with directional antennas.
7. The malicious devices are powerful in terms of battery power, memory, and processing capabilities.

2.2 Steps Involved in the Vampire Act of Sybil Attack

1. Let the malicious devices m_n have chosen their respective prey nodes x_{pk}, for sucking the battery. Here, k = 1, 2, …, n (the number of prey nodes is same as that of number of malicious devices) and x_{pk} $\in X$.
2. In the next step, all the malicious devices, i.e. m_n move towards their respective prey nodes x_{pk} and continuously follow the movement of x_{pk}.
3. During the cluster formation process, each of the malicious devices generates a set S of n' ($n' < N$) number of fabricated Sybil identities or nodes, represented as $s_0, s_1, \ldots, s_{n'-1}$. All these Sybil nodes are presented simultaneously and allowed to communicate directly by gradually reducing their transmission powers. In other words, if $R(S)$ represents the transmission range of Sybil nodes in the set S, then $R(s_0) > R(s_1) > \ldots > R(s_{n'-2}) > R(s_{n'-1})$, where $R(s_{n'-1})$ is less than or equal to the distance between malicious device m_n and its prey node x_{pk}, i.e. $R(s_{n'-1}) \le |m_n\, x_{pk}|$.
4. Since $|m_n\, x_{tk}| \ge R(s_{n'-1})$, all the n' numbers of Sybil nodes can establish link with the prey node. On the other hand, $|x_i\, x_{pk}| \le R(s_{n'-1})$, the number of Sybil nodes that can communicate with the other legitimate neighbors of the malicious node will always be less than or equal to the total number of Sybil nodes. That is, if n'' represents the number of Sybil nodes that are within the vicinity of other legitimate neighbors (except the prey node), then $0 \le n'' \le n'$. Thus, the prey node has the higher probability of being elected as a cluster head, as compared to other legitimate neighbors.

5. After succeeding in forcibly making a prey node as the leader of a cluster, all the n' Sybil nodes will start a session of continuous communication with it.
6. The above steps will be repeated till the complete consumption of battery of the prey node. At this point, an attacker can capture the identity of prey node to create a stolen Sybil identity.

2.3 Credibility of Current Mechanisms to Thwart Against this Variant of Sybil Attack

Various schemes have been proposed by authors to prevent or detect the Sybil attack in ad hoc networks. Some of the most commonly used schemes are based on the localization of nodes, mobility of nodes and random key pre distribution etc.

Authors have proposed an RSSI based solution to detect a Sybil attack, according to which two or more nodes having the same RSSI values are suspicious of being Sybil nodes[16,17]. This approach can be applied on the MANETs where all the nodes moving with same speed and in the same directions. However, this scheme fails to detect the proposed vampire act of the Sybil attack, due to variations in the transmission ranges of Sybil nodes.

Mobility of nodes has also been used to detect a Sybil node in MANETs[18]. According to this scheme, an observer nodes keeps on recording the neighbors of each node, it comes across over a period of time. A group of neighboring nodes, which is repeated a number of times can be identified as a group of Sybil nodes. But, the scheme fails completely if identification numbers of the Sybil nodes are altered frequently or the Sybil nodes are being communicated indirectly. Therefore, the proposed Sybil attack with vampire behavior cannot be detected using this scheme as it follows the first condition completely and the second condition partially (some of Sybil nodes may communicate directly, whereas other will communicate indirectly).

Random key pre distribution schemes[19–21] require multiple data transmission between two nodes and a number of encryption and decryption operations to authenticate each other. In a mobile environment, the nodes might go away from each other's vicinity, before the completion of authentication process. Thus the scheme is not suitable for highly mobile networks.

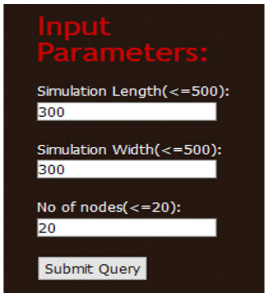
3. Simulation Environment and Results

Table 1 summarizes all the simulation parameters being used in our simulations. We have done our simulation in Java, using the concepts of animation, multithreding, swings and jdbc etc.

We have simulated a MANET initially with twenty legitimate nodes, deployed randomly in the simulation area of 300 × 300 pixels. However the simulation area can be taken a maximum up to 500 × 500 pixels, as shown in the Figure 3. After pressing the submit button, the nodes are deployed in the simulation area and move in random directions and speed using the Random Way Point mobility model[22]. Figure 4 shows the deployment and movement of the legitimate nodes (yellow color) inside the simulation area. All the twenty legitimate nodes are assigned their identities between 0 and 19. The speed of each node may lie between 0 to 10 pixels per second. The nodes can move in random directions between 0 and 360 degrees. The transmission range of all the legitimate nodes is 120 pixels. An adjacency table, shown in the Figure 5 represents the neighbor status of each node with respect to the other nodes. The adjacency table is updated with the movement of the nodes. The observation period

Table 1. Summary of the simulation environment

Parameter	Value
Simulator	Java
Simulation area	300 pixel × 300 pixel
Transmission range of the legitimate nodes	120 pixels
Number of legitimate nodes	20
Total number of observations	25
Time per observation	Variable, by selectioning the pause button
Mobility model	Random Waypoint Mobility Model
Speed of nodes	0–10 pixels/second
Movement direction in degree	0 to 2π
Number of malicious devices	1
Number of Sybil nodes	5
Presentation of Sybil nodes	Simultaneous
Transmission range of Sybil nodes	30, 25, 20, 15, 10
	50, 40, 30, 20, 10
	100, 80, 60, 40, 20



Input Parameters:

Simulation Length(<=500): 300

Simulation Width(<=500): 300

No of nodes(<=20): 20

Figure 3. Input the simulation area and number of nodes

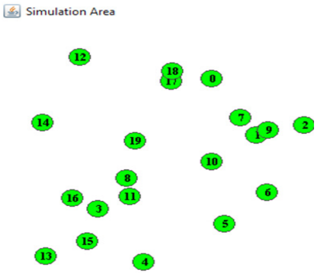
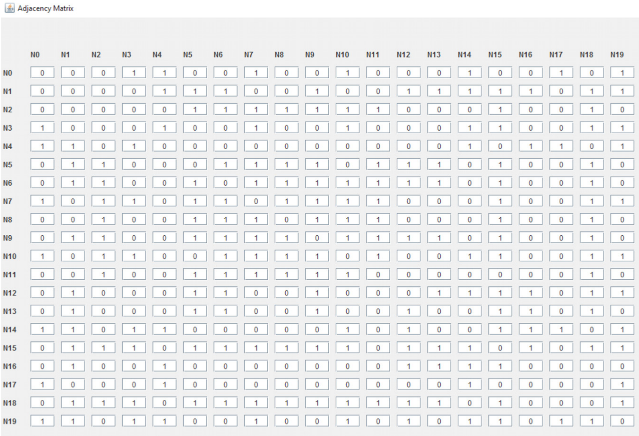


Figure 4. Nodes are deployed into the simulation area and are moving according to the Random Waypoint Mobility model


Adjacency Matrix

	N0	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	N12	N13	N14	N15	N16	N17	N18	N19
N0	0	0	0	1	1	0	0	1	0	0	1	0	0	0	1	0	0	1	0	1
N1	0	0	0	0	1	1	1	0	0	1	0	0	1	1	1	1	1	0	1	1
N2	0	0	0	0	0	1	1	1	1	1	1	1	0	0	0	1	0	0	1	0
N3	1	0	0	0	1	0	0	1	0	0	1	0	0	0	1	1	0	0	1	1
N4	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1
N5	0	1	1	0	0	0	1	1	1	1	0	1	1	1	0	1	0	0	1	0
N6	0	1	1	0	0	1	0	1	1	1	1	1	1	1	0	1	0	0	1	0
N7	1	0	1	1	0	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1
N8	0	0	1	0	0	1	1	1	0	1	1	1	0	0	0	1	0	0	1	0
N9	0	1	1	0	0	1	1	1	1	0	1	1	1	1	0	1	0	0	1	0
N10	1	0	1	1	0	0	1	1	1	1	0	1	0	0	1	1	0	0	1	1
N11	0	0	1	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0
N12	0	1	0	0	0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	1
N13	0	1	0	0	0	1	1	0	0	1	0	0	1	0	0	1	1	0	1	0
N14	1	1	0	1	1	0	0	0	0	0	1	0	1	0	0	1	1	1	0	1
N15	0	1	1	1	0	1	1	1	1	1	1	0	1	1	1	0	1	0	1	1
N16	0	1	0	0	1	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
N17	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
N18	0	1	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	0	0	1
N19	1	1	0	1	1	0	0	1	0	0	1	0	1	0	1	1	0	1	1	0

Figure 5. Adjacency matrix representing the neighbors of each node

is variable as the user can press the pause button any time to see the formation of clusters. Figure 6 shows the formation of clusters on the basis of the highest node degree algorithm, where each cluster is represented by a circular area. The blue nodes represent the heads of each cluster and the yellow nodes represent its member nodes or gateway nodes. Figure 7 depicts the details of the clusters formed during an observation, i.e. the cluster identity, the cluster heads and the members of each cluster head.

Then we introduce five Sybil nodes (red color) with their identities as 20, 21, 22, 23 and 24. Figure 8 illustrates the introduction of Sybil nodes in the simulation. All these Sybil nodes are presented simultaneously and are allowed to communicate directly by gradually reducing their transmission ranges to 30, 25, 20, 15 and 10 pixels, respectively. These Sybil nodes choose the node 17 as their prey node. All these Sybil nodes and very close to the prey node 17 and follow the direction and movement of this prey node. All these Sybil nodes contribute to increase the chances of this prey node, in becoming a cluster head. Figure 9 shows that the Sybil nodes have succeeded in making the prey node 17 as a cluster head.

After each observation, we collected the information about the number of clusters formed, along with their respective cluster heads and members. We have collected the results from 25 such observations. Details of the clusters formed during each observation are shown in the Table 2. For example, four clusters formed in the observations are given as:

17{8, 10, 12, 13, 16, 19, 20, 21, 22, 23, 24},
1{3, 5, 6, 10, 11, 12, 13, 14, 15, 18},
4 {0, 2, 3, 5, 7, 13, 16, 19}, and
9 {6, 8, 10, 12, 14, 15, 18}.

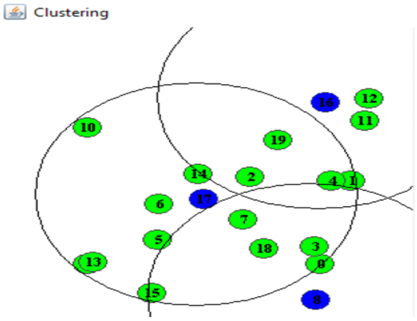
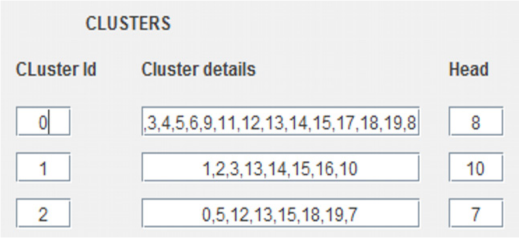


Figure 6. Cluster formation on the basis of highest node degree. Blue nodes represent the heads of each cluster



CLUSTERS

CLuster Id	Cluster details	Head
0	3,4,5,6,9,11,12,13,14,15,17,18,19,8	8
1	1,2,3,13,14,15,16,10	10
2	0,5,12,13,15,18,19,7	7

Figure 7. Details of the clusters formed in an observation

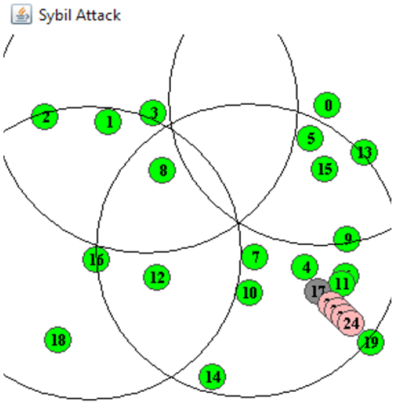


Figure 8. Inclusion of the five Sybil nodes, represented by red color (20–24) that are targeting the node 17

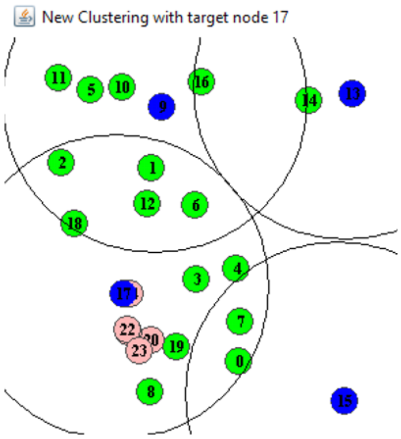


Figure 9. After cluster formation process, the Sybil nodes succeeded in making their prey node 17 as the cluster head

Table 2. Details of the cluster formation after 25 observations

Observation No	Number of Cluster formed	Cluster Head {Cluster Members}
1	4	**17**{8,10,12,13,16,19,20,21,22,23,24}, **1**{3,5,6,10,11,12,13,14,15,18 }, **4**{0,2,3,5,7,13,16,19}, **9**{6,8,10,12,14,15,18}
2	4	**17**{0,1,3,4,6,11,16,19,20,21,22,23,24}, **5**{2,6,7,8,12,13,14,15,18}, **9**{3,11,14,15,18}, **10**{2,7,12}
3	4	**17**{1,2,3,5,6,10,11,16,19,20,21,22,23,24}, **0**{2,3,4,6,7,8,14}, **12**{4,5,7,15,16}, **13**{3,6,8,9,18}
4	2	**6**{0,1,2,3,5,6,8,10,11,12,14,15,16,17,18,19,20,21,22,23,24}, **5**{1,4,7,10,11,12}
5	2	**17**{0,1,2,3,6,7,8,9,10,11,12,13,14,19,20,21,22,23,24}, **4**{12,13,14,15,16,18}
6	3	**12**{0,1,2,4,5,7,9,10,11,13,14,15,18,19}, **17**{9,10,13,16,18,19,20,21,22,23,24}, **8**{3,4,9,13,16,18,19}
7	4	**17**{9,10,11,13,18,19,20,21,22,23,24}, **2**{0,1,4,5,6,7,12,14}, **16**{4,12,14}
8	3	**0**{1,4,7,9,10,11,12,13,14,15,16,18}, **17**{2,3,7,19,20,21,22,23,24}, **5**{4,6,8,11,12}
9	3	**8**{0,1,2,4,5,6,7,9,10,11,12,13,15,16,18,19}, **17**{1,2,3,9,16,18,19,20,21,22,23,24}, **14**{0,5,10}
10	4	**17**{2,7,9,10,15,18,19,20,21,22,23,24}, **6**{0,1,3,8,9,10,11,13,14,16,18}, **12**{2,4,7,21,22}, **5**{4,14}
11	3	**17**{0,6,7,9,14,16,18,19,20,21,22,23,24}, **11**{1,3,7,8,9,10,13,14,15,19,20}, **12**{4,8}
12	3	**17**{6,7,8,12,14,15,19,20,21,22,23,24}, **16**{1,3,5,6,8,11,13,15,18,19}, **0**{3,6,8,9,10,15,18}
13	4	**17**{1,12,13,14,16,19,20,21,22,23,24}, **9**{1,5,8,10,18,19}, **7**{0,4,12}, **15**{11}
14	3	**17**{3,8,9,10,11,16,19,20,21,22,23,24}, **6**{0,1,2,3,11,14,18,24}, **15**{1,3,4,5,7,12,13}
15	3	**6**{0,2,3,4,5,7,8,11,13,14,16,18}, **17**{2,4,7,10,12,19,20,21,22,23,24}, **15**{1,7,9,12}
16	4	**5**{2,3,4,6,7,9,11,12,13,14,15,17,18,19}, **10**{2,3,7,8,11,15,19,22,23}, **16**{6,9,13,14,18}, **1**{0,2,7}
17	4	**17**{1,8,9,15,18,19,20,21,22,23,24}, **3**{0,1,2,5,6,9,10,11,16}, **14**{4,5,6,10,11,13}, **12**{1,4,7,13}
18	3	**17**{2,3,5,6,8,11,12,13,15,19,20,21,22,23,24}, **6**{0,1,4,7,9,12,14,16,18}, **10**{0,2,13}
19	3	**17**{3,14,15,16,18,19,20,21,22,23,24}, **5**{0,1,2,3,4,6,7,8,12,14,16}, **9**{8,13,15,18,19,20}
20	4	**5**{1,3,4,6,7,8,9,11,12,14,15,18}, **3**{0,2,4,7,10,11,13,15}, **16**{6,8,9,12,4,18}, **17**{19,20,21,22,23,24}
21	4	**17**{1,7,9,10,13,14,16,19,20,21,22,23,24}, **18**{4,5,6,11,12,14,16}, **3**{0,6,8,9,13,16}, **1**5{2,4,5,12,14,21}
22	3	**17**{1,2,6,8,9,10,11,18,19,20,21,22,23,24}, **6**{0,3,5,8,11,12,13,14,15,16}, **1**{0,4,7,12,13,14}
23	4	**17**{3,14,15,18,19,20,21,22,23,24}, **8**{1,2,3,4,6,7,10,11,12,14,15}, **9**{4,7,11,12,13,15,18}, **5**{13,15,18}
24	4	**17**{1,12,14,15,16,19,20,21,22,23,24}, **18**{0,5,8,9,13,16,19,21}, **4**{2, 6, 7, 10, 12}, **1**{3, 15}
25	3	**17**{1,3,6,8,9,11,12,13,19,20,21,22,23,24}, **15**{0,2,4,5,6,7,9,10,13,14,16,18}, **3**{9,14,18}

Here 17, 1, 4 and 9 represent the cluster heads and a set of values corresponding to each cluster head represents their members. On the basis of this information we computed the number of times each node became a cluster head out of 25 observations, which has been shown in the Figure 10. One can see from Figure 10 that the Sybil nodes succeeded in making the prey node 17 as the cluster head 23 times out of these 25 observations, i.e. with a success rate of 92 percent.

Similarly, we also tested the results with the two different sets of transmission ranges for the Sybil nodes at (50, 40, 30, 20, 10) and (100, 80, 60, 40, 20), depicted in Figure 11 and 12, respectively. Figure 11 shows that with the increase in the transmission ranges the percentage of cluster formation of the prey node 17 has reduced to 72 percent. Similarly, in Figure 12 the percentage has declined to 36 percent, by further increasing the transmission ranges. The reason lies in the fact that if the transmission ranges of Sybil nodes are increased, the other one-hop neighbors the malicious device may also fall within the vicinity of the Sybil nodes. Therefore, we can observe from above results that there is always an increase probability of forcibly making a prey node as the cluster head, with the decrease in the communication ranges of the Sybil nodes.

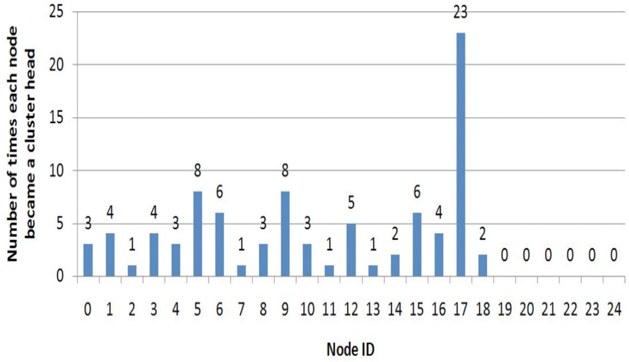


Figure 10. Sybil nodes with transmission ranges of 30, 25, 20, 15, 10

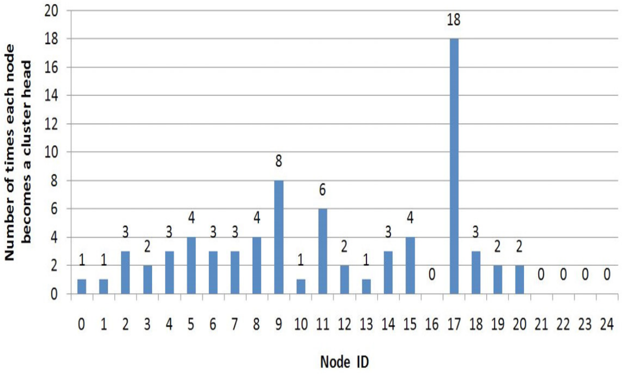


Figure 11. Sybil nodes with transmission ranges of 50, 40, 30, 20, 10

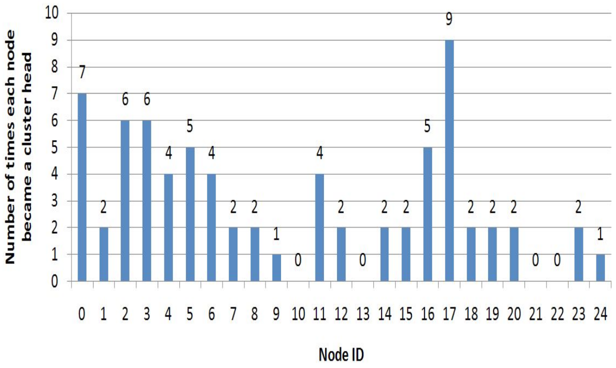


Figure 12. Sybil nodes with transmission ranges of 100, 80, 60, 40, 20

4. Conclusion and Future Work

This paper highlights the vampire behavior of Sybil attack in the sense that it is also capable in sucking the battery of its prey node. The ad hoc networks adopting the highest connectivity based clustering scheme are vulnerable to this kind of attack. During the cluster head election process, a malicious device can use its multiple ghost identities to increase one-hop connections of its prey node; thereby imposing the prey node to be elected as a cluster head. This is possible only if the prey node is within the vicinity of all the ghost nodes, whereas only a few nodes from the group of ghost nodes are within the vicinity of other legitimate neighbors of the malicious device. To achieve its goal, a malicious device involves its multiple Sybil nodes in the election process by reducing their transmission ranges (such that all Sybil nodes have different ranges). As a result, only a few ghost nodes with comparatively higher transmission ranges would be able to communicate with one-hop neighbors of the malicious device, including the prey node. In order to establish the connectivity of all the Sybil nodes with the prey node, the malicious device continuously pursues its prey node by keeping a small gap from it, so that at instance of time, its location is very near to the prey node. As a result, all the Sybil nodes would be able to communicate with the prey node. In this way, the involvement of Sybil nodes leads to increase in more number of connections for the prey node, as compared to the other legitimate neighbors. Therefore, the probability of the prey node to become a cluster head is high during the election. In the next step, the malicious device starts a session of continuous communication through its Sybil nodes to consume the battery of its prey node (cluster head). The above process can be repeated till the full consumption of prey node's battery. At this stage, the malicious device can capture the identity of its prey node to create a new stolen Sybil identity. In the future work we will also study the amount of energy consumed in a cluster head node, while transmitting to and receiving messages from multiple Sybil nodes. This will help in getting an idea of the complete drainage of battery of the prey node. In addition to this, we will also propose a mechanism to mitigate this variant of the Sybil attack in MANETs.

5. References

1. Toh CK. Ad hoc mobile wireless networks: protocols and systems, Prentice Hall: Englewood Cliffs, NJ, USA, 2002.
2. Bertsekas D, Gallager R. Data networks, Prentice Hall: NJ, USA, 2009.
3. Jiang M, Li J, Tay YC. Cluster Based Routing Protocol (CBRP), Draft-ietf-manet-cbrp-spec-01.txt, August 1999.
4. Belding-Royer EM. Hierarchical routing in ad hoc mobile networks. Wireless Communication and Mobile Computing. 2002; 2(5):515-532.
5. Wu B, Chen J, Wu J, Cardei M. A survey on attacks and countermeasures in mobile ad hoc networks. Xiao Y, Shen X, Du D-Z (eds), Wireless/mobile network security, Springer: New York, 2006, 103-135.
6. Hu YC, Perrig A, Johnson DB. Packet leashes: a defense against wormhole attacker in wireless ad hoc networks. Proceedings of IEEE Infocom, 2003, 1976-1986
7. Al-Shurman M, Yoo S-M, Park S. Black hole attack in mobile ad hoc networks. ACM Southeast Regional Conference; 2004. p. 96-97.
8. Hu YC, Perrig A, Johnson DB. Rushing attacks and defense in wireless ad hoc networks routing protocol. Proceedings of ACM WiSe, 2003, 30-40.
9. Douceur JR. The Sybil attack. First International Workshop on peer to peer systems (IPTPS'02), 2002, 1-6.
10. Newsome J, Shi E, Song D, Perrig A. The sybil attack in sensor networks: analysis and defenses. Proceedings of 3rd International Symposium on Information Processing in Sensor Networks, ACM, Berkeley, California, USA, 2004, 259-268.
11. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols. 2003; 1(2-3):293-315.
12. Gerla M, Tsai JTC. Multicluster, mobile, multimedia radio network. Wireless Networks, 1995, 255-265.
13. Chen YP, Liestman AL. A zonal algorithm for clustering ad hoc networks. International Journal of Foundations of Computer Science. 2003; 14(2):305-322.
14. Gibson JD. ed. The Mobile Communication Handbook, CRC Press Inc: 1996.
15. Basu P, Khan N, Little TD. A mobility based metric for clustering in mobile ad hoc networks. Proceedings of the 21st International Conference on Distributed Computing Systems Workshops (ICDCSW '01), 2001, 413–418.
16. Zhong S, Li L, Liu YG, Yang YR. Privacy-preserving location based services for mobile users in wireless networks. Technical Report YALEU/DCS/TR-1297, Yale Computer Science, 2004 July, 1-13.
17. Demirbas M, Song YW. An RSSI based scheme for sybil attack detection in wireless sensor networks. International Workshop on Wireless Mobile Multimedia (WOWMON'06), New York, USA, 2006, 564-570.
18. Prio C, Shields C, Levine BN. Detecting the sybil attack in mobile ad hoc networks. Proceedings of IEEE/ACM SecureComm, 2006 August, 1-11.
19. Bose P, Morin P, Stojmenovic I, Urrutia J. Routing with guaranteed delivery in ad hoc wireless networks. Wireless Networks. 2001; 7(6):609-616.
20. Du W, Deng J, Han YS, Varshney PK. A pair-wise key pre-distribution scheme for wireless sensor networks. ACM Trans, Information and System Security. 2005; 8(2):228-258.
21. Eschenauer L, Gilgor VD. A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communication Security, 2002, 41-47.
22. Mao S. Fundamentals of Communication Networks. In: Cognitive radio communications and networks, Academic Press: 2010; 201-234.