Perspectives of Sybil Attack in Routing Protocols of Mobile Ad Hoc Network

Manu Sood and Amol Vasudeva

Abstract It is cumbersome to achieve the security in a mobile ad hoc network due to 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. Two routing mechanisms 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 various cluster-based routing protocols such as lowest id, highest node degree and mobility based clustering. 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 MANETs.

Keywords Mobile ad hoc network · Sybil attack · Malicious node · Sybil node · Network security · Routing protocol

1 Introduction

Security is an important concern in the Mobile Ad hoc Networks (MANETs). However, the characteristics of MANETs pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity,

M. Sood
Department of Computer Science, Himachal Pradesh University,
Shimla, Himachal Pradesh, India

A. Vasudeva (✉)
Department of Computer Science and Engineering and Information Technology,
Jaypee University of Information Technology, Waknaghat,
Solan, Himachal Pradesh, India
e-mail: amol_dev@rediffmail.com

N. Chaki et al. (eds.), *Computer Networks & Communications (NetCom)*,
Lecture Notes in Electrical Engineering 131, DOI: 10.1007/978-1-4614-6154-8_1,

availability, access control and non-repudiation [1]. 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 [2], Rushing [3], wormhole [4] and Sybil attack [5] etc. A Sybil attack is an attack [5], 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 and Wagner have shown in [6] that multi-path routing and geographical routing schemes are affected by this attack. In case of multi-path routing a set of supposedly disjoint paths can all be passing through the same malicious node, which is using several Sybil identities. Also 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 various cluster-based routing protocols such as lowest ID [7], highest node degree [8] and mobility based clustering [9]. To the best of our knowledge, this is for the first time that the impact of Sybil attack has been shown in these cluster based routing algorithms. The rest of this paper is organized as follows. Section 2 describes the Sybil attack in details. Section 3 describes the following routing protocols: Split Multi-path Routing (SMR) [10], Greedy Perimeter Stateless Routing (GPSR) [11] and various cluster based routing protocols along with the effect of Sybil attack on these protocols, respectively. Finally, the Sect. 4 concludes the paper.

2 Sybil Attack

Sybil attack was first introduced by J. R. Douceur. According to Douceur, the Sybil attack is an attack by which a single entity can control a substantial fraction of the system by presenting multiple identities [5]. The Sybil attack can occur in a distributed system that operates without a central authority to verity the identities of each communicating entity [12].

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. If a single malicious node is able to

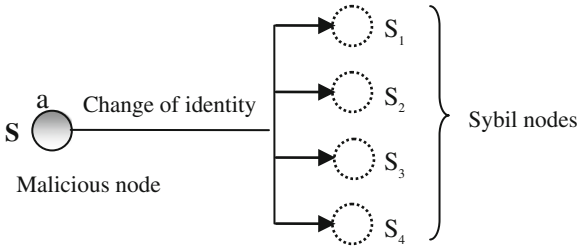

Fig. 1 A Sybil attacker with multiple IDs

convince its neighbors by presenting multiple identities, it will have control over the substantial portion of the network and can adversely affect the functioning of the network. According to Newsome [12], the mechanisms that are affected by the Sybil attack are: Data Aggregation, Fair Resource Allocation, Voting and Misbehavior Detection etc. Karlof and Wagner have shown in [6] that Sybil attack can also disrupt the functioning of certain routing protocols in MANETs such as multi-path routing protocols [10, 13, 14] and geographic based routing protocols [11, 15, 16].

The launching of the Sybil attack can be represented using three dimensions: Communication, Participation and Identity [12]. Newsome et al. state that there are two ways of communication: Direct and Indirect [12]. In a direct communication, as the name implies, the malicious node allows its Sybil nodes to communicate directly with the legitimate nodes. In case of indirect communication, the malicious node does not allow its Sybil nodes to communicate directly with the legitimate 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'. Participation 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. 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.

3 Sybil Attack in MANET Routing Protocols

In this section, we have illustrated the impact of Sybil attack on Split Multi-path Routing (SMR) and Greedy Perimeter Stateless Routing (GPSR). In addition to these routing protocols, we have shown that the Sybil attack can also disrupt the different forms of Cluster Based Routing Protocols such as Lowest ID Clustering, Highest Node Degree Clustering and Mobility based Clustering.

3.1 Sybil Attack in Split Multi-Path Routing (SMR)

Split Multi-path Routing (SMR) [10], one of the multi-path routing protocols based on Dynamic Source Routing (DSR) [17], establishes and utilizes multiple maximally disjoint paths. Unlike DSR, the intermediate nodes in SMR do not respond to route requests, in order to obtain maximal node disjoint paths. Intermediate nodes forward the first RREQ they receive and instead of dropping all the duplicate RREQ packets, rebroadcast those duplicate packets that are being received through a different incoming link and whose hop count is not greater than the previously received RREQs. When the destination node receives the first RREQ, it responds with RREP to the source node and then waits for certain duration of time, to receive additional requests. The destination node then selects the route that is maximally disjoint to the route that is already replied. Consider Fig. 2a, where the source node S floods the RREQ packets to find an optimal route to the destination node D. The intermediate nodes forward the duplicate RREQ packets that traversed through a different incoming link than the link from which the first RREQ is received, and whose hop count is not greater than that of the first received RREQ. Now assume that a Sybil attacker node M has established itself in the network with two fake IDs i.e. X and Y. Thus, in this case the packets are being forwarded through a single physical node i.e. M. When

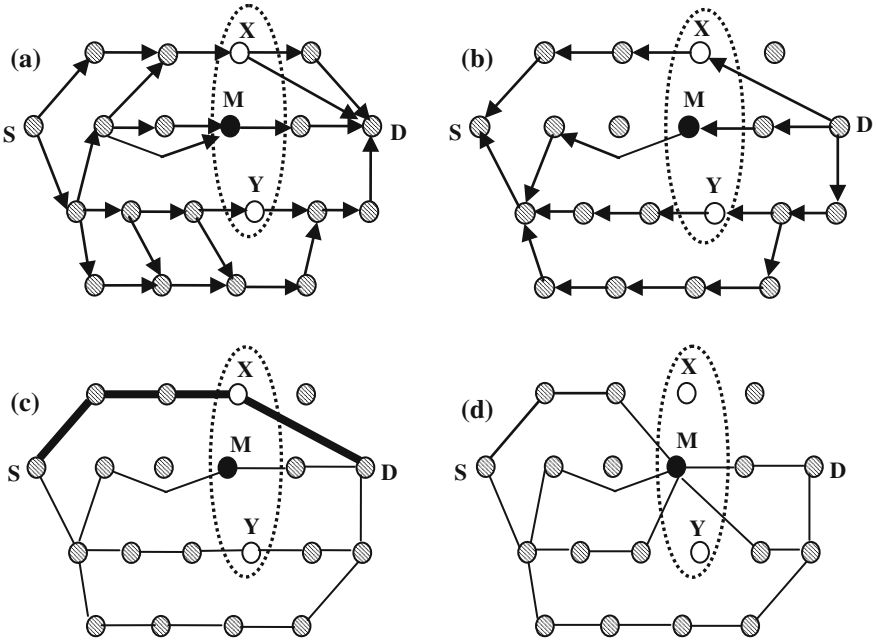

Fig. 2 **a** Flooding of RREQ packet from S to D. **b** RREP packets from D to S. **c** Selections of multiple disjoint paths. **d** Routes passing through the same node M. **S**-Source Node, **D**-Destination Node, **M**-Malicious Node, **X**, **Y**-Sybil Nodes

the RREQ packets have started to arrive at the destination node, it starts to send the RREP packets back towards the source node (Fig. 2b).
The path followed by each RREP packets is same as that of their corresponding RREQ packets. After receiving all the RREP packets the source node S makes the entry in its routing table. It then chooses the route with minimum hop count of 4 as shown in Fig. 2c by a thick line. But in reality, three routes are being passed through the same malicious node M and the Fig. 2d depicts that the routing mechanism has been disrupted, effectively.

3.2 Sybil Attack in GPSR Routing

The Greedy Perimeter Stateless Routing (GPSR) algorithm [11] works in two modes: greedy forwarding and perimeter forwarding. The algorithm starts forwarding with the greedy mode, by default. In greedy forwarding the source node looks for its neighbor that is closest to the destination and forwards the packet to that node. This process is repeated for the next node also and so on. Consider a MANET topology with 11 nodes as shown in the Fig. 3. Assume that the node C is a malicious node or Sybil attacker who somehow has succeeded to enter into the network. The actual position of this node is (7, 9). This node has presented two fake IDs i.e. the Sybil nodes D, E with their locations as (4, 11) and (11, 8), respectively. The node communicates with the other neighbors in its region by providing all the three locations (one actual and two fake). Thus, an adversary may claim to be present at more than one location for its neighbors by sending multiple HELLO messages, each time with different location information. Now suppose that the node A wants to send the packet to the destination I and to find the route it follows the greedy forwarding. A's radio range is denoted by the dotted circle about A and the arc with the radius equal to the distance between A and I is shown as arc about I. The node A forwards the packet to the Sybil node E, as it finds that the distance between E and I is less than between E and any of the A's other neighbors, according to the location information available in its Table 1. But in fact, node A has forwarded the packet to node C whose location is (7, 9) having a distance greater than the distance from node D (8, 2). Therefore, the routing scheme has been disrupted in the MANET with the entry of Sybil attacker.

3.3 Sybil Attack in Cluster-Based Routing Protocols

A Sybil attacker can also send the messages by varying its transmission power for all of its identities. The advantage of varying the transmission power for all the Sybil nodes is that the received signal strength at the receiving node with respect to these Sybil nodes will also be different. We have used the feature of variable transmission power to show that the Sybil attack can also disrupt various cluster based routing schemes such as lowest ID, highest node degree and mobility based clustering.

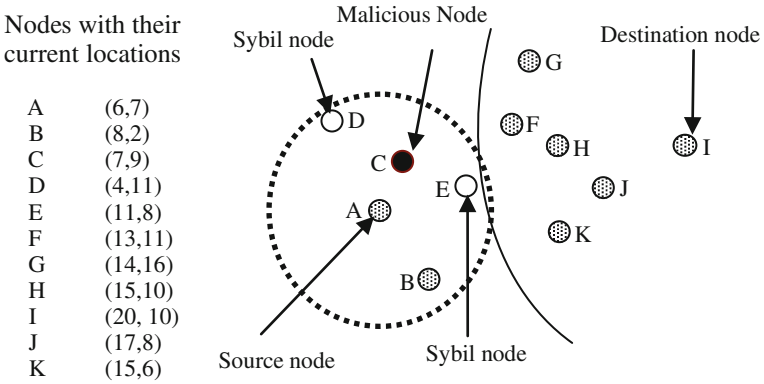

Fig. 3 A MANET topology with 11 nodes

Table 1 Location information of A's one hop neighbors

Neighbors of the source node A	Locations of A's neighbors	Distance of A's neighbors from the destination node I [10, 20]
B	(08, 02)	14.42
C	(07, 09)	13.04
D	(04, 11)	16.03
E	(11, 08)	09.22

Sybil Attack in Lowest ID Clustering Algorithm. In lowest ID algorithm [7], a node with the minimum 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).

Figure 4a 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 Fig. 4). 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.

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 introduce its Sybil node with lowest ID, to fulfill its purpose by becoming the clusterhead. The attack becomes more devastating and difficult to be detected if the malicious node introduces its fake identities (Sybil nodes) 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

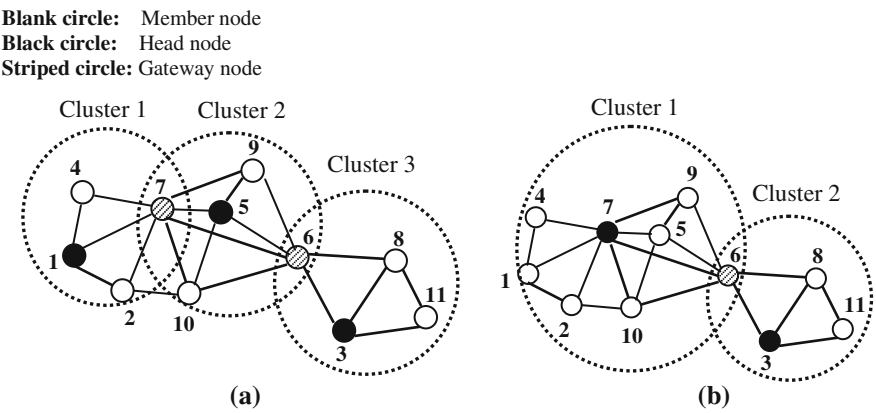

Fig. 4 Cluster formation process. **a** Lowest ID approach. **b** Highest node degree approach

of same signal strengths of its Sybil nodes [18]. Second, by decreasing the transmission power for different Sybil nodes, the message will not reach all the legitimate neighbors of the malicious node and hence cannot be detected on the basis of the fact that two different physical entities cannot have the same set of neighbors [19].

The Sybil attack can also disrupt the lowest ID based cluster routing by presenting multiple Sybil nodes with IDs higher than its neighboring legitimate nodes. Here the intention is to make the legitimate node with lowest ID, the clusterhead again and again to drain its battery. Once the battery is drained completely, the malicious node can impersonate its ID for one of its Sybil node to become a clusterhead.

Sybil Attack in Highest Node Degree Algorithm. In highest node degree algorithm [8], the degree of a node is computed on the basis of its neighbors. The node having maximum number of neighbors is elected as the clusterhead. If there is a tie between two or more nodes in terms of node degree, the node with lowest ID is chosen to be clusterhead. Figure 4b shows the result of using highest degree clustering for the same topology that was being used for the lowest ID algorithm.

The highest degree algorithm can also be disrupted by the Sybil attack. By presenting multiple Sybil nodes, a malicious node may claim to have more neighbors than the actual number. For example, in the Fig. 5, the node 5 is a malicious node with nodes 3, 4 and 6 as its one hop neighbors (hence node degree 3). The node 4 has the maximum node degree of 5 among its neighbors and should to be selected as a cluster head. But, the malicious node 5 also includes its three Sybil node, i.e. S_1, S_2 and S_3 so as to increase its node degree to 6 and hence becomes the clusterhead. Now the question is how to introduce these Sybil nodes to the legitimate neighboring nodes, i.e. with direct communication or indirect communication.

If indirect method of communication is followed, the malicious node will claim to have the specified number of Sybil identities as its neighbors and will not allow them to communicate directly with its legitimate neighboring nodes. But, due to mobile

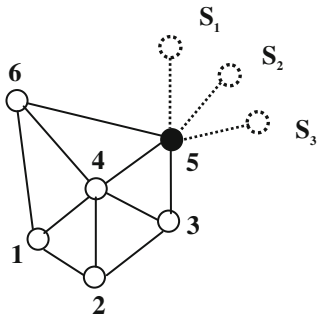

Fig. 5 A MANET topology with 6 nodes

nature of the MANET, it is not possible for these Sybil nodes to be in the transmission range of only a single node for the whole life of this MANET. If this trick is used by the malicious node repeatedly, the Sybil attack can be detected on suspicion of not communicating directly with the other legitimate nodes in the network for a long time. Also, the Sybil attack can be detected on the basis of movement of same set of nodes, by the observer nodes [20].

Therefore, to win the trust of legitimate neighboring nodes, a malicious node should allow its Sybil nodes to communicate directly with these legitimate neighboring nodes. But the problem in a direct communication is that the node degree of legitimate neighboring nodes will also increase by the same factor as that of the malicious node. For example, in Fig. 5, if a malicious node 5 allows its 3 Sybil nodes to communicate directly with its neighboring nodes, its own node degree becomes $(3+3) = 6$. But this will also lead to increase in the node degrees of its neighboring nodes 3, 4 and 6 by the same factor, i.e. 3. As a result the nodes degree of the node 4 becomes $(5 + 3) = 8$, and should be selected as the cluster head according to the algorithm.

A better option is to allow all the Sybil nodes to communicate directly with the neighboring nodes, by decreasing their transmission powers. After decreasing the transmission power, hello packets sent by the Sybil node will reach only to a subset of neighboring nodes that are closer to the malicious node. As a result, there will be increase in the node degree of this particular subset of neighbors of the malicious node, only. Before the inclusion of Sybil nodes, if the node degree of each node in this subset was less than the node degree of malicious node, the malicious node will become a clusterhead. Otherwise, one of the legitimate nodes present in that subset may become a clusterhead. Therefore, the probability of a malicious node to become a clusterhead is less in this scheme.

In order to increase the chances of becoming a clusterhead, the malicious node may claim to have some additional Sybil nodes by communicating them, indirectly. Therefore, in this scheme the Sybil nodes are kept in two different pools: one pool of

Sybil nodes for direct communication and the other pool of Sybil nodes for indirect communication. The malicious node will also keep on exchanging the Sybil nodes of these pools continuously, which makes the detection of Sybil attack very difficult.

Sybil Attack in Mobility based Clustering. Basu et al. in [9] have proposed an algorithm for the mobility based clustering (MOBIC) approach in MANETs. This algorithm uses mobility of the nodes as a feature to form the clusters. Each node in the Mobile Ad hoc Network computes the ratio of two successive "Hello" messages from all its neighbors. This gives the relative mobility metric of the nodes with respect to each of their respective neighbors. Then, by calculating the variance of relative mobility values of all the nodes with respect to their neighbors, the aggregate speed of all the mobile nodes can be estimated. Finally, the mobile node with lowest variance value in its neighborhood is elected as the clusterhead.

This algorithm can also be affected by the Sybil attack. For example, consider that we have to find the aggregate mobility of a node 4 with respect to its neighboring nodes 1, 2, 3, 5 and 6 as shown in the Fig. 5. Let the node 5 be a malicious node with three Sybil nodes S_1, S_2 and S_3. Therefore, in addition to itself the malicious node will also use its different Sybil nodes to send consecutive Hello messages, by varying its transmission power. The variation in the transmission power will be adjusted in such a manner that the second received signal strength at the legitimate receiving nodes is comparatively less than the first one. After computing the relative mobility values of all the neighboring nodes (legitimate nodes and Sybil nodes), the aggregated mobility of the node 4 is calculated by taking the variance of relative mobility values of all its neighboring nodes. The contribution of the Sybil nodes is only to increase the variance of the node 4, which is the measure of aggregated relative mobility. That is, greater the variance of a node, lesser is the chance for that node to become the clusterhead. The same process will be repeated for other legitimate nodes in the neighbor of the malicious node. Thus, the probability that the malicious node will become a clusterhead, will increase in this manner.

4 Conclusion and Future Work

In this paper, we have highlighted the impact of the Sybil attack on different routing schemes in the MANETs, such as multi-path routing, location based routing and cluster based routing. We have shown that a Sybil attack can disrupt the head selection mechanism of various cluster-based routing protocols, such as lowest ID, highest node degree and mobility based clustering. In the lowest ID clustering algorithm, a malicious node can present a Sybil node with lowest ID in its neighborhood to become the clusterhead. The attack becomes very difficult to detect and more destructive if the malicious node introduces its fake identities (Sybil nodes) by varying the transmission power. In the highest degree clustering algorithm, a malicious node may claim to have more number of neighbors by presenting multiple Sybil nodes. To achieve this, a malicious node keeps its Sybil nodes in two different pools. The Sybil nodes in

the first pool are allowed to communicate directly with the neighboring nodes, by decreasing their transmission powers. As a result, the hello packets sent by these Sybil nodes will not be received by all the neighbors of the malicious node. Therefore, there will be increase in the node degree to only a subset of neighbors that are closer to the malicious node. Prior to introduction of the Sybil nodes, if the node degree on any legitimate node in this subset was greater or equal to the node degree of the malicious node, then the chances for this malicious node to become a clusterhead are very low. Therefore, to increase the chances, this malicious node may claim to have some additional Sybil nodes by introducing them, indirectly. To disrupt the mobility based clustering scheme such as MOBIC, a malicious node uses its different Sybil node to send consecutive Hello messages, by varying its transmission power. The variation in the transmission power is adjusted in such a manner that the second received signal strength at the legitimate receiving nodes is comparatively less than the first one. Therefore, the malicious node along with its Sybil nodes will contribute in increasing the variance of its legitimate neighboring nodes, which decreases their probability to become a clusterhead. 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. Wu B, Chen J, Wu J, Cardei M (2006) A survey on attacks and countermeasures in mobile ad hoc networks. In: Xiao Y, Shen X, Du D-Z (eds) Wireless/mobile network security. Springer, New York, pp 103–135
2. Al-Shurman M, Yoo S-M, Park S (2004) Black hole attack in mobile ad-hoc networks. In: ACM Southeast Regional conference
3. Hu YC, Perrig A, Johnson DB (2003) Rushing attacks and defense in wireless ad hoc networks routing protocol. In: Proceedings of ACM WiSe2003
4. Hu Y, Perrig A, Johnson D (2002) Packet leashes: a defense against wormhole attacks in wireless ad hoc networks. In: Proceeding of IEEE INFORCOM
5. Douceur JR (2002) The Sybil attack. IPTPS '01: revised papers from the first international workshop on peer-to-peer systems. Springer Verlag, London, UK, pp 251–260
6. Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: attacks and countermeasures. Elsevier's Ad Hoc Netw J Special Issue Sens Netw Appl Protoc 1(2–3):293–315
7. Ephremides A, Wieselthier JE, Baker DJ (1987) A design concept for reliable mobile radio networks with frequency hopping signaling. Proc IEEE 75(1):56–73
8. Gerla M, Tsai JTC (1995) Multicluster, mobile, multimedia radio network. ACM/Baltzer Wirel Netw J 1:255–265
9. Basu P, Khan N, Little T (2001) A mobility based metric for clustering in mobile ad hoc networks. In: Proceedings of the 21st international conference on distributed computing systems workshops (ICDCSW '01), pp 413–418
10. Lee S-J, Gerla M (2001) Split multipath routing with maximally disjoint paths in ad hoc networks. In: Proceedings of the IEEE international conference on communications (ICC). Helsinki, Finland, pp 3201–3205, June 2001

11. Karp B, Kung HT (2000) GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of IEEE/ACM MobiCom, pp 243–254
12. Newsome J, Shi E, Song D, Perrig A (2004) The Sybil attack in sensor networks: analysis and defenses. In: Proceedings of the 3rd international symposium on information processing in sensor networks (IPSN '04), ACM, Berkeley, California, USA, pp 259–268
13. Lee S-J, Gerla M, Chiang CC (1999) On-demand multicast routing protocol (ODMRP). In: Proceedings of IEEE WCN'99, Sep 1999
14. Royer EM, Perkins CE (1999) Multicast operation of ad hoc on-demand distance vector routing protocol. In: Proceedings of ACM MOBICOM, pp 207–18, August 1999
15. Basagni S, Chlmtac I, Syrotiuk VR, Woodward BA (1998) A distance routing effect algorithm for mobility (DREAM). In: Proceedings of IEEE/ACM MobiCom, pp 76–84
16. Ko Y, Vaidya NH (1998) Location-aided routing (LAR) in mobile ad hoc networks. In: Proceedings of IEEE/ACM MobiCom, pp 66–75
17. Johnson DB, Maltz DA (1996) Dynamic source routing in ad hoc wireless networks. In: Imielinski T, Korth H (eds) Mobile computing. Kulwer Academic Publishers, Boston, pp 153–181
18. Demirbas M, Song YW (2006) An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In: International workshop on wireless mobile multimedia. New York, USA, pp 564–570
19. Ssu K-F, Wang W-T, Chang W-C (2009) Detecting Sybil attacks in wireless sensor networks using neighboring information. Comput Netw 53(18):3042–3056
20. Piro C, Shields C, Levine BN (2006) Detecting the Sybil attack in mobile ad hoc networks. In: Securecomm and workshops