ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Identifying and Preventing Sybil Attacks in Wireless Networks Using RSSI Value

Vinayaka AP, Nalinakshi B G

M. Tech II year scholar (CNE), Dept of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

Assistant Professor, Dept of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

ABSTRACT: Wireless networks are vulnerable to Sybil attacks, in which a malicious node poses as many identities in order to gain disproportionate influence. Many defences based on spatial variability of wireless channels exist, but depend either on detailed, multi-tap channel estimation—something not exposed on commodity 802.11 devices—or valid RSSI observations from multiple trusted sources, e.g., corporate access points—something not directly available in ad hoc and delay-tolerant networks with potentially malicious neighbours. We extend these techniques to be practical for wireless ad hoc networks of commodity 802.11 devices. Specifically, we propose two efficient methods for separating the valid RSSI observations of behaving nodes from those falsified by malicious participants. Further, we note that prior signalprint methods are easily defeated by mobile attackers and develop an appropriate challenge-response defense. Finally, we try implementing the Mason test concepts, the first implementation of these techniques for ad hoc and delay-tolerant networks of commodity 802.11 devices. We illustrate its performance in several real-world scenarios.

KEYWORDS: Wireless networks, Manets, Sybil attacks, RSSI value, Network vulnerability, Identity stealing

I. INTRODUCTION

A wireless networks is a way to establish communication among nodes without having hurdles of wires. Wireless networks may be implemented in various manners like mobile ad-hoc networks (MANET), vehicular ad-hoc networks (VANET), wire-less sensor networks etc. mobile ad-hoc network is collection of various wireless mobile nodes connected by wireless links. It is an autonomous system which does not require any pre-existing infrastructure and establish for temporary purpose. Ad-hoc is a Latin word which stands “for this” also known as IEEE 802.11 standard. It is a new technology emerged for fast, in ex-pensive network establishment without having burden of other devices like hub, switches or router. Here, devices are itself capable to behave as node or router to discover a route and forward packets. In MANET, each mobile node has communication range depend upon transmission power, antenna gain and loss along with antenna height. Communication in the net-works depends upon the connection among nodes using wireless links. A node can communicate to another node either through direct link connection or passing through multi-hop-routing nodes. It always depends upon radio range of node and connectivity among same.

Proposed defences (see Levine et al. for a survey fall into two categories. Trusted certification methods [7], [8] use a central authority to vet potential participants and thus are not useful in open ad hoc (and delay-tolerant) networks. Resource testing methods [9], [10], [11], [12] verify the resources (e.g., computing capability, storage capacity, real-world social relationships, etc.) of each physical entity. Most are easily defeated in ad hoc networks of resource-limited mobile devices by attackers with access to greater resources, e.g., workstations or data centres.

II. RELATED WORK

Many Sybil defence techniques are built on resource testing of wireless channels, because placing transmitters in many locations is much more difficult than acquiring additional computation or memory resources. Xiao et al. observe that in OFDM-based 802.11 channels, the coherence bandwidth is much smaller than the system bandwidth and thus the channel response estimates at wellspaced frequency taps are uncorrelated, forming a vector unique to the transmitter location and robust to changes in transmitter power [15]. Li et al. use the unique mapping between identity and wireless channel to develop a channel-based authentication scheme, using both pulse-type probing

DOI: 10.15680/IJIRCCE.2016. 0404184

in the time domain and multi-tone probing in the frequency domain for channel estimation. Although not originally designed for Sybil defence, applying this technique to detect multiple identities sharing the same channel is straightforward. A primary drawback of this class of work is its restriction to specialized hardware or firmware, as commodity 802.11 devices do not expose detailed channel information to the driver and operating system. Faria and Cheriton and Demirbas and Song independently developed the signalprint technique, which greatly simplifies channel estimations while maintaining high Sybil detection performance [16]. Instead of measuring probe responses, a vector of RSSIs reported by multiple receivers at different locations is used to characterize the sender's unique location and wireless environment. This class of work [16] has two disadvantages. First it relies on trusted external measurements, e.g., RSSIs from trusted 802.11 access points, which are generally unavailable in open ad hoc networks. Our work builds on their ideas, but does not rely on any particular external device being trustworthy. Second, it restricts the attack model to stationary devices, even though attackers can easily use mobile devices. Our work detects and rejects moving nodes, instead of accepting them as non-Sybil.

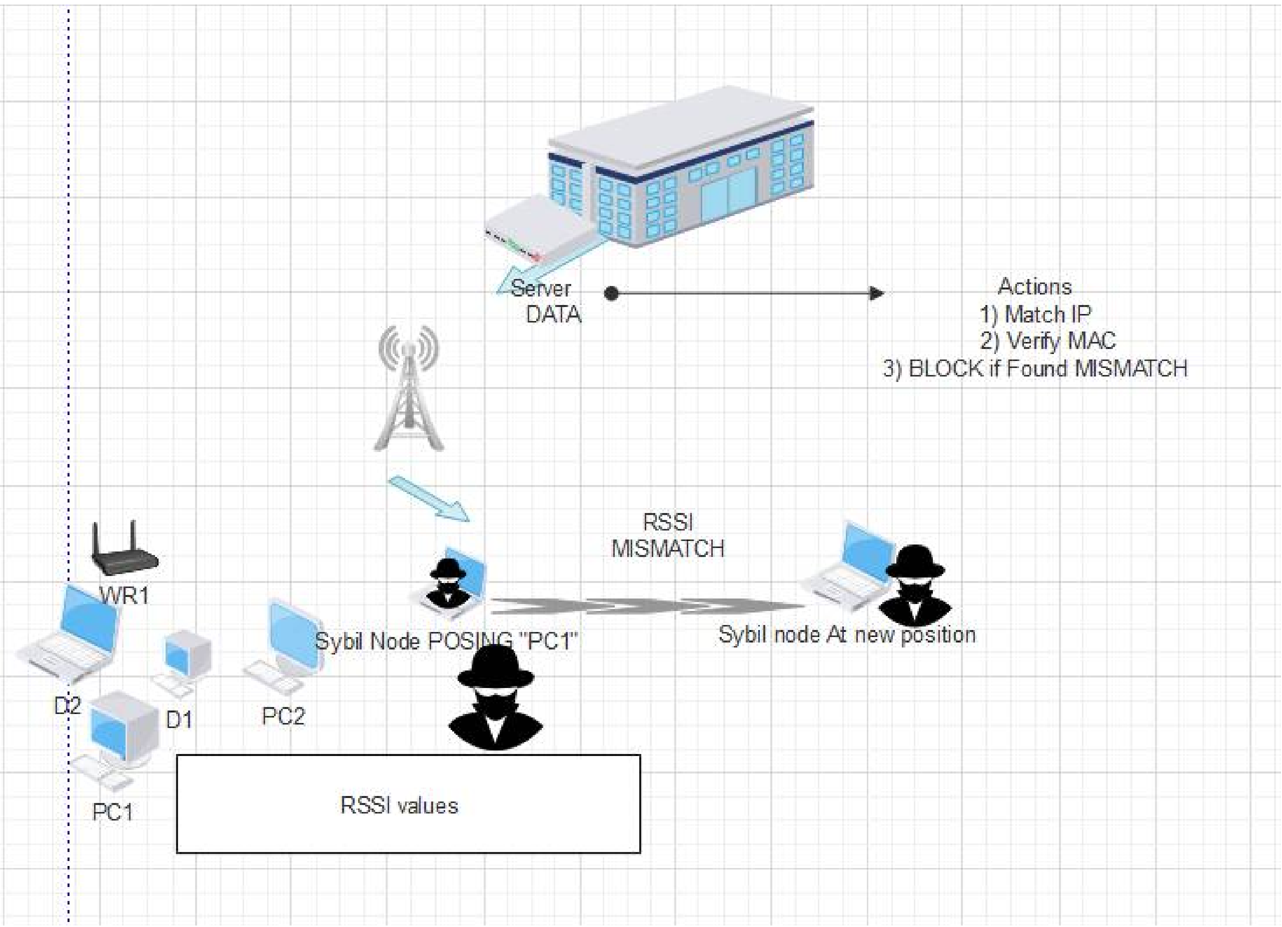
III. TYPES OF ATTACKS

Passive Attack– It is kind of where malicious node listens and observes the content of packet by eavesdropping and traffic analysis. But it does not make any fabrication and modification or drop packet.
Active attack **-** attacker may try to introduce malicious node inside the network or compromise the trusted node for Dropping of packets, denial of service attack, modification of data and sending fabricated spoofed message in network.
Smurf attack– Sybil node send ICMP echo message to broadcast address of network with spoofed IP address of legitimate node then ICMP echo-reply message from all host in network is designated to legitimate node which create flooding traffic for legitimate node
Fraggle attack – Sybil node broadcast UDP echo packet to network with spoofed identity of legitimate node and legitimate node flooded with reply traffic from network.
ARP-poisoning attack **-** Sybil node send reply message of arp request with spoofed IP address of gateway so it become gateway for node and perform active or passive attack on packet which send by nodes.
Routing loop **–** Sybil node send RREQ packet in network then nodes send RREP to Sybil node but the RREQ source not listed in network so RREP packet propagate in hole network until TTL value of IP packet is expired
TTL expiry attack **-** Sybil node decrement the TTL value to zero of IP packet which it received to forward ,then Sybil node send ICMP time exceeded with spoofed identity of legitimated node.so source node assume there is routing-issue with particular node and remove node form its routing table.

IV. PROPOSED ALGORITHM

- Following graphical representation is an illustration that how a Sybil can attack and where it can reside.
- This system shows how to prevent the arrival of Sybil requests
- RSSI calculation
- Identity change by a node posing as its original node

DOI: 10.15680/IJIRCCE.2016. 0404184



Design Considerations:

- Check for IP and MAC match in a black list
- Scalar RSSI values for range prediction
- Maintaining a database for Sybil nodes id
- Public key encryption
- Address verification

A. Description of the Proposed Algorithm:

Aim of the proposed algorithm is to maximize the security aspects of nodes in wireless network like manet by using the ip, mac check process and RSSI value calculation to enable the extensive features of security.

Step 1: IP Check in black list
Step 2: MAC check for verifying the node identity

Step 3: Calculate scalar RSSI values

Step 4: Establish a connection once the verification satisfies the authentication policies

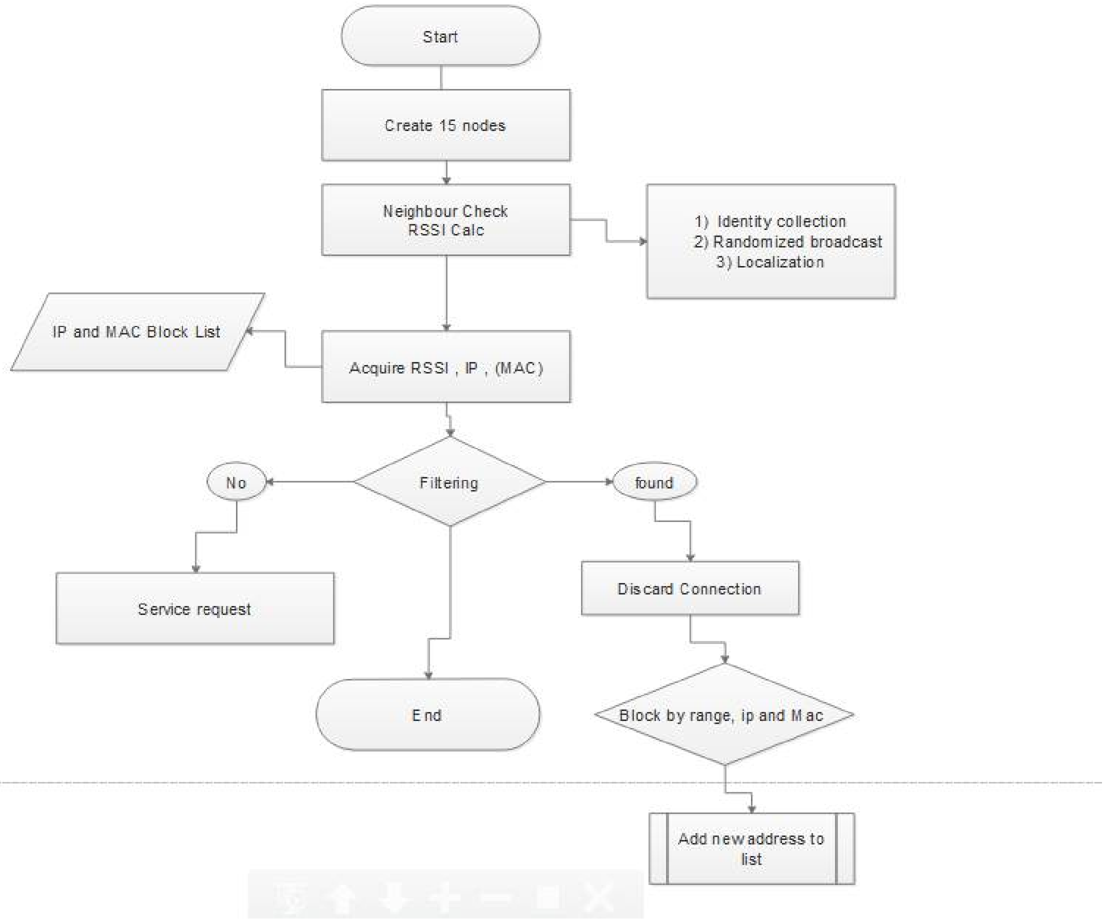
V. DETECTING THE MOVING ATTACKERS

A mobile attacker can defeat signalprint comparison by changing locations or orientations between transmissions to associate distinct signalprints with each Sybil identity. Instead of restricting the attack model to only stationary devices, we protect against moving attacks by detecting moving nodes. Moving nodes are treated as non-conforming, in essence, and will not be able to participate in network protocols until stationary enough to be tested for Sybilness again. Fortunately, in the networks we consider, most conforming nodes (e.g., human-carried smartphones and laptops) are stationary over most short time-spans (1 to 2 min), due to human mobility habits. Thus, multiple transmissions should have the same signalprints [15]. From this observation, we develop a protocol to detect moving attackers. Again, the lack of trusted observations is troublesome. Instead of comparing signalprints, we compare the initiator's observations: all transmissions from a conforming node should have the same RSSI. As shown in Section 9, this simple criterion yields acceptable detection.

VI. ALGORITHM/FLOW CHART

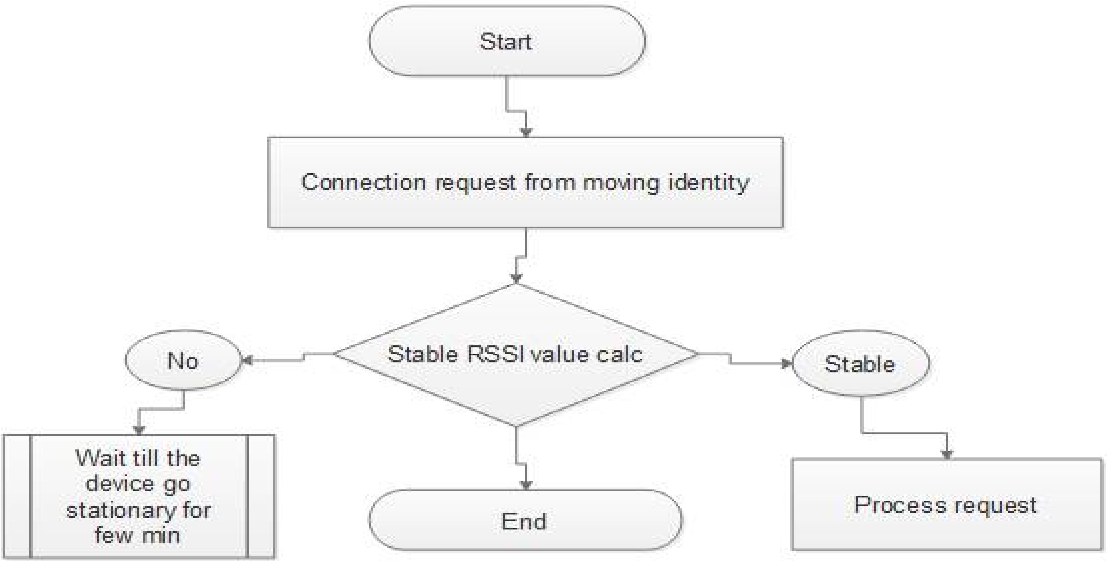
Establishing a connection between two peers and to a server can result in a unauthorized access to the network or to the available files in the system. Hence the requirement to avoid this is to check for the black list which is a part of the system we are proposing in which the predicted and detected sybil nodes would be stored. That enables the systems in network to have a primary security feature to achieve discard unwanted requests from random systems.

a) Phase1 – IP and MAC check for nodes requesting a service and Scalar RSSI calculation



Once the IP and MAC filtering is done, the RSSI values will be evaluated and provide with the service. If found with wrong or improper RSSI values for the requesting systems, it has to be discarded for the service. alculating stable RSSI values indicates the truthness of the systems to classify Sybil and non0Sybil systems among all.

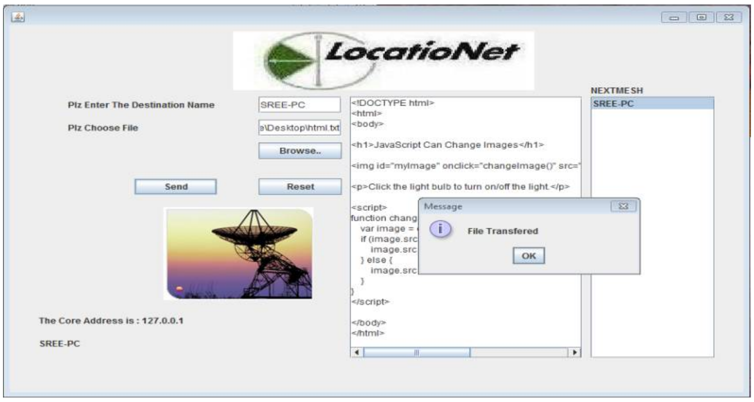
b) Phase 2- Service enablement


Start
Connection request from moving identity
Stable RSSI value calc
No
Stable
Wait till the device go stationary for few min
End
Process request

VII. SCREENSHOTS

1) Home window showing transmission of data to a non-sybil identity

The following screenshot shows the prompt that lists the available network terminals in the current network. Selecting a file to send to the destination is done using this terminal and encrypted with the public key encryption technique. We will receive a notification on the successful transmission of the data with flash message which is illustrated in the following picture.



Plz Enter The Destination Name SREE-PC

Plz Choose File e\Desktop\html.txt

```
<!DOCTYPE html>
<html>
<body>

<h1>JavaScript Can Change Images</h1>

<img id="myImage" onclick="changeImage()" src="

<p>Click the light bulb to turn on/off the light.</p>

<script>
function chang
   var image = 
   if (image.src
      image.src
   } else {
      image.src
   }
}
</script>

</body>
</html>
```

NEXTMESH
SREE-PC

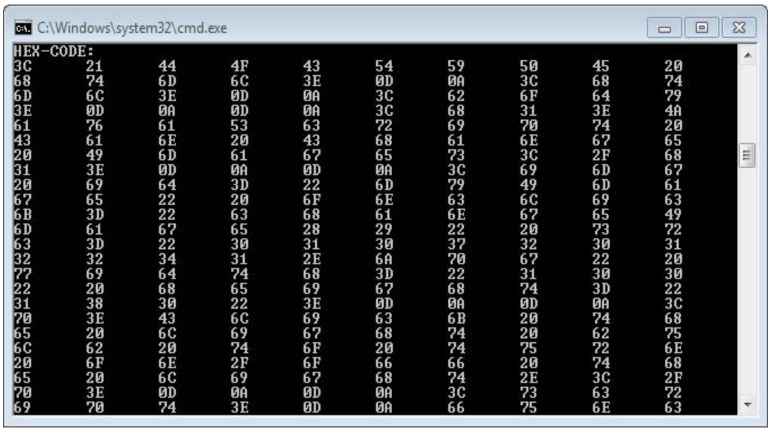
Message
File Transfered

The Core Address is : 127.0.0.1

SREE-PC

2) Encrypted data

As mentioned the data is being encrypted and sent over the network once the destination is prescribed by the sender. All this process can come into picture only if it bypasses the IP and MAC filtering. Thus the selected data will be converted into the cipher form to give a secure feature.



```
HEX-CODE:
3C      21      44      4F      43      54      59      50      45      20
68      74      6D      6C      3E      0D      0A      3C      68      74
6D      6C      3E      0D      0A      3C      62      6F      64      79
3E      0D      0A      0D      0A      3C      68      31      3E      4A
61      76      61      53      63      72      69      70      74      20
43      61      6E      20      43      68      61      6E      67      65
20      49      6D      61      67      65      73      3C      2F      68
31      3E      0D      0A      0D      0A      3C      69      6D      67
20      69      64      3D      22      6D      79      49      6D      61
67      65      22      20      6F      6E      63      6C      69      63
6B      3D      22      63      68      61      6E      67      65      49
6D      61      67      65      28      29      22      20      73      72
63      3D      22      30      31      30      37      32      30      31
32      32      34      31      2E      6A      70      67      22      20
77      69      64      74      68      3D      22      31      30      30
22      20      68      65      69      67      68      74      3D      22
31      38      30      22      3E      0D      0A      0D      0A      3C
70      3E      43      6C      69      63      6B      20      74      68
65      20      6C      69      67      68      74      20      62      75
6C      62      20      74      6F      20      74      75      72      6E
20      6F      6E      2F      6F      66      66      20      74      68
65      20      6C      69      67      68      74      2E      3C      2F
70      3E      0D      0A      0D      0A      3C      73      63      72
69      70      74      3E      0D      0A      66      75      6E      63
```

VII. Conclusion and Future Work

We have described a method to use signalprints to detect Sybil attacks in open ad hoc and delay-tolerant networks without requiring trust in any other node or authority. We use the inherent difficulty of predicting RSSIs to separate true and false RSSI observations reported by one-hop neighbours. Attackers using motion to defeat the signalprint technique are detected by requiring low-latency retransmissions from the same position. It eliminates 99.6–100 percent of Sybil identities in office environments, 91 percent in a crowded highmotion cafeteria, and 96 percent in a high-motion open outdoor environment. It accepts 88–97 percent of conforming identities in the office environments, 87 percent in the cafeteria, and 61 percent in the outdoor environment. The vast majority of rejected conforming identities were eliminated due to motion.

References

[1] Robert P. Dick, Member, IEEE, Z. Morley Mao, and Dan S. Wallach. The Mason Test: A DefenseAgainst Sybil Attacks in Wireless Networks Without Trusted Authorities.IEEE transaction | volume 4, 2015

[2] SuhasiniSodagudi et al | A Case Based Study to Identify Malicious Node in Packet Routing, International Journal of Computer Science Engineering and Technology(IJCSET) | November 2014 | Vol 4, Issue 11,308-313

[3] David Robinson Bild, Non-Hierarchical Networks for Censorship-Resistant Personal Communication 2014

[4] Comparison between Sybil Attack Detection Techniques: Lightweight and Robust, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 2, February 2014 Copyright to IJAREEIE www.ijareeie.com 7142

[5] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the Sybil attack," Dept. Comput. Sci., Univ. Massachusetts Amherst, Amherst, MA, USA, Tech. Rep. 2006-052, Oct. 2006.

[6] H. Zhou, M. Mutka, and L. Ni, "Multiple-key cryptographybased distributed certificate authority in mobile ad-hoc networks," in Proc. Global Telecommun. Conf., vol. 3, Nov. 2005, pp. 1681–1685.

[8] M. Ramkumar, and N. Memon, "An efficient key Predistribution scheme for ad hoc network security," IEEE J. Select. Areas Commun., vol.23,no.3,pp.611–621,Mar.2005.

[9] N. Borisov, "Computational puzzles as Sybil defenses," in Proc. Int. Conf. Peer-to-Peer Comput., Sep. 2006,pp.171–176.

[10] F. Li, P. Mittal, M. Caesar, and N. Borisov, "SybilControl: Practical Sybil defense with computational puzzles," in Proc. Workshop Scalable TrustedComput., Oct. 2012, pp. 67–78.

[11] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "SybilGuard: Defending against Sybil attacks via social networks," in Proc. SIGCOMM Comput. Commun. Review, Sep. 2006, pp. 267–278.

[12] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A nearoptimal social network defense against Sybil attacks," in Proc. Symp. Security Privacy, May 2008, pp. 3–17.

[13] T. S. Rappaport, Wireless Communications: Principles & Practice. Englewood Cliffs, NJ, USA: Prentice-Hall,2002.

[14] A. Haeberlen, E. Flannery, A. M. Ladd, A. Rudys, D. S. Wallach, and L. E. Kavraki, "Practical robust localization over large-scale 802.11 wireless networks," in Proc. Int. Conf. Mobile Comput. Netw., Sep.2004,pp.70–84.

[15] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," IEEE Trans. Inform. Forensics Security, vol. 4, no. 3, pp. 492–503, Sep.2009.

[16] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proc. Workshop Wireless Security, Sep. 2006, pp. 43–52.

BIOGRAPHY

Vinayaka APis a post graduate student in the Information Science Department pursuing computer network engineering at The oxford college of Engineering, Bangalore.He received B.E degree in 2014 from VTU, Belagaum, India. His research interests are Computer Networks (wireless Networks), IOT, PROSE , WSN etc.

Nalinakshi B G is currently working in Dept of ISE,at The oxford college of Engineering, Bangalore.Received the Bachelor's Degree in Information Science and Engineering from, Tontadarya College of Engineering, Gadag, Visvesvaraya Technological University, Belgaum, Karnataka State, India, and the Master Degree in Computer Science and Engineering from Basaveshwar Engineering College Bagalkot, Karnataka State, India. Her areas of interest are Biometrics, Image processing, and Computer Graphics.