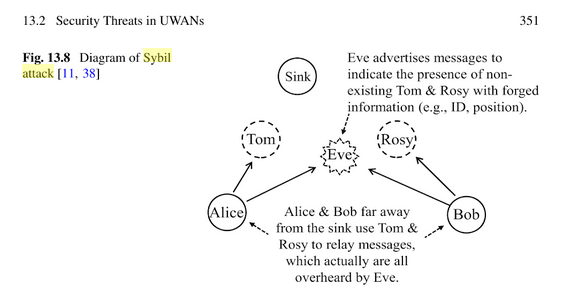
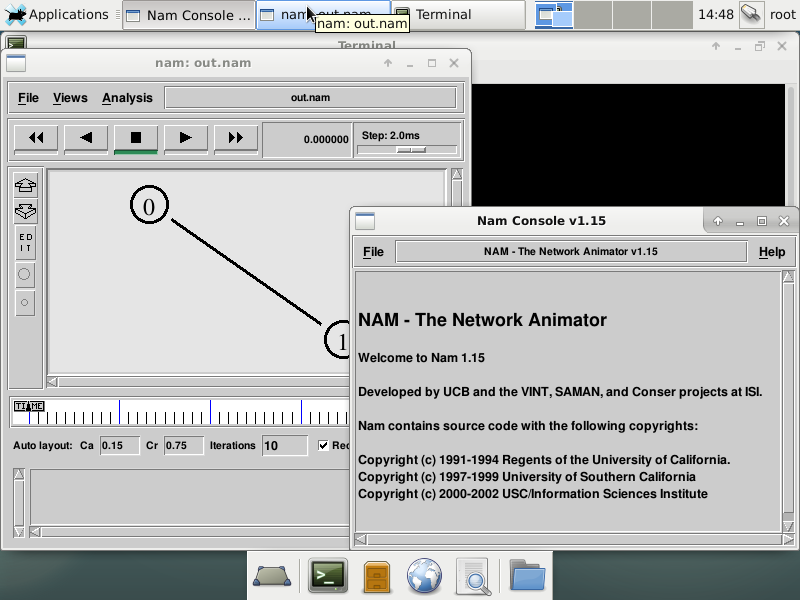
1. What are Sybil Attacks?
   1. Sybil attacks use one or more nodes with falsify their identity to subvert reputation systems to gain more access, change other nodes behavior, or restrict access to other node in the peer-to-peer networking.
   2. Sybil attacks are different than man in the middle attacks because man in the middle require an infrastructure; Sybil attacks work in Ad-Hoc networks.
      1. Sybil attacks are relevant in highly distributed networks that lack a central control method.
      2. Attacks are possible without some centralized method of verifying identity.
      3. Attacks are also possible if a method of validation is based on a threshold of peer nodes agreeing to the validity of a node or transmission.
   3. The human version of Sybil Attacks is called Sock-puppeting.
      1. Sock-puppeting and Sybil attacks main goal is to deceive other peers into acting in ways they wouldn’t otherwise act.
2. Appeals of Sybil attacks
   1. Attackers can deploy a Sybil attack by creating one node that more resources than expected to create many different fake nodes.
      1. By sharing the same radio, an attacker broadcasts in serial their falsified identity; More than one radio will be in parallel with a limit by the number of radios. (Chris Piro)
   2. The false nodes allow for the attacker to change routing, corrupt or insert invalid data, or deny access to other nodes.
      1. In each type of ad-hoc or distributed network, each node has processing to do that is required by the overall application of the network.
   3. Sybil attacks are attractive attacks because they take advantage of trust based on one node one identity.
      1. However, identities and node count are not one to one and are separate properties.
3. What type of networks do Sybil attacks impact?
   1. Wireless networks
      1. Ad-hoc wireless networks are vulnerable to Sybil attacks as they do not have a centralized infrastructure controlling and routing access to the wireless channel.
   2. Wireless sensor or data collection networks
      1. In data collection or sensor networks, each sensor passes its results along, but injecting false values it can corrupt the validity of the results over time.
   3. Block chain networks
      1. Block chain networks use a threshold voting system of 51%.
      2. This threshold can be overrun with fake identities so that it allows the owners of the fake identities to control the creation of new records in the block chain.
   4. P2P routing networks
      1. The fake identities suggest paths that misdirect, deny, or flood traffic to or from other nodes.
      2. Ad-hoc wireless networks use P2P routing and are impacted in this same way.
4. How do they impact wireless networks?
   1. Wireless networks use a shared channel.
      1. Each wireless node uses carrier-sense multiple access or code division multiple access.
         1. No one node has more access than others without creating more identities in the network.
         2. By Creating more nodes, one node uses more of the limited bandwidth and/or channels.
            1. Allowing for more access to resources and abuse the channel.
   2. Sybil attacks can slow down a wireless network.
      1. The offending node can fill the shared channel with more transmissions flooding the channel.
         1. This is most prevalent in CSMA-CA networks with exponential back off.
         2. Each perceived collision will make a node wait from 0 to 2^k-1 units of time (k is the number of collisions)
      2. Since one node has many identities, it can continue to broadcast on each of these pseudo-nodes.
         1. This can fill the channel and deny service to other nodes.
   3. Wireless networks with dynamic routing require information from the nodes in order to make the routing of traffic efficient.
      1. Information that is collected wireless networks
         1. Received power
         2. Accessible nodes
         3. MAC addresses (layer 2)
         4. IP addresses (layer 3)
         5. Each of these parts make up an identity of a wireless network node.
5. Why are Sybil Attacks important to security in a Wireless network?
   1. Ad-hoc networking have benefits of being very low cost and easy to setup for mobile applications.
      1. P2P networking in wireless networks allow for greater range of the network
      2. Range of the network is proportional to the size of the network in nodes shared by the channel
      3. Not to geographic bound by central infrastructure system such as an Access Point.
      4. Nodes may join and drop out of the network easily.
   2. Sybil attacks can be used to change or deny the routing of other nodes in the network.
      1. One way to do this is through false reporting of the power signal of nodes in RSSI (received signal strength indicator)
         1. Fake the location of another node on the network. (Alhasanat, 2016)
            1. Locations can be estimated by the power level.
      2. False reporting of non-existent nodes in manet protocols
         1. AODV protocol can be abused by a sybil node by falsely responding to RREQ multicast messages reporting back a non-existent route or replying when with false route to a hello message.
         2. In DSDV, create false notes with better routes in the sybil node, and waiting until all the other nodes update with this incorrect information.
            1. This could be used to reroute all data through the sybil node regardless if it’s the most efficient route
            2. DSDV nodes all have a table and each broadcast their routing tables periodically.
            3. These tables can have invalid data by a sybil node causing invalid routing by the network.
         3. With the GPSR protocol, a sybil node could broadcast several invalid nodes beacons or copy the beacon of the intended destination node.
            1. GPSR is stateless and relies on these beacons to tell who can hear who. (MIT, 2018)
   3. Anyone can interact with the network via the airspace.
      1. The open nature of ad-hoc networking means that security is challenging because there isn’t a great way to validate a node before it is connected.
      2. The marginal costs to listen or interact to the Manet is very low.
      3. Technology is readily available and easy to use.
6. What are the methods and problems of detecting Sybil Attacks?
   1. Douceur’s work shows that there is no practical defense against Sybil attacks; Even PKI system must check if each node is only one node. (Douceur, 2002)
      1. Checking each node is can be cost prohibitive vs the cost to create new nodes.
         1. This difference is the reason why this attack is effective.
   2. Current methods of detection depend on looking for markers that suggest more than one identity is being used by only one node.
   3. Validating each marker defeats the benefits of manet wireless connections.
7. What are methods of mitigating Sybil Attacks?
   1. Authentication
      1. Sybil attacks exist because a node is reporting a one or more false identities.
      2. Using a 3rd party to validate identity solves this issue
         1. Certificate Authority is an example of this principle.
         2. System is not perfect because attacker may buy or steal more CA certificates
            1. The 3rd party also has a perverse incentive to allow it.
      3. Authentication is expensive and creates overhead.
      4. Authentication depends on a way to validate all the parts of identification.
   2. Detection
      1. Simple Sybil node detection requires passive listening to the channel in defined time-buckets. Piro, shields, and Levine, demonstrate that these slots allow for method computation of affinity of two nodes. By creating a graph with undirected edges using a threshold of 0.1 to remove irrelevant affinities. After a depth first search, the greatest values are the Sybil nodes. (Chris Piro)
8. First Implementation attempt was with Opnet



* 1. This was based on this diagram with a sybil attack making a sinkhole (Jiang, 2018)
  2. Jiang describes, that “CTS should not transmit during the time period indicated by the RTS and CTS. However, a malicious node may violate this rule and transmit even after overhearing a CRS destined for a legitimate node”
  3. After creating the project with the manet objects, and adding my wireless nodes, attempting to run the project failed.
     1. Without knowing how Opnet modeler works with this new model set, I opened up the example MANET from c:\opnet
     2. The expectation is that these models would run without modification, however, they failed to run. I tried all of them.
  4. I learned that Opnet allows for the modeling of AODV, DSDV, and GPSR routing.
  5. Outside of the fact that Opnet was missing something in its configuration that was keeping manet models from running, I also found it challenging to configure more than one identity for the sybil node.
  6. I was unable to find the configuration for Opnet CTS or RTS.
  7. I abandoned this attempt.

1. Attempt: NS2
   1. Installed ns2 on linux, which was very easy.
   2. Learned that NS2 uses TCL and C++ for modeling.
   3. Looked at tcl and I don’t understand it right away.
   4. Tried to run a sample ad hoc network sample in ns2, got errors about -channel that referenced master\_mdif.tcl
      1. This master file said that multiple interfaces are not supported on nodes.
   5. Confirmed that NS2 and nam was installed correctly with but running a simple sample.
   6. 
   7. The wireless ad-hoc example I found in ns2 didn’t run. I was unable to troubleshoot the problem to make it run.
   8. Without a working example to start from I was forced to abandon this attempt.
2. Conclusion
   1. Wireless Sybil attacks are difficult attacks to mitigate, detect, and prevent. These issues are because trust is assumed first by other nodes in the network. Sybil attacks abuse this trust of one node to one identity by creating more than one identity. The masquerading node can change routing in the network, disrupt services, and create breach in network security.
   2. Detection and prevention of sybil nodes is resource intensive and counter productive to ad-hoc networking.

Wireless Sybil Attacks

Dustin Watson

CNA 465

# Overview of Sybil Attacks

Sybil attacks use one or more nodes with falsify their identity to subvert reputation systems to gain more access, change other nodes behavior, or restrict access to other node in the peer-to-peer networking.

Sybil attacks are different than man in the middle attacks because man in the middle require an infrastructure; Sybil attacks work in Ad-Hoc networks. Sybil attacks are relevant in highly distributed networks that lack a central control method. Attacks are possible without some centralized method of verifying identity. Attacks are also possible if a method of validation is based on a threshold of peer nodes agreeing to the validity of a node or transmission.

Sybil attacks main goal is to deceive other peers into acting

in ways they wouldn’t otherwise act.

# Appeal of Sybil attacks

Sybil attacks are attractive attacks because they take advantage of trust based on one node one identity. However, identities and node count are not one to one and are separate properties.

Attackers can deploy a Sybil attack by creating one node that more resources than expected to create many different fake nodes. By sharing the same radio, an attacker broadcasts in serial their falsified identity; More than one radio will be in parallel with a limit by the number of radios. (Chris Piro) The false nodes allow for the attacker to change routing, corrupt or insert invalid data, or deny access to other nodes. In each type of ad-hoc or distributed network, each node has processing to do that is required by the overall application of the network.

# Types of networks Sybil attacks impact

## Wireless networks

Ad-hoc wireless networks are vulnerable to Sybil attacks as they do not have a centralized infrastructure controlling and routing access to the wireless channel.

## Wireless sensor or data collection networks

In data collection or sensor networks, each sensor passes its results along, but injecting false values it can corrupt the validity of the results over time.

## Block chain networks

Block chain networks use a threshold voting system of 51%. This threshold can be overrun with fake identities so that it allows the owners of the fake identities to control the creation of new records in the block chain.

## P2P routing networks

The fake identities suggest paths that misdirect, deny, or flood traffic to or from other nodes. Ad-hoc wireless networks use P2P routing and are impacted in this same way.

# Impact of Sybil attacks on Wireless networks

Wireless networks use a shared channel which makes them vulnerable to sybil attacks. Each wireless node uses carrier-sense multiple access or code division multiple access. No one node has more access than others without creating more identities in the network. By Creating more nodes, one node uses more of the limited bandwidth and/or channels. Allowing for more access to resources and abuse the channel. By doing this, Sybil attacks can impact the security of the network.

Sybil attacks can slow down a wireless network. The offending node can fill the shared channel with more transmissions flooding the channel. This is most prevalent in CSMA-CA networks with exponential back off. Each perceived collision will make a node wait from 0 to 2^k-1 units of time (k is the number of collisions) Since one node has many identities, it can continue to broadcast on each of these pseudo-nodes. This can fill the channel and deny service to other nodes.

Wireless networks with dynamic routing require information from the nodes in order to make the routing of traffic efficient. Information that is collected wireless networks: Received power, Accessible nodes, MAC addresses (layer 2), IP addresses (layer 3). Each of these parts make up an identity of a wireless network node.

# Security and Sybil attacks in a Wireless network

Sybil attacks can be used to change or deny the routing of other nodes in the network. One way to do this is through false reporting of the power signal of nodes in RSSI (received signal strength indicator). Fake the location of another node on the network. (Alhasanat, 2016). Locations can be estimated by the power level. False reporting of non-existent nodes in manet protocols. AODV protocol can be abused by a sybil node by falsely responding to RREQ multicast messages reporting back a non-existent route or replying when with false route to a hello message. In DSDV, create false notes with better routes in the sybil node, and waiting until all the other nodes update with this incorrect information. This could be used to reroute all data through the sybil node regardless if it’s the most efficient route. DSDV nodes all have a table and each broadcast their routing tables periodically. These tables can have invalid data by a sybil node causing invalid routing by the network. With the GPSR protocol, a sybil node could broadcast several invalid nodes beacons or copy the beacon of the intended destination node. GPSR is stateless and relies on these beacons to tell who can hear who. (MIT, 2018)

Anyone can interact with the network via the airspace. The open nature of ad-hoc networking means that security is challenging because there isn’t a great way to validate a node before it is connected. The marginal costs to listen or interact to the Manet is very low. Technology is readily available and easy to use.

# Methods and problems of detecting Sybil Attacks

Douceur’s work shows that there is no practical defense against Sybil attacks; Even PKI system must check if each node is only one node. (Douceur, 2002). i. Checking each node is can be cost prohibitive vs the cost to create new nodes. This difference is the reason why this attack is effective. Current methods of detection depend on looking for markers that suggest more than one identity is being used by only one node. Validating each marker defeats the benefits of manet wireless connections.

# Methods of mitigating Sybil Attacks

## Authentication

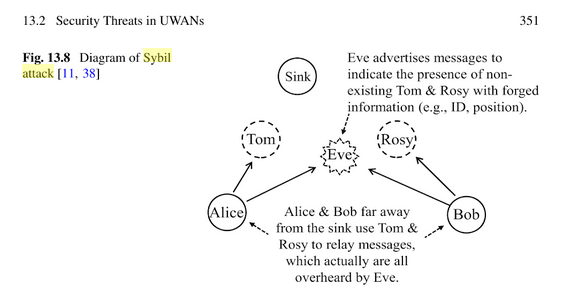
Sybil attacks exist because a node is reporting a one or more false identities. Using a 3rd party to validate identity solves this issue. Certificate Authority is an example of this principle. System is not perfect because attacker may buy or steal more CA certificates. The 3rd party also has a perverse incentive to allow it. Authentication is expensive and creates overhead. Authentication depends on a way to validate all the parts of identification.

## Detection

Simple Sybil node detection requires passive listening to the channel in defined time-buckets. Piro, shields, and Levine, demonstrate that these slots allow for method computation of affinity of two nodes. By creating a graph with undirected edges using a threshold of 0.1 to remove irrelevant affinities. After a depth first search, the greatest values are the Sybil nodes. (Chris Piro)

# Implementation Simulation Attempts

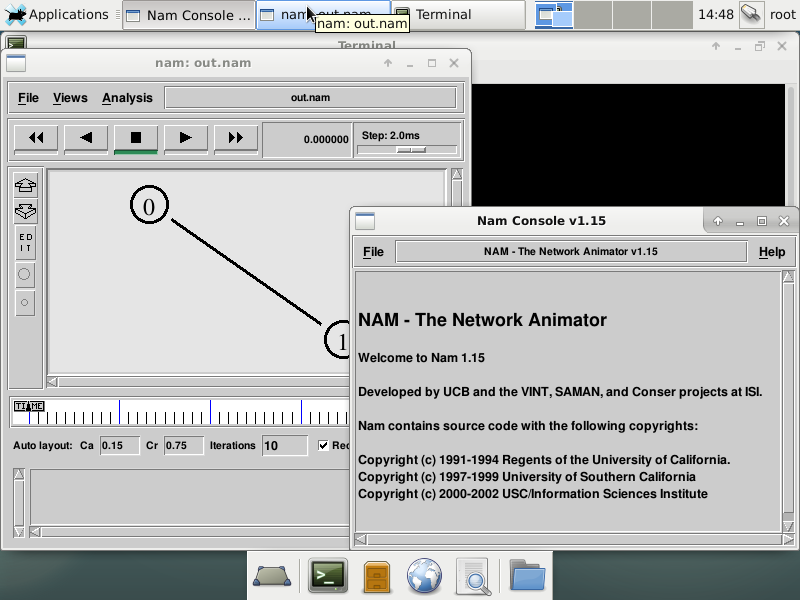
## Attempt with Opnet



This was based on this diagram with a sybil attack making a sinkhole (Jiang, 2018) Jiang describes, that “CTS should not transmit during the time period indicated by the RTS and CTS. However, a malicious node may violate this rule and transmit even after overhearing a CRS destined for a legitimate node”. After creating the project with the manet objects, and adding my wireless nodes, attempting to run the project failed. Without knowing how Opnet modeler works with this new model set, I opened up the example MANET from c:\opnet The expectation is that these models would run without modification, however, they failed to run. I tried all of them. I learned that Opnet allows for the modeling of AODV, DSDV, and GPSR routing. Outside of the fact that Opnet was missing something in its configuration that was keeping manet models from running, I also found it challenging to configure more than one identity for the sybil node. I was unable to find the configuration for Opnet CTS or RTS. I abandoned this attempt.

## Attempt with NS2

Installed ns2 on Linux, which was very easy. Learned that NS2 uses TCL and C++ for modeling. Looked at tcl and I don’t understand it right away. Tried to run a sample ad hoc network sample in ns2, got errors about -channel that referenced master\_mdif.tcl This master file said that multiple interfaces are not supported on nodes. Confirmed that NS2 and nam was installed correctly with but running a simple sample.



The wireless ad-hoc example I found in ns2 didn’t run. I was unable to troubleshoot the problem to make it run. Without a working example to start from I was forced to abandon this attempt.

# Conclusion

Wireless Sybil attacks are difficult attacks to mitigate, detect, and prevent. These issues are because trust is assumed first by other nodes in the network. Sybil attacks abuse this trust of one node to one identity by creating more than one identity. The masquerading node can change routing in the network, disrupt services, and create breach in network security. Detection and prevention of sybil nodes is resource intensive and counterproductive to ad-hoc networking.