A Survey: Detection and Mitigation Techniques of Sybil in the Networks

Meena Bharti[1], Dr Shaveta Rani[2] and Dr Paramjeet Singh
[1]*Research Scholar, I.K. Gujral Punjab Technical University, Kapurthala, Punjab, 144603, INDIA*
[2]*Professor, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, 151001, INDIA*
[3]*Professor, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, 151001, INDIA*

Article Info
Page Number: 51 – 59
Publication Issue:
Vol 71 No. 2 (2022)

Abstract
Wireless networks are complicated to put together, and the more people use them over time, the more complicated they become. Wireless networks are made up of many different types of technology, which means they have vulnerabilities. One vulnerability is that they are easily spoofed or impersonated by Sybil attacks. In a Sybil attack, the attacker disguises themselves as someone else and generates various identities to have access to the system. This type of attack is typically accomplished by creating multiple fake user accounts. The attacker then uses these fake accounts to promote their content or ideas, vote for their own content or ideas, and/or harass other users. Since wireless networks are very resource-constrained, it is vital to develop more efficient and lightweight trustworthy security mechanisms to identify & track Sybil attacks as these are a major concern for the stability or security of the network. There are some security schemes for prevention against Sybil attacks, like cryptography, privacy-preserving solutions and lightweight authentication. Cryptography and privacy-preserving techniques require key management and additional infrastructure overhead, which makes them difficult to establish and maintain in a limited resource environment. The lightweight trusted system detects & avoids single node and multi-node attacks under different conditions. In this paper, a survey is conducted on various techniques for the detection of Sybil attacks.

Article History
Article Received*: 05 December 2021*
Revised*: 12 January 2022*
Accepted*: 02 February 2022*
Publication*: 10 March 2022*

Keywords: Sybil Attack, Wireless Network, Defence Mechanism, Social Network

1. INTRODUCTION

More wireless networks are being deployed every year. Sensors will also be used in the future to monitor temperature, humidity, and other conditions. Due to the fact that these are so easy to hack, this is where most attacks are happening too. If you're not careful, hackers will be able to see your information & sensitive data whilst simply sitting back and monitoring the wireless signal [1]. In particular, the two most common but also damaging types of attacks are spoofing and Sybil. In spoofing, we can masquerade as other devices and create more than one illegitimate identity for networks for malicious purposes. For example, we all know that mac address spoofing is a relatively simple process for an adversary to do. They can do this by using a few different techniques, such as vendor-supplied NIC drivers or open-source ones. And a malicious person could also pretend to be an authorized wireless access point or client so they can fool you into giving up your security info with them. For example, Denial-of-Service (DoS) attack may be launched and prevent you from finishing

your tasks [2]. On the other hand, a type of cyber-attack is a Sybil attack in which an individual or organization gains control of multiple online accounts and uses them to create false identities. Sybil attacks are often used to make it seem like there is widespread support for a particular opinion, idea, product, or person. It can also be used to make it seem like a group is more popular than they are. The term "Sybil" comes from the book "Sybil" by Flora Rheta Schreiber [3]. It tells the story of a dysfunctional woman with multiple personalities. Sybil attacks are bad news for network security. Basically, it's an AI infiltration tactic that circumvents group-based voting mechanisms and redundant backup systems. It works by overloading the system with meaningless requests so that it breaks down entirely [4], [5]. In the future, wireless and sensor networks will be targeted for take-over by attackers looking to disrupt business. The use of identity-based attacks is a serious problem and needs to be stopped to prevent network failures. Figure 1 depicts a schematic of the Sybil attack [6].

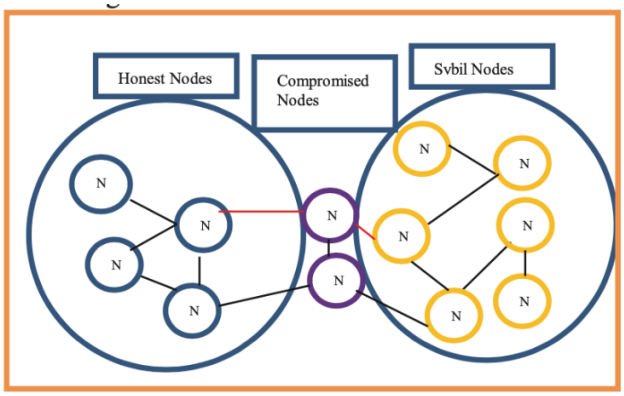

Figure 1: Sybil Attack

These attacks occur frequently in the networks with open channels for communication. They allow a bad actor to create multiple identities in order to sabotage decisions made by voting and disrupt network services [7]. Sybil nodes can also help prevent Sybil attacks from being successful. To do this, it's important to use things like authentication. Not many people know that! However, this only works if you have the right cryptography system in place for key management and maintenance. Whilst traditional approaches to tackling identity-based attacks involve implementing and efficiently distributing and maintaining cryptography, this can be a costly process which that takes time. Sensor node limited power and resources might not be able to support authentication. This can be a problem if the nodes have been compromised through cryptographic encryption methods because memory contents have been hacked. It's wise to use different parameters. It doesn't incur any additional overhead [6].

2. LITERATURE SURVEY

In my literature review, the different methods of detecting and preventing Sybil attacks are analyzed that are being used in distributed systems. In this proposal [8], A Sybil attack is an effort of an attacker to create false nodes in the system to disrupt the network. When they are manipulated to pose as legitimate nodes, it can interfere with communications between legitimate users on the network. However, the RSS is used by the authentication scheme to identify these unlawful attackers and maintain all communications within its network. In a network of devices that measures the signal strength for transmissions. The threshold refers to the smallest RSS value. If the RSS for that node exceeds the threshold, a new node will be added to the

network. If they are the same, you can verify their RSS values. The RSS metrics signify whether a new node has been discovered as a Sybil node. The benefits of the scheme are high true positives, low false positives and high levels of accuracy.

Random Password Comparison, or RPC, is a method for guarding against Sybil attacks [9]. This would allow to move your router nodes around. It also stores a routing database that contains each node's ID and time. It will also store the intermediate nodes located between the source and destination. The information at the intermediate node is then compared to that in the RPC database. If they match, it is assumed to be a normal node. However, if they don't match up, then you know there has been some kind of attack. Every few seconds, the network of nodes generates completely new passwords for each of their nodes and sends them to all of the other nodes. "During the time that destination node is communicating with source node, the ID, delay and random password corresponding to delay are compared with the database." If the information (sent to one node) matches the data on the other node(s), then both nodes communicate with each other. If not, then it's considered a Sybil attack and the sender will be rejected. This is a dynamic & accurate tracking technique that optimizes data transmission in networks and has improved throughput too.

Researchers [10] have been experimenting to find the best way to detect this type of thing by looking at two more parameters - energy and frequency. They checked the velocity, energy and frequency of node while it was entering. They considered 3 different threshold values and if all these threshold values are lower or equal to node’s velocity, energy or frequency the node is considered as legitimate otherwise as Sybil.

A vote trust algorithm [11] was used to detect a Sybil attack. Trust is determined by evaluating how much you have of each resource and the total acceptance rate of the network. If the node's GAR falls below the threshold, it is designated as a Sybil node. Trust voting used to identify small communities of Sybil nodes in the greater graph of the internet. Once these are identified, Google can run tests on voting patterns to make sure they are not fraudulent.

One proposed protocol for routing is the Remote Procedure Call (RPC) protocol [12]. When encrypting this protocol, three things are stored in each node's location table: their unique ID, the time of access, and the password used to access that node. If the data on both nodes match, then it's said to be a normal node. If there's no match between two nodes, they're said to be "Sybil nodes." Every time interval, a new password is generated. The current node is talking to the previous node, and it will compare its ID, time delay and random password with the other data in their database of RPC requests. If there's a match, it will transmit the specified code.

The author [13] proposes an efficient method Channel-Based for detecting Sybil attacks on wireless networks. To detect a Sybil attack, a new authentication method relies on the fact that radio channels in inhabited environments have spatial instability because signals get 'lost' or changed by reflections from other objects. Hide your SSID and MAC address to prevent detection by the Sybil client detector! This method can easily be implemented because it does not require expensive equipment or heavy research. It can also be mixed in with other security strategies such as detecting an attack.

The author [14] suggests that one way to identify Sybil identities is by looking at node changes. Identities that are usually looked together are called Sybil identities, while unique nodes that move independently are called authentic nodes. When density of nodes is high, there are some chances of false positives which can be solved with some adjustments. For example, if soldiers are launched towards an objective, it won't make sense if they return before reaching the objective.

The author [15] proposed that security is achieved in MANETs by exploiting the inherent mobility of nodes. This means that nodes establish security associations solely through mutual agreement with other nodes. Users

can set up a secure point-to-point connection between their personal devices by adding each other to a WPA2-codepage which is saved on their device. The author of the paper argues that by using these security seals, it will be hard for your identity to be stolen or impersonated. However, this would only work if you were able to keep the seal on at all times and make sure to use a wired or infrared connection.

3. DETECTION MECHANISM

In the mobile environment, a single device will be identified only by one single identity at the time. How they're restricted to one identity is that they're all nodes on the same physical device. Contrastingly, when we talk about "nodes" when it comes to computers or computers networks, they can be free of any limitations and constraints with regards to this type of. As nodes move geographically, their Sybil identities will change over time [2]. For example, if a single attack channel is compromised, the attacker can only have one of the two identities transmitting at a time. If their range expands to include multiple channels, the number of Sybil identities required simultaneously will drop off exponentially according to the number of channels available. The identities a Sybil attacker assumes are different from those of an honest node [16]. A single node can only simulate a limited number of identities at a time, so it is resource-limited in computation, storage, and bandwidth. There doesn't seem to be an easy or perfect solution to the Sybil attack, but there are several approaches that can help. Different attacks will require different defensive strategies, so it's important that you tailor your defences appropriately. Some methods can be used to reduce the seriousness of these attacks on a system without it slowing down too much. The use of Sybil prevention techniques is not the only way to isolate malicious node behaviour, but they are worth considering. Techniques to prevent Sybil attacks are as under Table 1.

Table 1: Detection Schemes of Sybil Attack

S. No.	Mechanism Name	Architecture	Summary
1.	Secure Address Allocation [17]	Distributive	Sybil attacks are prevented by assigning unique addresses to each node.
2.	Robust Sybil Attack Detection [18]	Distributive	The same nodes with similar paths or patterns are often identical Sybil nodes.
3.	Lightweight Sybil Attack Detection [10]	Distributive	Nodes that join the network with a greater than threshold rate of speed are detected as Sybil nodes
4.	Received Signal Strength-based [7]	Distributive	In this method RSS value of nodes is visualized to confirm and supervise the behaviour of new node, in addition to their social acceptance.

3.1 Secure Address Allocation

To allocate a unique IP address to a node, it uses a partition function f(n) which is based on fundamental number theory principles. The partition function used in the field of graph theory is also called the state function. A seed represents the starting node or state, which is usually drawn with an arrow coming to it from nowhere. The different values these seeds generate will create a different sequence of integers within the following limits:

a) One of my colleagues is interested in your sequence and identified a possible problem: there appears to be a long gap between the numbers which is repeated in the sequence.
b) The likelihood of seeing the same number in a sequence is very less.
As counting numbers involve discerning allocated numbers or assigning different ones, this can stop the repetition of the same IP address [4]. Propagating key addresses throughout the network has its disadvantages. Particularly, if a malicious node wants to send spoof messages, they can do so because the seed value remains the same for all nodes. The secure address allocation detection technique is a more advanced form of address allocation. In this, these variables Authentication of seed value, Improvement, Exponential array, Priority are used to form a relationship.

3.2 Robust Sybil Attack Detection

Robust Sybil Attacks use the authentication mechanism for traffic manipulation[18]. For the sender to establish authenticity, packets are formed with the sender's own special key and they are also signed by nodes on their way to reach their destination. As long as the time and location of the packet are verified, it will be sent in a specific direction. With that, you can ensure that the data packets will reach their destinations without any hiccups. The similarity of the path is checked to detect Sybil nodes. These nodes are detected when their paths match in every location.

3.3 Lightweight Sybil Attack Detection

Nodes in a network usually share RSS (Received Signal Strength) with their neighbours and we can use the values to identify if nodes are legitimate and Sybil nodes. If the newest node has a low RSS and joins the network, we consider it to be a legitimate node [10]. Below flowchart depicts lightweight Sybil attack detection as a figure 2.

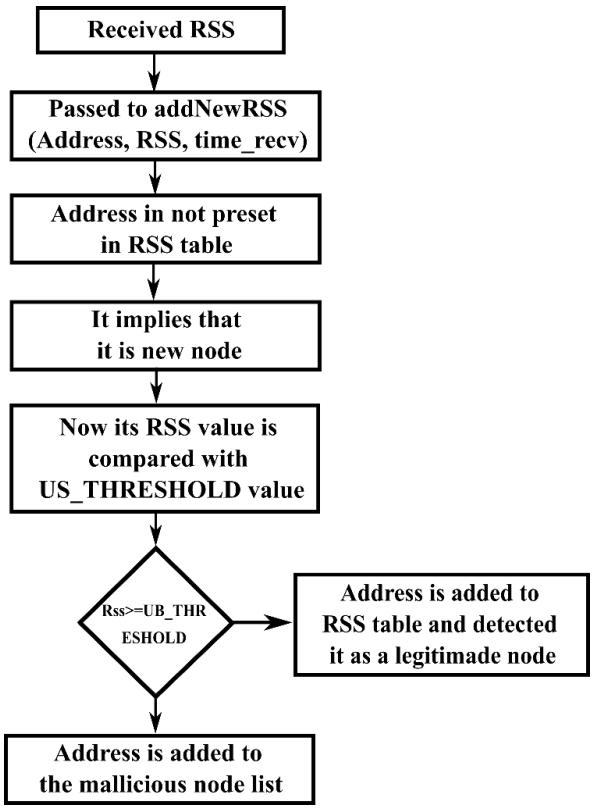

Figure 2: Detection of Lightweight Sybil Attack

3.4 Received Signal Strength-based

Wireless networks measure RSSI to determine the strength of an incoming signal. The RSSI method is simplest and commonly used for spotting fake nodes or "Sybil nodes". In Sybil attack fake identities are created or stolen in which the attacker gains control over multiple accounts and uses them to distort the perception of reality. A victim's account is taken over by the attacker, who then creates many other fake accounts under their control [7]. This strategy of creating many fake identities can be used to sway public opinion, cause disruption, or steal data. The RSSI value is an indicator of how strong a wireless signal is. It can be calculated using the following formula:

RSSI = 10*log(P/N), Where P is the power in watts received by a receiver antenna and N is the noise power density in watts per square meter.

RSSI values are a good indicator of a network's health. If RSSI values are low, it can indicate that the signal strength is being interfered with by something [7]. This may be caused by an object or a person in the area. RSSI values can also be used to find out if there is a problem with the antennae on the device, or if there is an issue with the Wi-Fi router. In order to properly maintain and protect your network from disaster, you need to know how to read and interpret RSSI values. The RSSI value is a measure of how strong the signal from your wireless device is relative to the signal from the access point that it's connecting to. The higher the dBm value, the stronger signal that node has relative to other nodes on that wireless network.

In order for an attacker to successfully carry out a Sybil attack, they need more than one wireless device with the same SSID name on the network. When this happens, devices will automatically connect to whichever access point has the strongest signal strength relative to their current position.

4 MITIGATION TECHNIQUES

Though there's no general answer to the Sybil attack, but various researchers have proposed various solutions for its detection and prevention. Some techniques can reduce the risk of attack from these vulnerabilities to a satisfactory level without a noticeable performance impact. They won't stop it happening altogether, but they will help a lot. Mechanisms to prevent Sybil attacks are:

4.1 Recurring Costs

This process is similar to using resource discovery, where tests take place at set intervals and the attacker has to pay a "cost" every time he wants to create an affinity between two identities on the network.

However, the vast majority of scientists endorsing this method worked on it with the computational power of their research labs. This is not enough to guarantee that it is impervious to attack; we need more evidence. The ability for malicious users to spend minimal cost can make it difficult to detect them [19]. One way to determine the economic value of an attack is to do a cost-benefit analysis from the attacker's perspective. The attack is only considered successful when the probability multiplied by benefit exceeds a pre-specified threshold [20]. They suggest recurrent costs for a single "identity" rather than a one-time fee will be more effective in deterring Sybil attacks.

4.2 Random Key Pre-distribution

Using this technique WSN can make secure connections and can communicate with each other secretly [21]. Each node is assigned a random set of keys that should share some common keys with their neighbouring nodes. This is done by using the assigned common key as a shared secret between communicating nodes. The goal of this proposal is to assign one identity with one key & then validate that key. Validation is when the

network can verify that your keys are valid. A forged Sybil identity won't fool a key validation test. Due to the fact that this false identity will usually lack access to any of the public/private keys associated with an attacker's network, it'll fail every test.

4.3 Location Verification

This technique is specifically used for ad hoc wireless networks. It relies on the fact that any single device projecting an identity can only be in 1 place at a time, so locations are verified using specific methods [22]. A single, physical attacker would need to have Sybil identities all log in to the same place or appear to converge at one point [19].

4.4 Resource Testing

To prevent Sybil attacks, it is common to limit computing resources. The idea is that each entity on the network should only have a set amount of computing power and that no one entity can take over more than its allotted share. One verification will be carried out to ensure that each ID has the same number of resources as what is matched by the device it is associated with. If data is changing, it will point to the possible location of the attacker. Systems like wireless sensor networks can be difficult to design because of the vast number of factors that you would need to think about. One important factor is storage space, but an attacker could have access to this which presents a new risk. One problem with sensor networks is that messages requesting verification may swamp the system making it useless for all other purposes. So, none of these are good choices.
Radio resource testing can be used to develop a feedback system for a wireless application [23]. This approach is based on two key assumptions concerning communication. One is that a device only has one radio and the other is that it cannot transmit & receive messages on more than one channel at any given time. More research needs to be done to see how reliable this strategy would be because many researchers believe this will help in the long run. By investing in these tests, businesses can substantially reduce their vulnerability to this type of attack.

4.5 Incentive-based Detection

Informant aims to incentivize Sybils for revealing information honestly. This is done in an economic incentive policy, which can be applied in any context, not just one application-specific domain [20]. The detective provides their security deposit and a certain reward to the target peer. Dutch auctions are commonly used to find the minimum number of peers needed to reveal a Sybil node. Unlike approaches that need physical tokens like radios and clocks, there's no need for this when doing a Dutch auction.

4.6 **Trusted Certification**

The very basic countermeasure to defend against Sybil attack is by issuing a certificate that can't be duplicated. Basically, it starts with a trusted authority that confirms that you are one with your identity on the internet. A centralized certificate authority can help you avoid communicating with new people every time [3]. The only way to completely get rid of Sybil attacks is a researcher certification. Although this approach seems like the perfect measure, there are many difficulties in laying down concrete implementations. A common concern is how an identity mapping system will establish who you are in cyberspace.

5. CONCLUSION

Sybil attacks, a type or false-positive attack, are one example. It creates fake identities to control the system. This is a common attack on reputation systems. Users create fake accounts to make false statements or to vote against content. This paper explores Sybil attacks, which can be deployed on different applications domains. To solve these attacks, a list has been created of possible detection and prevention strategies. A system that detects and blocks cheating is evaluated by four key metrics: detection rate, False positive rate, False negative rate and non-trustworthy rate. The long-term objective is to build a cost-effective and efficient surveillance network that minimizes false alarms while increasing detection. The future scope will primarily focus on increasing accuracy and reducing false positives.

REFERENCES

[1] D. S. David and T. J. George, "Identity-based Sybil attack detection and localization," *Artech J. Eff. Res. Eng. Technol*, vol. 1, pp. 94–98, 2020.

[2] A. M. Bhise and S. D. Kamble, "Review on detection and mitigation of Sybil attack in the network," *Procedia Computer Science*, vol. 78, pp. 395–401, 2016.

[3] "Sybil attack," *Wikipedia*. Feb. 26, 2022. Accessed: Mar. 07, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Sybil_attack&oldid=1074026148

[4] W. Wei, F. Xu, C. C. Tan, and Q. Li, "SybilDefender: A defense mechanism for sybil attacks in large social networks," *IEEE transactions on parallel and distributed systems*, vol. 24, no. 12, pp. 2492–2502, 2013.

[5] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A near-optimal social network defense against sybil attacks," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, 2008, pp. 3–17.

[6] V. Sujatha and E. M. Anita, "An efficient trust based method for Sybil node detection in mobile wireless sensor network," in *AIP Conference Proceedings*, 2018, vol. 2016, no. 1, p. 020138.

[7] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *2006 International symposium on a world of wireless, mobile and multimedia networks (WoWMoM'06)*, 2006, p. 5 pp. – 570.

[8] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7560–7572, 2015.

[9] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks," *International Journal of Computer Trends and Technology*, vol. 1, no. 2, pp. 9–17, 2011.

[10] R. Garg and H. Sharma, "Proposed lightweight Sybil attack detection technique in MANET," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 3, no. 5, pp. 7142–7147, 2014.

[11] Z. Yang, J. Xue, X. Yang, X. Wang, and Y. Dai, "VoteTrust: Leveraging friend invitation graph to defend against social network sybils," *IEEE Transactions on dependable and secure computing*, vol. 13, no. 4, pp. 488–501, 2015.

[12] R. Amuthavalli and R. S. Bhuvaneswaran, "DETECTION AND PREVENTION OF SYBIL ATTACK IN WIRELESS SENSOR NETWORK EMPLOYING RANDOM PASSWORD COMPARISON METHOD.," *journal of theoretical & applied information technology*, vol. 67, no. 1, 2014.

[13] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 492–503, 2009.

[14] C. Piro, C. Shields, and B. N. Levine, "Detecting the sybil attack in mobile ad hoc networks," in *2006 Securecomm and Workshops*, 2006, pp. 1–11.

[15] S. Capkun, J.-P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," *IEEE Transactions on Mobile Computing*, vol. 5, no. 1, pp. 43–51, 2005.

[16] G. Wang, F. Musau, S. Guo, and M. B. Abdullahi, "Neighbor similarity trust against sybil attack in P2P e-commerce," *IEEE transactions on parallel and distributed systems*, vol. 26, no. 3, pp. 824–833, 2014.
[17] H. Zhou, "Secure prophet address allocation for mobile ad hoc networks," in *2008 IFIP International Conference on Network and Parallel Computing*, 2008, pp. 60–67.
[18] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.
[19] B. Awerbuch and C. Scheideler, "Group spreading: A protocol for provably secure distributed name service," in *International Colloquium on Automata, Languages, and Programming*, 2004, pp. 183–195.
[20] N. B. Margolin and B. N. Levine, "Quantifying sybil attacks against network applications," *Technical Report 67 Dept. of Computer Science*, 2005.
[21] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 2, pp. 228–258, 2005.
[22] R. John, J. P. Cherian, and J. J. Kizhakkethottam, "A survey of techniques to prevent sybil attacks," in *2015 International Conference on Soft-Computing and Networks Security (ICSNS)*, 2015, pp. 1–6.
[23] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Third international symposium on information processing in sensor networks, 2004. IPSN 2004*, 2004, pp. 259–268.