**Sybil Attack and Proposed Energy Efficient Prevention Approach**

**Background:**

The Sybil attack is an attack wherein a [reputation system](https://en.wikipedia.org/wiki/Reputation_system) is subverted by forging identities in [peer-to-peer](https://en.wikipedia.org/wiki/Peer_to_peer) [networks](https://en.wikipedia.org/wiki/Computer_network). It is named after the subject of the book [Sybil](https://en.wikipedia.org/wiki/Sybil_(book)), a case study of a woman diagnosed with [dissociative identity disorder](https://en.wikipedia.org/wiki/Dissociative_identity_disorder).

**Description:**

A Sybil attack is an attack where a single adversary is controlling multiple nodes on a network. It is unknown to the network that the nodes are controlled by the same adversarial entity. Microsoft researcher John Douceur describes that a Sybil attack relies on the fact that a network of computers cannot ensure that each unknown computing element is a distinct, physical computer. It is important to recognize any Sybil attack in order to protect and secure yourself.

It is a type of security threat when a node in a network claims multiple identities. For example, an adversary can create multiple accounts with different usernames and e-mail addresses and pretend that they all exist in different locations. Mostly networks are based on assumptions of identity, where each computer represents unique identity. Sybil attacks have appeared in many scenarios causing serious problems and threats for security, safety and trust. An attacker with many identities can use them to act maliciously, by either stealing information or disrupting communication.

**Prevention Approaches:**

There are many ways in which we can avoid this attack but avoiding Sybil attacks with a prevention that is energy efficient is very difficult problem.

We can use a centralized systems to avoid these attacks. Centralized systems ensures one-to-one correspondence between an identity and also by requiring that an individual IP cannot create more than a specific number of accounts in a given time interval or position, a centralized system can possibly avoid Sybil attacks.

A successful Sybil attacks prevention technique is presented in Bitcoin. It is by requiring block generation ability to be proportional to computational power available through the proof-of-work mechanism. In this way an adversary is limited number of blocks they can produce.

We can detect the locales from where the node is joining to avoid the possible attack. If we are using detecting a Sybil attack for some mobile devices, we can also make use of the mobile locations.

We can use trusted devices or trusted certification to prevent a Sybil attack. For trusted devices identities are associated to specific hardware devices but there are no special methods of preventing an attacker from obtaining multiple devices other than manual intervention.

Sybil attack may not effect directly as a virus or something, but this can affect the online e-commerce and communication.

**References:**

[1]Yu, Haifeng, Michael Kaminsky, Phillip B. Gibbons, and Abraham Flaxman. "Sybilguard: defending against sybil attacks via social networks." In *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 4, pp. 267-278. ACM, 2006.

[2] Levine, Brian Neil, Clay Shields, and N. Boris Margolin. "A survey of solutions to the sybil attack." *University of Massachusetts Amherst, Amherst, MA* 7 (2006): 224.

[3] Hoffman, Kevin, David Zage, and Cristina Nita-Rotaru. "A survey of attack and defense techniques for reputation systems." *ACM Computing Surveys (CSUR)* 42, no. 1 (2009): 1.

[4] https://en.wikipedia.org/wiki/Sybil\_attack