# Security Issues and Sybil Attack in Wireless Sensor Networks

Pooja[1], Manisha[2], Dr. Yudhvir Singh[3]

[1]*M.Tech(CS) Student, AIM & ACT Department, Banasthali Vidyapith, Tonk, Rajasthan, India*
[2]*M.Tech(CS) Student, CS Department, Banasthali Vidyapith , Jaipur, Rajasthan, India*
[3] Associate Professor, *Computer Science & Engineering Department, U.I.E.T., M. D. University, (Rohtak), Haryana, India*

***Abstract:*** *Due to broadcast nature of Wireless Sensor Networks and lack of tamper-resistant hardware, security in sensor networks is one of the major issues. Hence research is being done on many security attacks on wireless sensor networks. Sybil attack is a particular harmful attack. When a node illegitimately claims multiple identities or claims fake id, is called Sybil attack.*
*This paper focuses on various security issues, security threats, Sybil attack and various methods to prevent Sybil attack.*

***Keywords:*** *Wireless Sensor Networks, Security, Sybil Attack.*

## 1. INTRODUCTION

A wireless sensor network (WSN) is a homogeneous system consisting of spatially distributed autonomous devices that use millions of tiny, inexpensive sensors to monitor physical or environmental conditions. The sensor networks have a wide variety of applications in a number of domains due to the availability of micro-sensors and low-power wireless communications. These sensor nodes will perform significant signal processing, computation, and network self-configuration to achieve scalable, robust and long-lived networks [1,20]. WSNs is a special class of ad hoc networks that operate with little or no infrastructure and have attracted researchers for its development and many potential civilian and military applications such as environmental monitoring, battlefield surveillance, and homeland security. In many important military and commercial applications, it is critical to protect a sensor network from malicious attacks, which presents a demand for providing security mechanisms in the network [2]. Therefore traditional security techniques in computer networks are not suitable for wireless sensor networks. Researchers have begun focusing on building a sensor trust model to solve the problems beyond the capability of traditional techniques and they have tried to address the challenges of maximizing the processing capabilities wireless sensor nodes while also securing them against attackers

## 2. WSN ARCHITECTURE

In a basic WSN architecture (fig 1), the many nodes are deployed to acquire measurements such as temperature, voltage, or even dissolved oxygen. The nodes are part of a wireless network administered by the gateway, which governs network aspects such as client authentication and data security. The gateway collects the measurement data from each node and sends it over a wired connection, typically Ethernet, to a host controller. There, software such as the NI LabVIEW graphical development environment can perform advanced processing and analysis and present your data in a fashion that meets your needs.


**Figure 1: WSN Architecture**

## 3. SECURITY ISSUES

There are usually several security issues which need to be considered during design of a security protocol. An effective security protocol should provide services to meet these requirements. The security requirements [1], [3], [4], [5], [6], [7] of a wireless sensor network can be classified as follows:

**Data Integrity**: Data integrity is to ensure that information is not changed in transit to send the sensor network into disarray [8]. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver [9]. Thus, integrity is an assurance that packets are not modified in transmission. This is a basic requirement for communications because the receiver needs to know exactly what the sender wants her to know. However, this is not an easy task in wireless communications. The standard approach for ensuring data integrity is through the use of message integrity code, etc.

**Data Authentication**: Data authenticity is an assurance of the identities of communicating nodes. WSN communicates sensitive data to help in many important decisions making. Thus, it is very important for every node to know that a received packet comes from a real sender. Otherwise, the receiving node can be cheated into performing some wrong actions [8]. Authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle) [9].

**Data Confidentiality:** Confidentiality is an assurance of authorized access to information. It is the ability of the network to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential [10, 8]. Thus, it ensures the protection of sensitive information and not revealed to unauthorized third parties. Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. In such applications, nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality [8].

**Data Freshness:** Even if confidentiality and data integrity are assured we also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. In order to ensure the freshness of packet, a timestamp can be attached to the packet. A receiving node can compare the timestamp in the packet with its own time clock and determine whether the packet is valid or not [9].

**Availability:** Availability is an assurance of the ability to provide expected services as they are designed in advance. It is a very comprehensive concept in the sense that it is related to almost every aspect of a network [8]. To ensure the availability of message protection, the sensor network should protect its resources (i.e., sensor nodes) from the unnecessary processing of key management messages in order to minimize energy consumption and extend the life of the network. The standard approach for keeping confidentiality is through the use of selective forwarding, multipath routing, etc.

**Self Organization:** A wireless sensor network requires every sensor node be independent and flexible enough to be self organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating [9].

**Flexibility:** Sensor networks will be used in dynamic battlefield scenarios where environmental conditions, threat, and mission may change rapidly. Changing mission goals may require sensors to be removed from or added to an established sensor node. Furthermore, two or more sensor networks may be fused into one, or a single network may be split in two .Key establishment protocols must be flexible enough to provide keying for all potential scenarios a sensor network may encounter [9].

**Time Synchronization:** Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. [8], proposes a set of secure synchronization protocols for sender-receiver (pair wise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization [9].

## 4. TYPES OF ATTACKS

Sensor networks are particularly vulnerable to several key types of attacks. Some of the critical

attacks [7], [11], are categorized as follows:

**Denial of Service Attacks:** Denial of Service (DoS) attack diminishes or eliminates a network's capacity to perform its expected function. It causes the jamming of a node or set of nodes. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently [9]. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization [8].

**Sybil Attack:** Sybil attack is defined as a malicious device illegitimately taking on multiple identities. Sybil attack [12], an adversary can "be in more than one place at once" as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and misbehavior detection.

**Wormhole:** Wormhole attack is a critical attack in which a malicious node picks the packets (or bits) at one location in the network and tunnels those to another location in the network which replays it locally. In the wormhole attack, an adversary (malicious nodes) eavesdrop the packet and can tunnel messages received in one part of the network over a low latency link and retransmit them in a different part. This generates a false scenario that the original sender is in the neighborhood of the remote location. The tunneling procedure forms wormholes in a sensor network [8].

**Sinkhole (Blackhole):** Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm and lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example) [13].

**Hello Flood:** Hello flood attack uses HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within radio range of the sender. In this type of attack an attacker with a high radio transmission range (termed as a laptop-class attacker) and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. This assumption may be false. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker. A laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbor, so that all the nodes will respond to the HELLO message and waste their energy [8].

## 4. SYBIL ATTACK

We define the Sybil attack (fig 2) as a malicious device illegitimately taking on multiple identities. We refer to a malicious device's additional identities as Sybil nodes. Sybil attacks occur when the one-to-one correspondence between an entity and its identity is violated.

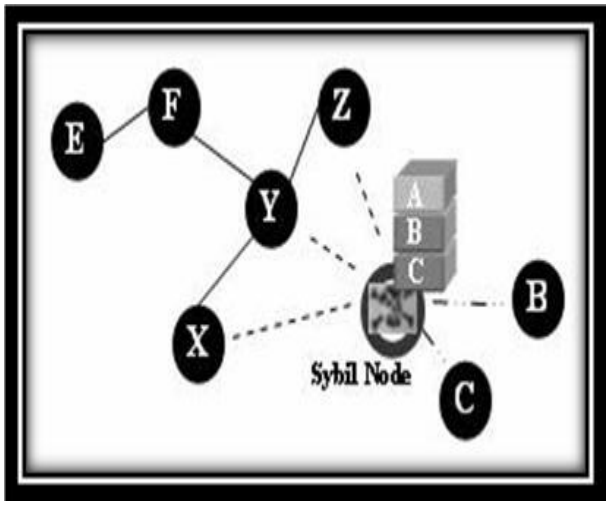


**Figure 2: Sybil Attack**

### 4.1 Sybil Attack Taxonomy

We propose three orthogonal dimensions: direct vs. indirect communication, fabricated vs. stolen identities, and simultaneity.

**Dimension I: Direct vs. Indirect Communication:**

**Direct Communication:** One way to perform the Sybil attack is for the Sybil nodes to communicate directly with legitimate nodes. When a legitimate node sends a radio message to a Sybil node, one of the malicious devices listens to the message. Likewise, messages sent from Sybil nodes are actually sent from one of the malicious devices [14].

**Indirect Communication:** In this version of the attack, no legitimate nodes are able to communicate directly with the Sybil nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil nodes. Messages sent to a Sybil node are routed through one of these malicious nodes, which pretend to pass on the message to a Sybil node [14].

**Dimension II: Fabricated vs. Stolen Identities:**

**Fabricated Identities:** In some cases, the attacker can simply create arbitrary new Sybil identities. For instance, if each node is identified by a 32-bit integer, the attacker can simply assign each Sybil node a random 32-bit value [14].

**Stolen Identities:** Given a mechanism to identify legitimate node identities, an attacker cannot fabricate new identities. For example, suppose the name space is intentionally limited to prevent attackers from inserting new identities. In this case, the attacker needs to assign other legitimate identities to Sybil nodes. This identity theft may go undetected if the attacker destroys or temporarily disables the impersonated nodes [14].

**Dimension III: Simultaneity:**

**Simultaneous:** The attacker may try to have his Sybil identities all participate in the network at once. While a particular hardware entity can only act as one identity at a time, it can cycle through these identities to make it appear that they are all present simultaneously [14].

**Non-Simultaneous:** Alternately, the attacker might present a large number of identities over a period of time, while only acting as a smaller number of identities at any given time. The attacker can do this by having one identity seem to leave the network, and have another identity join in its place. A particular identity might leave and join multiple times, or the attacker might only use each identity once [14].

### 4.2 Known threats posed by Sybil attack

**Distributed Storage:** Douceur observes that the Sybil attack can defeat replicated storage and redundancy mechanisms in Peer to Peer and sensor networks [12]. Data may be replicated across several nodes (distributed hash table) to achieve redundancy. However due to the presence of a malicious node assuming multiple identities, data may be stored on the identities generated by same node (data may be actually stored on same node).

**Multipath Routing:** Sensor nodes may use geographic routing to route the data to the base station. In a sensor network, data may be routed through multiple node disjoint paths (multipath routing) to achieve benefits like fault tolerance, increased bandwidth or improved security. However, a malicious node assuming multiple identities can be a part of multiple node disjoint paths which makes multipath routing ineffective.

**Data aggregation:** In a sensor network, in order to reduce the total number of messages sent and hence save energy, sensor readings from multiple nodes may be processed at aggregation points. By assuming multiple identities, a malicious node may be able to contribute to an aggregate many times. With enough Sybil nodes, an attacker may be able to completely alter an aggregate reading.

**Voting:** Depending on the number of identities a malicious node assumes, a malicious node may be able to determine the outcome of any vote. A malicious node can either claim that a legitimate node is misbehaving or Sybil nodes can vouch for each other.

**Fair-Resource Allocation:** A malicious node assuming multiple identities can obtain an unfair share of any resource. Consequently, a malicious node can cause Denial of service to legitimate nodes, and also give an attacker more resources to perform attacks.

**Misbehavior Detection:** Suppose that the network can potentially detect a particular type of misbehavior. It is likely that any such misbehavior detector has some false positives. **As** a result, it might not take action until it observes several repeated offenses by the same node. An attacker with many Sybil nodes could "spread the blame", by not having any one Sybil identity misbehave

enough for the system to take action. Additionally, if the action taken is to revoke the offending node, the attacker can simply continue using new Sybil identities to misbehave, never getting revoked himself.

### 4.3 Defenses against Sybil Attack

The Sybil attack was first described by Douceur in the context of peer-to-peer networks. He pointed out that it could defeat the redundancy mechanisms of distributed storage systems. Karloff and Wagner noted that the Sybil attack also poses a threat to routing mechanisms in sensor networks.
To defend against the Sybil attack, we would like to validate that each node identity is the only identity presented by the corresponding physical node. There are two types of ways to validate an identity.

**Direct Validation:** The first type is direct validation, in which a node directly tests whether another node identity is valid.

**Indirect Validation:** The second type is indirect validation, in which nodes that have already been verified are allowed to vouch for or refute other nodes.

Since the first analysis of the Sybil attack, several different approaches have been proposed to prevent or mitigate the attack

**Trusted certification**: Certification is by far the most frequently cited solution to defeating **Sybil** attacks [15]. It involves the presence of a trusted certifying authority (CA) that validates the one is to one correspondence between an entity on the network and its associated identity. This centralized CA thus eliminates the problem of establishing a trust relationship between two communicating nodes. Douceur has proven that trusted certification is the only approach that has the potential to completely eliminate Sybil attacks. However, trusted certification relies on a centralized authority that must ensure each entity is assigned exactly one identity, as indicated by possession of a certificate. In fact, Douceur offers no method of ensuring such uniqueness, and in practice it must be performed by a manual or in-person process. This may be costly or a create a performance bottleneck in large-scale systems. Moreover, to be effective, the certifying authority must ensure that lost or stolen identities are discovered and revoked. If the performance and security implications can be solved, then this approach can eliminate the Sybil attack[16].

**Resource testing**: Resource Testing is the most commonly implemented solution to averting Sybil attacks. The basic principle is that the quantum of computing resources of each entity on the network is limited. A verifier then checks whether each identity has as many resources as the single physical device it is associated with. Any discrepancy indicates the possibility of a compromised node. Storage, computation and communication were initially proposed as resources. However, for a system such as a wireless sensor network, an attacker might have storage and computation resources in large capacities compared to resource-starved sensor nodes. Alternatively, verification messages for verifying communication resources might flood the entire system itself. Hence, all three are inadequate choices for sensor network

**Radio Resource Testing:** Radio resource testing, proposed by Newsome et al. in, is an extension of the resource testing verification method for wireless sensor networks. The key assumptions of this approach are that any physical device has only one radio and that this radio is incapable of transmitting and receiving messages on more than one channel at any given time. As a concrete example, consider that a node wants to verify that none of its neighbors are Sybil identities. It can assign each of its n neighbors a different channel to broadcast some message on. It can then choose a channel randomly on which to listen. If the neighbor that was assigned that channel is legitimate, it should hear the message.

Resource tests have been suggested by many as a minimal defense against Sybil attacks where the goal is to reduce their risk substantially rather than to eliminate it altogether [17].

**RSSI-based scheme**: In [17, 18] Demirbas and Song introduce a method for Sybil detection based on the Received Signal Strength Indicator (RSSI) of messages. The cooperation of one additional node (and hence one message communication) is required for the proper functioning of this protocol. Upon receiving a message, the receiver will associate the RSSI of the message with the sender-id included, and later when another message with same RSSI but with different sender-id is received, the receiver would detect Sybil attack. A localization algorithm is used in this scheme. Sybil attacks can be detected with a completeness of 100% with few false positive alerts. Despite the fact that RSSI is unreliable and that transmissions via radio are non-isotropic, the use of ratios of RSSIs from multiple receivers solves this problem.

**Random Key Predistribution:** This technique enables nodes to establish secure links to other nodes in wireless sensor networks. In random key predistribution, a set of keys are assigned at random to a node enabling it to discover or

compute the common keys that it shares with its neighboring nodes. The key ideas are the association of the identity with the key assigned to a node and the validation of the key. Validation involves ensuring that the network is able to validate the keys that an identity might have. Consequently given a limited set of captured keys, there is little probability that an arbitrarily generated identity is going to work, for the keys associated with a random identity are not likely to have a significant intersection with the compromised key set, making it hard for the fabricated identity to pass the key validation.

**Location / Position Based Verification:** This solution is specific to Wireless ad hoc Networks. This technique makes use of the fact that any identities that are projected by any single physical device must be in the same location. Locations are verified using specific methods such as triangulation [19]. So for an attacker with a single physical device, all Sybil identities will be in the same place or will appear to move together. Tangpong et al. have proposed a solution based on the above strategy [17].

## Conclusion:

In this paper , we presented a concise survey on sensor networks security, security issues and attacks. Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. Then we discussed one of the major attack- Sybil attack and and establish a taxonomy of this attack by distinguishing different attack types. The definition and taxonomy are very important in understanding and analyzing the threat and defenses of a Sybil attack. We have also listed notable methods that have been proposed over time to tackle these attacks, their advantages and disadvantages.

## References

[1] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[2] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[3] E. Yoneki and J. Bacon, "A survey of Wireless Sensor Network technologies: research trends and middleware's role", Technical Report, 2005. http://www.cl.cam.ac.uk/TechReports, ISSN 1476-2986.

[4] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security - a survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press, 2007.

[5] L.L. Fernandes ,"Introduction to Wireless Sensor Networks Report", University of Trento. 2007,http://dit.unitn.it/~fernand/downloads/iwsn.pdf

[6] A.T. Zia, "A Security Framework for Wireless Sensor Networks", 2008, http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf

[7] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" Journal of Theoretical and Applied Information Technology, 2010, pp. 14-27.

[8] Shio Kumar 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- May to June Issue 2011, ISSN: 2231-2803.

[9] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti, **"**A Survey on Wireless Sensor Networks Security", **SETIT 2007** 4th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications March 25-29, 2007 – TUNISIA.

**[10]** M.J. Karmel Mary Belinda and C. Suresh Gnana Dhas, "A Study of Security in Wireless Sensor Networks", MASAUM Journal of Reviews and Surveys", Sept. 2009, vol. 1, Issue 1, pp. 91-95.

[11] H.K. Kalita and A. Kar, "Wireless Sensor Networks Security Analysis", International Journal of Next-Generation Networks (IJNGN), vol. 1, no. 1, Dec. 2009, pp. 01-09.

[12] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[13] Hemanta Kumar Kalita and Avijit Kar ,"WIRELESS SENSOR NETWORK SECURITY ANALYSIS", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

[14] James Newsome, Elaine Shi. Dawn Song and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", ***ZPSN'O4,*** April 26-27, 2004, Berkeley, California, USA. Copyright 2004 ACM 1-581 13-846-6/04/0004 ... $5.00.

[15] B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack, University of Massachusetts Amherst, Amherst, MA, 2006.

[16] H. Rowaihy, W. Enck, P. McDaniel, and T. La Porta. Limiting sybil attacks in structured p2p networks. In INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, pages 2596 {2600, may 2007}

[17] Nitish Balachandran, Sugata Sanyal," A Review of Techniques to Mitigate Sybil Attacks", Int. J. Advanced Networking and Applications Volume: Issue: Pages.

[18] Karlof, C., Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, Ad hoc Networks Journal (Elsevier) 1(2–3) (2003) 293–315.

[19] Athichart Tangpong, Managing Sybil Identities in Distributed Systems, Ph.D. Thesis at the Pennsylvania State University, May 2010.

[20] Jitender Singh, Yudhvir Singh; "A Review of Securiy in Wireless Ad hoc Networks"; International Conf. on Challenges in Networking & Future of e- Commerce, CNFE-05