SYBIL ATTACK ON LOWEST ID CLUSTERING ALGORITHM IN THE MOBILE AD HOC NETWORK

Amol Vasudeva[1] and Manu Sood[2]

[1]Department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh, India
amol_dev@rediffmail.com
[2]Department of Computer Science, Himachal Pradesh University, Summar Hill, Shimla, Himachal Pradesh, India
soodm_67@yahoo.com

ABSTRACT

It is quite a challenging task to achieve security in a mobile ad hoc network because of its open nature, dynamically changing topology, lack of infrastructure and central management. A particular harmful attack that takes the advantage of these characteristics is the Sybil attack, in which a malicious node illegitimately claims multiple identities. This attack can exceedingly disrupt various operations of the mobile ad hoc networks such as data aggregation, voting, fair resource allocation scheme, misbehavior detection and routing mechanisms etc. Two routing mechanisms known to be vulnerable to the Sybil attack in the mobile ad hoc networks are multi-path routing and geographic routing. In addition to these routing protocols, we show in this paper that the Sybil attack can also disrupt the head selection mechanism of the lowest ID cluster-based routing protocol. To the best of our knowledge, this is for the first time that a Sybil attack is shown to disrupt this cluster based routing protocol. To achieve this, we illustrate to have introduced a category of Sybil attack in which the malicious node varies its transmission power to create a number of virtual illegitimate nodes called Sybil nodes, for the purpose of communication with legitimate nodes of the Mobile Ad Hoc Network. The variation in the transmission power makes the Sybil attack more deadly and difficult to be detected.

KEYWORDS

Mobile Ad Hoc Network, Network Security, Sybil Attack, Malicious node, Sybil Node, Lowest ID Clustering Algorithm.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) has been the topic of interest among researchers for last two decades. A MANET is a collection of mobile nodes that are connected via wireless links without requirement of any infrastructure or centralized administration. The topology of the MANET is dynamic in nature due to the constant movement of nodes. The mobile nature of nodes, limited bandwidth, high error rates, limited battery power and continuously changing topology brings out new complexities while designing the routing protocols for this kind of network [1]. The conventional routing protocols need to be refurbished or modified, in order to compensate the MANETs mobility and to provide efficient functionality. A number of routing protocols have been proposed by a number of researchers that can be classified into proactive, reactive and hybrid [2]. Proactive protocols are also called table driven protocols in which each node maintains the routing information of other nodes in the network, through regular exchange of network topology packets. In reactive routing protocols, the packets are flooded into network to discover the routes, on demand. Hybrid protocols are the combination of both proactive and reactive protocols.

DOI : 10.5121/ijnsa.2012.4511

Security is also an important concern in the Mobile Ad hoc Networks. The use of open and shared broadcast wireless channel brings out new security challenges in MANETs [3]. Moreover, due to distributed nature of this network, the centralized security control is hard to implement. These characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control and non-repudiation.

There are a wide variety of attacks that target the weakness of MANET routing protocols. Most sophisticated and subtle routing attacks have been identified in some recently published papers such as Blackhole [4], Rushing [5], Byzantine [6], wormhole [7] and Sybil attack [8] etc. A Sybil attack is an attack [8] in which a malicious node illegally claims multiple identities by impersonating other nodes or by claiming fictitious identities. Sybil attacks are also capable of disrupting the routing mechanisms in mobile ad hoc networks. Karlof & Wagner have shown in [9] that multi-path routing and geographical routing schemes are affected by this attack. In case of multi-path routing, there is a possibility that a set of supposedly disjoint paths may be passing through multiple Sybil identities of a single malicious node. In location based routing a malicious node can present multiple Sybil nodes with different positions to its neighbors. Therefore, a legitimate node may choose any of the Sybil nodes while forwarding the packet on the basis of nearest location to the destination node; but in reality it will be passing the packets through the malicious node.

In addition to these routing protocols, we have shown in this paper that the Sybil attack can also disrupt the head selection mechanism of lowest ID based cluster routing algorithm. To the best of our knowledge, this is for the first time that a Sybil attack has been shown to disrupt this routing algorithm. To achieve this, we illustrate to have introduced a category of Sybil attack in which the malicious node varies its transmission power to create a number of virtual illegitimate nodes called Sybil nodes, for the purpose of communication with legitimate nodes of the Mobile Ad Hoc Network. We have used a variant of Sybil attack in which the attacker node introduces its fake IDs to the other nodes in the network, by changing its transmission power; this makes the attack more devastating and difficult to be detected. The rest of this paper is organized as follows. Section 2 describes the Sybil attack in details. Section 3 describes the lowest ID clustering algorithm. Section 4 describes how a Sybil attack can disrupt the clusterhead selection mechanism of the lowest ID clustering algorithm. Section 5 describes various mechanisms for the detection of Sybil attack. Finally, the section 6 concludes the paper.

2. Sybil Attack

Sybil attack was first introduced by J. R. Douceur [8]. According to Douceur, the Sybil attack is an attack in which a single entity can control a substantial fraction of the system by presenting multiple identities [8].

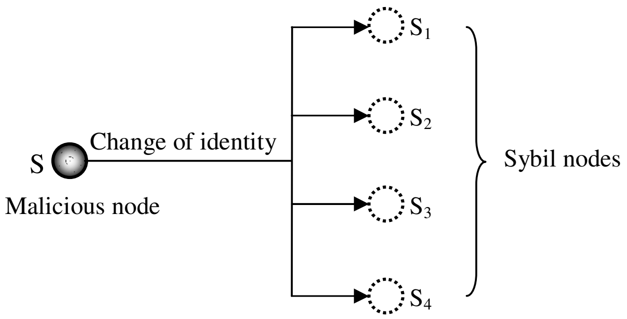

Figure 1. A Sybil attacker with multiple identities

In other words, a simple presentation of multiple identities for a single physical node can be considered to be a Sybil attack. The Sybil attack can occur in a distributed system that operates without a central authority to verity the identities of each communicating entity [10].

In a Mobile Ad hoc Network, the only way for an entity to detect the presence of other entities is by sending and receiving the messages over a shared broadcast communication channel. By taking the advantage of this feature, a malicious node can send messages with multiple fake identities. The node spoofing the identities of the nodes is called malicious node/Sybil attacker, and the nodes whose identities are spoofed are called Sybil nodes. Figure 1 represents a malicious node S along with its four Sybil nodes (S_1, S_2, S_3 and S_4). If this malicious node communicates with any legitimate node by presenting all its identities, the legitimate node will have illusion that it has communicated with five different nodes. But in actual, there exists only one physical node with multiple different IDs.

2.1. Dimensions of Sybil Attack

The launching of the Sybil attack can be represented using three dimensions: Communication, Participation and Identity [10], as shown in the figure 2.

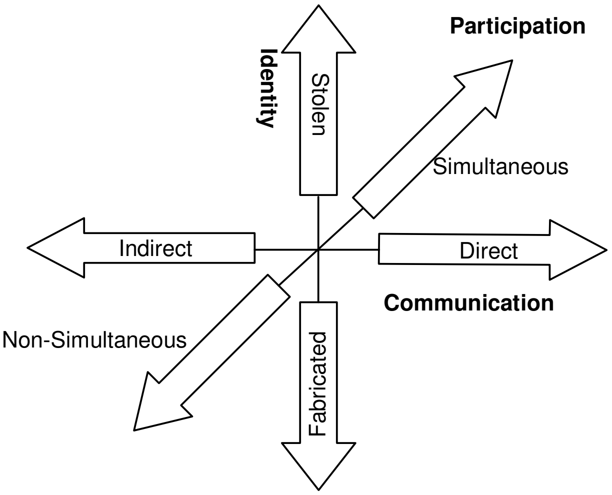

Figure 2. Three dimensions for launching the Sybil attack

2.1.1. Communication

According to Newsome et al, communication is concerned with how the Sybil nodes are introduced into the legitimate nodes in the network [10]. They state that there are two ways of communication: Direct and Indirect. In a direct communication, as the name implies, the malicious node allows its Sybil nodes to communicate directly with the legitimate nodes. Thus, the legitimate nodes will have an illusion of having these Sybil nodes as their neighbors. But in fact, the messages are being sent and received by the malicious node. In case of indirect communication, the malicious node does not allow its Sybil nodes to communicate directly with the legitimate nodes; but instead it claims to have its Sybil nodes as its neighbors that are not within the reach of the legitimate nodes. Therefore, the legitimate nodes will be using the malicious node as a router to reach these Sybil nodes. However, the authors are of the opinion that the title ‘Establishment of the Connection’ would have been more appropriate instead of the title ‘Communication’.

2.1.2. Participation

This dimension is concerned about the participation of Sybil nodes in the communication with legitimate nodes in the network. These nodes can participate simultaneously or non-simultaneously. In a simultaneous participation, the malicious node launches all the fake identities i.e. the Sybil nodes at once. On other hand, in a non-simultaneous way of launching the attack, the malicious node presents the Sybil identities one by one, after fixed or variable interval of time.

2.1.3. Identity

This dimension represents the spoofing of identities for the Sybil nodes. There are two methods by which a Sybil node can get the identity: In the first method a Sybil node can steal the identity of a legitimate node by impersonating it. The second method involves the fabrication of a fresh fake identity.

2.2. Effects of Sybil Attack in Mobile Ad Hoc Networks

If a single malicious node is able to convince its neighbours by presenting multiple identities, it will have control over the substantial portion of the network and can adversely affect the functioning of this network. Once a Sybil attack has been launched in the system, it also opens the doors for different types of other attacks. According to Newsome at. el in [10], the mechanisms that can be disrupted by the Sybil attack are:

2.2.1. Data Aggregation

A single Sybil attacker with multiple fake identities can participate in the aggregation, a number of times and can alter the result of the data aggregation

2.2.2. Fair Resource Allocation

Fair resource allocation scheme is also affected by the Sybil attack. For example some network resources may be allocated on a per node basis; in that case a malicious node can have a larger share of any resource by presenting multiple identities.

2.2.3. Voting

A Sybil attacker node is also capable of altering the result of a voting scheme. For example, in a vote based intrusion detection system, a malicious node with multiple Sybil nodes can expel a legitimate node from the network by voting against this node. Also, to win the trust of the legitimate nodes in the network, a Sybil attacker can take advantage of its multiple Sybil nodes that will vote in its favour.

2.2.4. Routing

Sybil attacks can also impact the functioning of certain routing protocols in MANETs such as geographic based routing protocols [11, 12, 13] and multi-path routing protocols [14, 15, 16, 17]. In geographic routings, the nodes exchange their location information with their neighbors, to route the packets in an efficient manner. Here, a single malicious can present multiple identities with different fake coordinate positions [9]. Thus the legitimate nodes will have false routing information in their tables and will lead to disruption in the routing process. In multi-path routing protocol, if the Sybil attacker has presented multiple Sybil nodes among the legitimate nodes, then for the legitimate sender nodes it may appear that the route request packets are being forwarded through different paths, whereas they are being actually passed through a single malicious node.

3. Lowest ID Clustering Algorithm

In the lowest ID clustering algorithm [18], a node with the lowest ID is chosen as a clusterhead. Each node is provided with a unique ID and it periodically broadcasts the list of its neighbor's IDs, including itself. A node which only hears nodes with ID higher than itself is a clusterhead (CH). The lowest ID node that a node hears is its clusterhead, unless the lowest ID specifically gives up its role as a clusterhead when a node with a lower ID enters into the same cluster. This is a simple algorithm and the process of cluster formation is very fast. Also, the rate of change of clusterhead is low and hence the system performance is better in terms of throughput. On the other hand, the number of clusters may become undesirably high due to which the packet delivery delay may become excessive. Moreover, clusterheads with smaller IDs suffer from the battery drainage, resulting in short lifetime of the system. Figure 3 shows a schematic of the result of using lowest ID clustering. There are 11 nodes with unique IDs, which form a connected graph. After the Lowest-ID clustering algorithm is executed, three clusters are formed, as depicted by the dotted circles. The black colored balls inside each cluster represent the clusterheads (1, 5 and 3 in figure 5). The striped balls (6 and 7) that are within the communication range of two or more different clusters represent the gateway nodes and the empty balls are the member nodes.

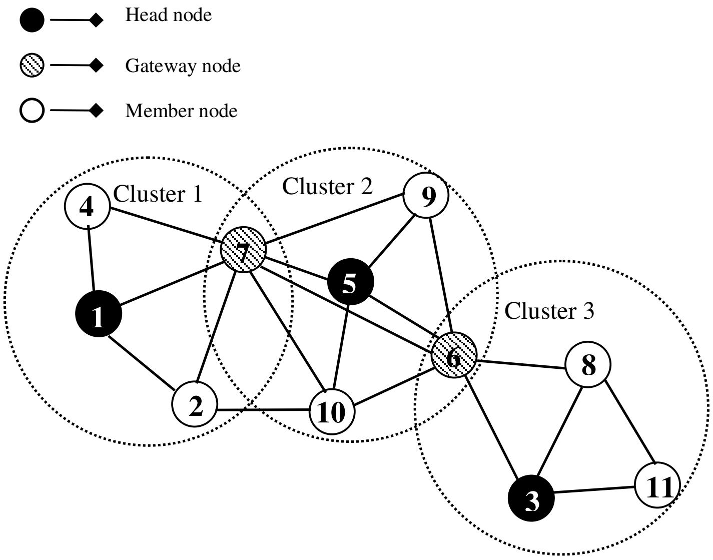

Figure 3. Cluster formation using lowest ID clustering algorithm

4. Sybil Attack in Lowest ID Clustering Algorithm

To become a cluster head, a malicious node can present the Sybil node with lowest ID in its neighborhood. For this, the malicious node will have to behave normally for the period until it has accessed the information about the whole network i.e. its one-hop, two-hop and n-hop neighbors and their respective IDs. After gaining the appropriate information, the malicious node can present its Sybil node with lowest ID to fulfill its purpose by becoming the clusterhead. The Sybil attack can also disrupt the lowest ID based cluster routing protocol by presenting multiple Sybil nodes with IDs higher than the neighboring legitimate nodes. Here the intention is to make a legitimate node with lowest ID, the clusterhead again and again to drain its battery. The clusterheads are responsible for managing resources within their own cluster as well as forwarding resource queries to clusterheads in other clusters. They are also responsible for maintaining the topological information as well as the membership information in a cluster to support route finding. Because nodes with cluster head role consume more power than ordinary nodes, mobile node with lowest ID discharges soon. Once the battery is drained completely, the malicious node can impersonate its ID for one of its Sybil node to become a clusterhead. If a number of malicious nodes are spread across all over the network, the impact of the Sybil attack will be more on this clustering scheme, as most of the clusters will be under the control of these Sybil attacker nodes. The following subsections, with the help of suitable illustrated examples, highlight how the Sybil attack can disrupt the lowest ID clustering algorithm in two different ways.

4.1. Lowest ID Based Sybil Attack for Disruption of Lowest ID Clustering

Assumptions

1. Let N be the number of nodes in a Mobile Ad Hoc Network, at any instant of time, (The number of nodes may vary in these networks due to the movement of the nodes in different directions and also due to drainage of their battery) with their IDs as

   $x_i : i = 1,2,.......,N.$

2. One of the nodes in the network, say x_m, is a malicious node.
3. It is possible for any node to send the messages by varying its transmission power [19]. Various authors [20, 21, 22, 23] have used this feature in power control schemes, to minimize the energy consumption while delivering the packets and also to increase the spatial reuse of the wireless channel. We have used a variant of Sybil attack in which a malicious node introduces its Sybil nodes by varying the transmission power.

Steps

1. The malicious node x_m will have to generate a Sybil node such that its ID is minimum in the network, i.e., if x_s is a Sybil node's identity then

   $x_s < x_i$

2. In the next step, the malicious node x_m will introduce itself and its Sybil node to the network. To achieve this, the malicious node broadcasts the Hello packet with its original ID. Let n neighboring nodes respond with their respective IDs.

3. Next time the malicious node will use its Sybil node to broadcast the Hello packet, by decreasing its transmission power. This variation in the transmission power is required to convince other nodes in the neighborhood that it is not the same malicious node. Otherwise, a Sybil attack can be detected on the basis of the following facts:

   a. Sybil nodes of a malicious node will always move together [24].
   b. Two different physical entities in the MANET cannot have the same set of the neighbors [25].
   c. The received signal strengths of the messages sent by the attacker node and its Sybil nodes will be almost the same (there can be some variation due to the movement of nodes) [26].

4. In this manner, the number of nodes that will respond to the Sybil Node will always be less than or equal to n; i.e. if n' is the number of nodes that responded to the Sybil node then

   $n' \le n$

5. During the election process, every node will broadcast its neighbor list, including itself. Since the ID of the Sybil node is the smallest in the whole network, it will always defeat the lowest ID clustering scheme by becoming the clusterhead again and again.

Here is an illustration that shall help in better understanding of the introduction of Sybil attack in the lowest ID clustering scheme. Consider a topology of the Mobile Ad Hoc network with ten nodes represented by $x_1, x_2, ...x_{10}$, as shown in the figure 4. The line shows the direct link between the nodes. Among these nodes one of the node say x_3 (represented by a black color ball) is a malicious node that has generated a Sybil node x_0 in such a way that its ID is smallest in the network. The node x_3 broadcasts the Hello messages to know its current one-hop neighbors. All the nodes within in its communication range, i.e. $\{x_1, x_2, x_4\}$ respond with their respective IDs. Immediately after sending the first Hello packet with its ID as x_3, the same malicious node again broadcasts the Hello packets, but with different ID as x_0 (Sybil node) and by decreasing its transmission power. As shown in the figure 4, after decreasing the transmission power, the Hello packets are received only by the nodes x_2 and x_4, but not by x_1.

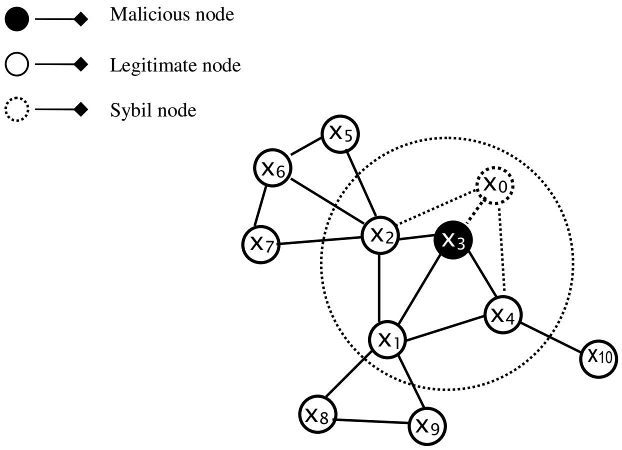

Figure 4. The topology of a MANET with 10 nodes; x3 is a malicious node

Thus, the neighbor list of the Sybil node x_0 is given as: $\{x_2, x_3, x_4\}$. But in reality, a single malicious node x_3 is responsible to maintain two different neighbor's lists: one for itself i.e. $\{x_0, x_1, x_2, x_4\}$and other for its Sybil node x_0 i.e. $\{x_2, x_3, x_4\}$.

Table 1. Neighbor list of the nodes

Node ID	Neighbors
x_0	x_2, x_3, x_4
x_1	x_2, x_3, x_4, x_8, x_9
x_2	x_0, x_1, x_3, x_5, x_6, x_7
x_3	x_0, x_1, x_2, x_4
x_4	x_0, x_1, x_3, x_{10}

According to the lowest ID algorithm, when the election process is invoked, each node will periodically broadcast the list of its neighbors, including itself, which are given in the table 1. Since the ID of the Sybil node x_0 is less than all its neighbors therefore it will become a clusterhead (figure 4). But in reality, it is the malicious node x_3 that will act as the clusterhead for the Sybil node x_0.

4.2. Impersonation Based Sybil Attack Disrupting the Lowest ID Clustering

Assumptions

1. Let N be the number of nodes in a Mobile Ad Hoc Network, at any instant of time, with their IDs as
   $x_i : i = 1,2,.......,N.$
2. One of the nodes in the network, say x_m, is a malicious node.
3. The malicious node x_m is capable of introducing its Sybil nodes by varying the transmission power.

Steps

1. After behaving normally for some time, this malicious node will gain the access to the necessary information about the network including its neighbors and their IDs.
2. In the next step the malicious node x_m generates S number of Sybil nodes that can communicate with the legitimate neighboring nodes. Let the IDs of Sybil nodes are
   $n_j : j = 1,2,.........,S$ where $S < N.$
   These IDs are chosen such that
   $n_j > n_i$
3. Now, in addition to itself, the malicious node will also include its Sybil nodes for the selection of clusterhead. Since the IDs of all the Sybil nodes is greater than the IDs of all other legitimate nodes in the networks, the legitimate node with the lowest ID will become cluster head, repeatedly. In addition, the Sybil attacker node x_m will also use its Sybil nodes to communicate again and again using its different IDs so as to keep the head node busy all the time, until its battery is drained, completely.
4. After the battery of this clusterhead node is drained completely, the malicious node can impersonate its ID and assign it to one of its Sybil nodes to make it a clusterhead.

The problem with this scheme is that the target node may move out of the range of the malicious node. Thus, it is necessary for the malicious node to move in the direction of target node. For this the malicious node can be equipped with the localization scheme to track the position of the target node. The other problem is that the battery of the malicious node will also get drained after a particular period of time, due to regular communication with the target node. Thus, a malicious node is required to be equipped with the more resources in terms of memory, battery power and processing power. As an alternative, once the battery of the malicious node has been drained to a certain threshold level, this malicious node can be substituted by another fresh malicious node. In doing so, the previous malicious node will have to transfer its complete information to the newer node before being getting disabled.

5. Detection Mechanisms of Sybil Attack

Douceur in [8] proposed a resource testing approach to defend against the Sybil attack, which is based on the assumption that each physical entity is limited in some resource. According to this approach computation, storage and communication can be used for resource testing. In [10], Newsome et al. showed that computation and storage are not suitable to ad hoc networks, because the attacker can use more computational and storage resources than the legitimate node. Instead, they suggested a scheme based on radio resource testing. This scheme assumes that each node has only one radio which is not capable of sending or receiving on more than one channel, simultaneously. If a node wants to verify the presence of Sybil nodes in its neighbors, it will assign each of its neighbors a different channel to broadcast messages. The node then randomly selects a channel to listen. If the node hears the message on the channel assigned by the verifying node, then it is a legitimate node. Otherwise, the neighboring node is treated as the Sybil node. However, how a sensor node assigns the radio channels to its neighbor nodes is an unsolved problem. In addition, this testing process may consume a lots of battery power.

Newsome et al. also proposed a random key pre-distribution and registration based key validation method [10]. In this scheme each node randomly picks $'k'$ keys from a large pool of $'m'$ keys. The number $'m'$ is chosen such that two nodes will share at least one key with some probability after they pick their keys. The identity of the node is then combined with the particular set of keys which it chooses. In this way, any node can be authenticated by verifying some or all of the keys which it claims to possess. But this method requires more memory space for storing pair wise keys with its neighbors. Moreover, if an adversary is some how able to compromise some keys, it can falsely claim the identities of many non-compromised nodes

Karlof & Wagner in [9] proposed a protocol similar to Needham-Schroeder [27] to verify the identities of two nodes. In this scheme a trusted base station acts as the Key Distribution Centre where all the nodes share their unique symmetric key. The base station then provides a shared key for each pair of nodes to verify each other's identity. This method can limit the capability of the Sybil attack but cannot locate and remove it. If an adversary succeeds in compromising a node, then it can create multiple fake identities to communicate with other nodes.

Zhang et al. in [28] introduced the concept of location-based cryptographic keys, called pairing. In this scheme, the private key of each node is combined with its ID and the geographic location. The Location-Based Keys (LBKs) are generated using pairing based on identity based cryptography by a trusted authority. The protocol also includes a secure LBK-based neighborhood authentication scheme, and methods for establishing both immediate and multi-hop pair wise shared keys. When a malicious node intends to impersonate a legitimate node, it does not have the authentic LBK and thus, cannot successfully finish mutual authentication with other legitimate nodes. Similarly, a malicious node cannot claim forged IDs and locations without being detected. Therefore, the Sybil attack is effectively defeated. This method is not suitable for large scale networks. Also, the pairing is an energy consuming method.

Bazzi et al. in [29] proposed a Sybil defense based on network coordinates in order to differentiate between nodes. The mechanism relies on the assumption that a malicious user can have only one network position, defined in terms of its minimum latency to a set of beacons. In this scheme the node that wants to authenticate itself submits a geometric certificate consisting of verified ping times to a collection of standardized beacon nodes. Multiple virtual machines located at the same physical location will end up with essentially the same certificate, and can be treated as one (possibly corrupted) node. However, with network coordinates in a d-dimensional space, an adversary controlling more than d malicious nodes at d different network positions can fabricate an arbitrary number of network coordinates, and thus break the defense. This mechanism is very complex and energy consumptive.

Demirbas and Song in [26] proposed Received Signal Strength Indicator (RSSI) based solution to detect the Sybil attack in the wireless sensor networks. It is based on the fact that a malicious node with a number of fake IDs will have the same signal strength. They showed that even though RSSI is time varying and unreliable in general and radio transmission is non-isotropic; using the ratio of RSSIs from multiple receivers it is feasible to overcome these problems. The malicious node can vary its transmission power for its Sybil node leading to different received signal strength and hence inaccurate detection of Sybil identities. This approach is not suitable for the MANETs, if the nodes move with non-uniform speeds.

Wen et. al in [30] proposed a mechanism similar to [26], based on the time difference of arrival (TDOA) between the source node and beacon nodes. This method requires at least three beacon nodes; one of them is the primary beacon node and the others are called as secondary beacon nodes. When a malicious node broadcasts a message using one of its Sybil IDs, all the beacon nodes record the arrival time of this message, respectively. The secondary beacon nodes transmit their message arrival time information to the primary beacon node. The primary beacon node then computes the ratio of the difference of arrival time of the message at the secondary beacon nodes with respect to itself. Next time, if the same malicious node broadcasts another message with a different Sybil node, the above process of computing the ratio of time difference of arrival is repeated again. If this ratio is approximately same as that of the previous ratio, the Sybil attack is detected. But, this mechanism is also not suitable for the MANETs where the nodes move in different directions, with non-uniform speeds.

Piro et al. in [24] used the mobility of nodes as a feature to detect the Sybil attack in MANETs. This mechanism is based on the fact that all the Sybil nodes of a malicious node will always move together. If a set of nodes are seen together for a long period of time by an observer node, then they are suspected to be the identities of Sybil attacker. The accuracy of the detection mechanism can be further improved by using multiple trusted observer nodes. However, this scheme fails if the malicious node continuously changes the identities of its Sybil nodes. Moreover, the trusted nodes can also be impersonated by the Sybil attacker node as discussed in the section 4.2 of this paper.

Tangpong et al. in [31] proposed a location-based Sybil attack detection scheme for MANETs based on path similarity. The identities that traverse the similar paths are considered Sybil nodes. Instead of selecting some trusted observer nodes as in [24], each node in the network observes and exchanges traffic observations in order to analyze the potential existence of a Sybil attack. Moreover, to prevent a malicious node from fabricating with an observation, a hop-by-hop authentication protocols is being used.

Ssu et al. in [25] proposed a detection scheme in which the node identities are verified simply by analyzing the neighboring node information of each node. This detection method is based on the fact that in a dense network, two different nodes cannot have the same set of neighbors. Because in a Sybil attack, all the Sybil nodes are created by the same malicious node, therefore, each of them will have same set of neighbors. This loophole of the Sybil nodes can be used to detect the presence of a Sybil attack. However, this scheme is not suitable for mobile or semi mobile Ad hoc networks.

6. CONCLUSION AND FUTURE WORK

In this paper we have discussed the Sybil attack in context of how it can disrupt the head selection mechanism of the lowest ID based clustering scheme for routing in MANETs. The Sybil attack has been illustrated through two different ways: lowest ID Based Sybil Attack and

Impersonation based Sybil Attack. In lowest ID based Sybil attack, a malicious node can become clusterhead by presenting a Sybil node with lowest ID. The attack becomes more devastating and difficult to be detected if the malicious node presents its fake identities by varying the transmission power. It takes the advantage of varying the transmission power in two ways: First, it cannot be detected on the basis of same signal strengths of its Sybil nodes. Second, by decreasing the transmission power for different Sybil nodes, the message will not reach all the neighbors of the malicious node and hence cannot be detected on the basis of the fact that if a set of nodes are seen together for a long period of time by an observer node, then they are suspected to be the identities of Sybil attacker. In an impersonation based Sybil attack, a malicious can also disrupt the lowest ID based cluster algorithm by presenting multiple Sybil nodes with IDs greater than its neighboring legitimate nodes. It will target a legitimate node with lowest ID to make it clusterhead again and again, so as to drain its battery. It also utilizes its multiple Sybil nodes to communicate repeatedly with the clusterhead so as to make it busy all the time. After completely draining the battery of head node, the malicious node can impersonate its ID for one of its Sybil node to become the clusterhead. If a number of malicious nodes are spread across all over the network, the impact of the Sybil attack will be more on this clustering scheme, as most of the clusters will be under the control of these Sybil attacker nodes.

In this paper we investigated two ways by which a Sybil attack can disrupt the head selection mechanism of lowest ID clustering scheme. One of the objectives of this study is to have a better understanding of challenges offered by the Sybil attack on this routing protocol. Presently we are in the process of designing an appropriate Sybil attack detection mechanism. The credibility and efficiency of this mechanism will be tested for the various forms of Sybil attack, using the network simulator.

REFERENCES

[1] C. -K. Toh, (2002), “Ad Hoc Mobile Wireless Networks: Protocols and Systems”, *Prentice Hall PTR.*

[2] E. M. Royer and C. -K. Toh, (1999), “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks,” *IEEE Personal Communications.*

[3] L. Buttyan and J. P. Hubaux, (2002), “Report on a working session on security in wireless ad hoc networks”, *Mobile Computing and Communications Review.*

[4] M. Al-Shurman, S. -M. Yoo, and S. Park, (2004), “Black Hole Attack in Mobile Ad-Hoc Networks”, *ACM Southeast Regional Conf*erence.

[5] Y. C. Hu, A. Perrig and D. B. Johnson, (2003), “Rushing Attacks and Defense in Wireless Ad Hoc Networks Routing Protocol”, *In Proceedings of ACM WiSe2003.*

[6] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, (2002), “An On-demand Secure Routing Protocol Resilient to Byzantine Failures”, *Proceedings of the ACM Workshop on Wireless Security*, pp. 21-30.

[7] Y. Hu, A. Perrig and D. Johnson, (2002), “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, *Proc. of IEEE Infocom.*

[8] J. R Douceur, (2002), “The Sybil Attack”, *IPTPS ’01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pp. 251–260, Springer Verlag, London, UK.

[9] C. Karlof and D. Wagner, (2003), “Secure routing in wireless sensor networks: Attacks and Countermeasures”, *Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols,* Vol. 1, No. 2-3, pp. 293-315.

[10] J. Newsome, E. Shi, D. Song and A. Perrig, (2004), “The Sybil Attack in Sensor Networks: Analysis & Defenses”, IPSN ’04. *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp. 259–268, ACM, Berkeley, California, USA.

[11] S. Basagni, I. Chlmtac, V. R. Syrotiuk and B. A. Woodward, (1998), “A Distance Routing Effect Algorithm for Mobility (DREAM)”, *In Proceedings of IEEE/ACM MobiCom*, pages 76-84.

[12] B. Karp and H. T. Kung, (2000), “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”, *In Proceedings of IEEE/ACM MobiCom*, pages 243-254.

[13] Y. Ko and N. H. Vaidya, (1998), “Location-Aided Routing (LAR) in Mobile Ad Hoc Networks”, *In Proceedings of IEEE/ACM MobiCom*, pages 66-75.

[14] J. J. Garcia-Luna-Aceves, and E. L Mada-uga, (1999), “The core assisted mesh protocol”, *IEEE JSAC*, Vol 17, No. 8, pp. 1380-1394.

[15] S. -J. Lee, M. Gerla and C. C. Chiang, (1999), “On-demand multicast routing protocol (ODMRP)”, *Proceedings of IEEE WCN’99.*

[16] E. M. Royer and C. E. Perkins, (1999), “Multicast Operation of Ad Hoc On Demand Distance Vector Routing Protocol”, *In Proceedings of ACM MOBICOM*, pp. 207-18.

[17] S. -J. Lee and M. Gerla, (2001), “Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks”, *In Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 3201-3205, Helsinki, Finland.

[18] J. Zhao and R. Govindan, (2003), “Understanding Packet Delivery Performance in Dense Wireless Sensor Networks”, *In Proc. ACM Sensys.*

[19] S. Agarwal, S. Krishnamurthy, R. H. Katz and S. K. Dao, (2001), “Distributed Power Control in Ad-hoc Wireless Networks”, *In Proc. PIMRC01.*

[20] M. Krunz, A. Muqattash and S-J. Lee, (2004), “Transmission Power Control in Wireless Ad-hoc Networks: Challenges, Solutions, and Open Issues”, *.IEEE Network*, 18:8–14.

[21] J. -P. Ebert, B. Stremmel, E. Wiederhold and A. Wolisz, (2000), “An Energy-efficient Power Control Approach for WLANs”, *Journal of Communications and Networks (JCN),* 2(3):197-206.

[22] J. -P. Ebert and A. Wolisz, (1999), “Combined Tuning of RF Power and Medium Access Control for WLANs”, *In IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99).*

[23] J. Gomez, A. T. Campbell, M. Naghshineh and C. Bisdikian, (2001), “Conserving Transmission Power in Wireless Ad Hoc Networks”, *In Proc. 9th International Conference on Network Protocols (ICNP 2001)*, Riverside, California.

[24] C. Piro, C. Shields, B. N. Levine, (2006), “Detecting the Sybil Attack in Mobile Ad-hoc Networks”, *Securecomm and Workshops*, pp 1-11.

[25] K. -F. Ssu, W-T. Wang and W-C. Chang, (2009), “Detecting Sybil attacks in Wireless Sensor Networks using Neighboring Information”, *Computer Networks*, vol. 53, (18), pp.3042-3056.

[26] M. Demirbas and Y. W. Song, (2006), “An RSSI-Based Scheme for Sybil Attack Detection in Wireless Sensor Networks”, *International Workshop on Wireless Mobile Multimedia (WOWMOM’06)*, New York, USA., pp. 564–570.

[27] R. Needham and M. Schroeder, (1978), “Using Encryption for Authentication in Large Networks of Computers”, *Communications of ACM.*

[28] Y. C. Zhang, W. Liu, W. J. Lou and Y. G. Fang, (2006), “Location based compromise-tolerant security mechanisms for wireless sensor networks”, *IEEE Journal on Selected Areas in Communications*, 24(2): pp. 247–260.

[29] Rida A. Bazzi, Young-ri Choi and Mohamed G. Gouda, (2009), “Hop chains: Secure routing and the establishment of distinct identities”, *Theoretical Computer Science*, 410 (6-7): 467-480.

[30] M. Wen, H. Li, Y-F. Zheng and K-F. Chen, (2008), “TDOA-Based Sybil Attack Detection Scheme for Wireless Sensor Networks”, *Journal of Shanghai University (English Edition)*, Vol. 12, No. 1, pp. 66-70.

[31] A. Tangpong, G. Kesidis, H-Y. Hsu and A. Hurson, (2009), “Robust Sybil Detection for MANETs”, *In Proceedings of the 18th International Conference on Computer Communications and Networks, IEEE ICCCN 2009*, San Francisco, California.

Authors

Mr. Amol Vasudeva received his Master of Computer Application from IGNOU in 2001 and Master of Technology in Computer Science from Jaypee University of Information Technology, Waknaghat in 2009. He is pursuing his Ph.D. in Computer Science from Himachal Pradesh University, Shimla, Himachal Pradesh, India. He is currently working as Senior Lecturer, in the Department of Computer Science & Engineering and Information Technology, at Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh, India. He has been associated with this department for the last 7 years. His areas of research include Parallel Computing, Security and Localization in MANETs and Sensor Networks.

Dr. Manu Sood received his Bachelor of Engineering degree in Electronics and Telecommunications from Rani Durgawati University in Jabalpur, Madhya Pradesh, India, Master of Technology in Information Systems and Ph.D. form Delhi University, Delhi, India. At present, he is working as a Professor in the Department of Computer Science, H.P University, Shimla, Himachal Pradesh, India. He has been associated with this department for the last 19 years and had been the Chairperson of this department for one complete term. He a life time member of Computer Society of India. He has been associated with many on-campus and off-campus computerization activities. He has been the member of technical program committees of various international conferences. His areas of research include requirements engineering, software engineering, SOA, Cloud Computing, e-learning, and MANETs.