Survey on Orthogonal Dimensions of Sybil Attack in Wireless Sensor Network

Purva Sharma
Computer Science & Engineering
JIET School of Engineering and Technology for Girls,
Jodhpur, India

ABSTRACT
Wireless Sensor Networks (WSNs) continue to grow and become widely used in many applications in military, ecological, home automation and health-related areas. Due to distributed nature of sensor networks security becomes fundamental requirement for communication among sensor nodes. The inclusion of wireless communication among various sensor nodes suffers from various types of security threats. The intent of this paper is to analyze the Sybil attack for wireless sensor networks (WSN). To sense the inflection of the Sybil attack, analyze three orthogonal dimensions: direct v/s indirect communication, fabricated v/s stolen identities, and simultaneous and non-simultaneous and corresponding defense mechanisms for wireless sensor networks.

Keywords
WSN, Sybil attack, Orthogonal dimension.

1. INTRODUCTION
Wireless sensor networks are grids or networks composed of large number of immobile tiny sensor nodes, running separately, all of which have sensing capabilities that are used to detect, monitor and track various 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 connections [1]. Sensor nodes have minimum computational and storage resources, so it can easily be assaulted [2]. Various types of attacks such as selective forward attacks, wormhole attacks, sinkhole attacks and Sybil attack can be present in a sensor networks while communication takes place among the nodes. An especially injurious attack against WSNs is the Sybil attack. Sybil attack is where a node illegitimately claims multiple identities [2]. The interesting feature of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks, while the routing criteria and wireless sensor network modeling are getting much precedence, the security concerns are yet to get pervasive focus. In this paper, present the crucial parameters, three orthogonal dimensions: direct v/s indirect communication, fabricated v/s stolen identities, and simultaneous and non-simultaneous that requires extensive investigations and explore the security issues for WSNs.

2. ATTACKS IN WIRELESS SENSOR NETWORKS
Most of the wireless sensor network routing protocols are convenient and straightforward. Because of this reason they are permeable to attacks. In this section of the paper, attacks on sensor network routing have been discussed. The attacks which act on the network layer are called routing attacks. These network attacks are occurs while routing the information among various nodes of sensor network. There are different types of routing attacks in WSNs which can be categorized as following:

- Spoofed, altered, or replayed routing information,
- Selective forwarding,
- Sinkhole attacks,
- Sybil attacks,
- Wormholes,
- HELLO flood attacks,
- Acknowledgement spoofing [3].

2.1 Spoofed, altered and replayed routing information
This attack is a straight attack against a wireless sensor network routing protocol, is to aim the routing information transferred among the nodes. These types of attacks, in which every node acts as a router, can directly modify the routing information among the nodes of wireless sensor network. By spoofing, replaying or altering network routing information between two nodes, adversaries may be able to generate various stages that arise various problems, these problems are as following:

- Create routing loops.
- Attract or repel network traffic.
- Extend or shorten source routes.
- Generate false error messages.
- Partition the network.
- Increase end-to-end latency [3].

2.2 Selective forwarding attack
Selective forwarding attacks are typically most dominant when the attacker is explicitly included on the way of a data stream that flow in wireless sensor network. In sensor networks it is assumed that nodes faithfully forward received information. But some conciliated node might ignore to forward packets, however nearby nodes might start using other route.

When node have to alienate the packets from multiple paths in routing, in this duration, any of the node may be settled with the attacker node, suppose if the node alienated the packets by multiple nodes, in this duration attacker could obtain the packets and which has dropping and delivering the packets choicely, Therefore it could not broadcast the packets to accurate path, at last it would not reach the accurate destination.

2.3 Sinkhole
Sinkhole attack is traffic attractive attack that number of attacker nodes will be covers the certain region in sensor network by wrongly manipulated information. In this attack, a malicious node acts as a black hole to attract all the traffic in

the sensor network [4]. Originally, sinkhole attack can affect even the nodes those are especially away from the base stations.

In a sinkhole attack, the adversary's goal is to forage nearly all the traffic from a particular area through a conciliated node, creating a sinkhole with the adversary at the origin. Because network nodes on, or near, the route that packets follow have many opportunities to tamper with application information, sinkhole attacks can able many another attacks (selective forwarding, for example) [3].

2.4 Wormhole

Wormhole attack is a hazardous attack to wireless sensor network in which the attacker records the packets at one place of the network over a low-latency path and grants those to another place. Wormhole attack is a valuable threat, because it could be executed even at the initial stage when the sensors start to search the neighboring information. The convenient phenomenon of wormhole attack is a single node established between two other nodes dispatching messages between the two of them.

An adversary situated close to a base station may be able to completely disrupt routing by creating a located wormhole. An emulator could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole [3].

2.5 HELLO flood attack

HELLO flood attack is a modern attack against sensor networks. In wireless sensor networks most of the protocols has a node to broadcast HELLO packets to announce themselves to their nearby nodes, and a receiver network node getting such a packet may imagine that it is within normal range of the sender node. For example, an adversary advertising a very high-quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this path, but those network nodes sufficiently far away from the adversary would be sending packets into oblivion [3].

In this attack, HELLO packets are used as a tool to convince the sensors in WSNs. An attacker has a high radio transmission range and processing power to send HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN [5]. The sensors are thus affected that the opponent is their neighbor.

2.6 Acknowledgement spoofing

Various wireless sensor network routing algorithms believe on implicit or explicit link layer receipts. Due to the implicit broadcast channel, an adversary can spoof link layer receipts for ''overheard'' packets addressed to nearby nodes. The target of that includes convincing the sender that a weak link is strong or that a dead or disabled node is alive. [3] Illustration, a routing protocol for sensors may choose the next hop in a path using link reliability.

2.7 Sybil Attack

Sybil attack is an attack in which a solo node operates as multiple identities to other nodes in the wireless sensor network. Sybil attacks also pose a significant threat to geographic routing network protocols. Location based routing often requires networking nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets [3].

Sybil attack attempts to reduce the security, integrity of data and resource utilization that the distributed algorithm tries to accomplish. Sybil attack can be performed for attacking the fair resource allocation, misbehavior detection, distributed storage, voting, data aggregation and routing mechanism [4].

In this paper, tell about the Sybil attack in wireless sensor network, Firstly, presents the introduction of Sybil attack, defense mechanisms against the Sybil attack and lastly three orthogonal dimensions.

3. INTRODUCTION OF SYBIL ATTACK

Sybil attack is an attack in which a solo node operates as multiple identities to other nodes for wireless sensor network routing protocol. Sybil attack is an exclusively noxious attack against wireless sensor and ad hoc networks, where a network node never legitimately claims for multiple identities. The node responds itself to make many copies of our self to confuse and disrupt the sensor network. There are two types of attack: internal and external attack. External attacks can be prevented by any security mechanism. Internal attack should be prevents by one to one mapping between identity and entity, but Sybil attack overleaps this one-to-one mapping by creating multiple identities.

This attack is very vulnerable to wireless sensor network because this nature could be gateway of any other attacks such as wormhole, sinkhole, selective forwarding etc… This attack makes more threatening problems in distributed storage, voting and resource allocation, same as appeared in wireless sensor network. But due to their limitation of sensor node, could not directly implement the traditional security concepts in to their sensor network [6].
The Sybil attack defined as an inimical device illegitimately receiving on multiple identities. An inimical device's additional identities as Sybil nodes to attack on wireless sensor network algorithms. Sybil attacks occur when the one-to-one relationship between an entity and its identity is intruded.

In figure 1, Sybil Attack shows that a node has multiple identities of other nodes. A node which has a multiple identities called Sybil node. In this figure indicates that node A act as node B and node C also, so node A is called a Sybil node. When information is transmitting in wireless sensor network through routing algorithm to node B and node C, due to Sybil attack it is transmitted to Sybil node A.

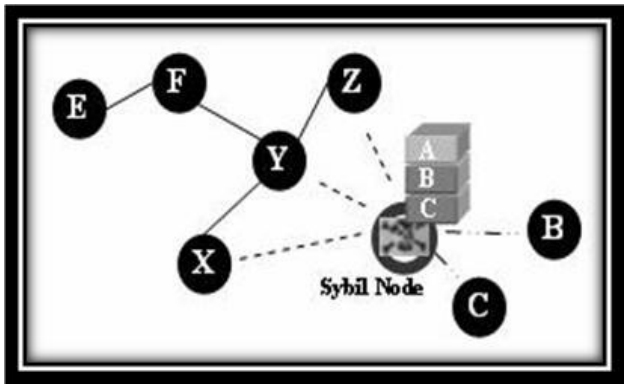

Fig 1: Sybil Attack [1]

4. DEFENSE MECHANISMS AGAINST THE SYBIL ATTACK

To protect against the Sybil attack, validate the identity of each node is only identity presented by the compatible physical node. There are two methods to validate an identity of a node.

Direct Validation: In this method of validation a node directly checks the identity of another node whether it is valid or not.

Indirect Validation: In this method of validation a node indirectly checks the identity of another node whether it is valid or not. Validity of that node checks by other means such as devices, resources, and another node that are not included in WSN.

There are various different techniques have been proposed to inhibit or reduce the attack.

4.1 Trusted Certification

Certification is most popular referred solution to protect sensor network against Sybil attacks. 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 [1]. Trusted certification depends on a centralized authority that must assure each node is assigned a fix unique identity.

4.2 Resource Testing

Resource Testing is mostly referred defense mechanisms against the Sybil attack. This mechanism is solution to averting Sybil attacks. The basic theory of resource testing is that the amount of computing resources of each entity on the sensor network is confined. A verifier then checks whether each identity has as many resources as the single physical device it is associated with [1]. In wireless sensor network, an attacker might have storage, computation and communication resources in great efficiency compared to resource-famished sensor nodes.

4.3 Radio Resource Testing

Radio resource testing is a defense mechanism which is an extension of the resource testing verification method for sensor network routing algorithms. The basic theory of radio resource testing are that any physical resource has only one radio and this radio is unable for transmitting and receiving information on more than one channel at any given time.

Consider that a node wants to verify that none of its neighbors are Sybil identities. It can assign each of its neighbors a different channel to broadcast some messages on. It can then choose a medium randomly on which to listen. If the neighbor that was assigned that channel is legitimate, it should hear the message. Let‘s’ be the total number of the nodes ‘n’ be the number of Sybil networking nodes. The possibility of detecting the Sybil node is s/n [2].

4.4 RSSI-based scheme

RSSI is a method for Sybil attack detection based on the Received Signal Strength Indicator (RSSI) of information. The collaboration of one additional node is expected for the proper working of this sensor network protocol. Upon receiving a message, the receiver will associate the RSSI of the message with the sender-id associated, and later when other message with similar RSSI but with different sender-id is received, the receiver would detect Sybil attack [1].

4.5 Random Key Pre-distribution

To protect the Sybil attack, random key pre-distribution method has a set of keys that are assigned randomly to the nodes of network, authorizing it to search or count the generic keys that it shares with its neighboring nodes. The basic theory of random key pre-distribution is that association of the identity with the key assigned to a node and the accreditation of the key. Accreditation involves assuring that the wireless sensor network is efficient to confirm the keys that an identity might have.

4.6 Location / Position Based Verification

Location based verification is a promising solution to protecting against the Sybil attack on wireless sensor network (WSN). This technique plays use of the fact that the sensor nodes are immobile once these nodes are deployed in network. In this technique, the sensor network confirms the physical location of each node. Sybil nodes can be detected using this approach because they will appear to be at exactly the same position as the malicious node that generates them [2].

5. ORTHOGONAL DIMENSIONS

In organization of wireless sensor network to protect the routing protocols against the Sybil attack as an inimical device illegitimately receiving on multiple identities, it is essential to recognize the various taxonomies To grasp the circumvolution of the Sybil attack, analyze three orthogonal dimensions: direct v/s indirect communication, fabricated v/s stolen identities, and simultaneous and non-simultaneous and corresponding defense mechanisms for wireless sensor networks.

5.1 Direct and Indirect Communication

In direct communication, the Sybil attack is completed when the Sybil nodes communicate directly with legitimate networking nodes. When not an illegitimate node transmits a radio message to a Sybil networking node, one of the malicious resource listens to the message. Likewise, messages sent from. Sybil nodes are actually sent from one of the malicious devices [7].

5.1.1 Direct Defense Mechanisms:

This is observed that the direct communication is detected by the radio resource testing defense mechanism.

In indirect communication, the Sybil attack is completed when the Sybil nodes communicate indirectly with legitimate nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil networking nodes. Messages transmit to a Sybil networking node are routed through one of these malicious nodes, which pretend to pass on the message to a Sybil node [7].

5.1.2 Indirect Defense Mechanisms:

This is observed that the indirect communication is detected by the resource testing defense mechanism and location based verification.

5.2 Fabricated and Stolen Identities

In wireless sensor network, there are two methods for a Sybil node to obtain an identity. Sybil node can fabricate a new identity, or it can steal an identity from a node in network.

In fabricated identities, the attacker can simply create arbitrary new Sybil identities. For instance, if each node is identified by a 32-bit integer value, the attacker can simply define each Sybil node a random 32-bit value. Or it creates a new identity

for itself based on the identities of the legitimate networking nodes, that is, if illegitimate networking nodes have an ID with length of 32 bit integer value, it randomly generates ID of 32 bit integer value. These networking nodes have fabricated identities [7].

5.2.1 Fabricated Identities Defense Mechanisms:

In this, it is observed that to detect fabricated identities the defense mechanism random key pre-distribution and RSSI-based scheme is used.

Stolen identity is a mechanism to identify legitimate node identities, new identities cannot fabricated by an attacker. In stolen identities, identifies legitimate identities by attacker and then uses these identities. If the networking node whose identity has been stolen is destroyed than the attack may go unidentified. When the same identities are used many times in the same places is identity replication [7].

5.2.2 Stolen Identities Defense Mechanisms:

In this, it is observed that to detect stolen identities the defense mechanism random key pre-distribution and trusted certificate verification is used.

5.3 Simultaneous and non-simultaneous attack

In simultaneous attack, all the Sybil identities participate in the network at a time. Since only single identity appears at a same time, It appear simultaneous will make by cycling through identities practically [7].

5.3.1 Simultaneous Attack Defense Mechanisms:

I observe that the simultaneous attack is detected by location based verification.

In non-simultaneous attack, alternately the attacker might present a large number of identities over a time period, while only acting as a minimum number of identities at any particular given time. To do this the attacker only having one identity seems to leave the network, and have another identity join in its location. A special identity might leave and join multiple times, or the attacker might only use each identity once [7].

5.3.2 Non-Simultaneous Attack Defense Mechanisms:

I observe that non-simultaneous attack is detected by radio resource testing defense mechanism.

Orthogonal Dimensions	**Defense Mechanism**
Direct Communication	Detected by the radio resource testing defense mechanism.
Indirect Communication	Detected by the resource testing defense mechanism and location based verification.
Fabricated Identities	Detected by the random key pre-distribution and RSSI-based scheme
Stolen Identities	Detected by the random key pre-distribution and trusted certificate verification
Simultaneous attack	Detected by the location based verification
Non-simultaneous attack	Detected by radio resource testing defense mechanism

Table1: Observation Table for Orthogonal Dimension

6. CONCLUTION

Each of the defense mechanism against orthogonal dimensions of the Sybil attack in WSNs has different tradeoffs. It is analyzed that most defense mechanisms are not capable of defending against all of orthogonal dimensions. The radio resource verification defense mechanism against the Sybil attack may be breakable with custom validation and radio hardware may be valuable in terms of energy. Position verification can only put a bound on the number of Sybil nodes an attacker can generate unless it is able to very precisely verify node positions. Node registration requires human work in order to securely add nodes to the network, and requires a way to securely maintain and query the current known topology information.

7. REFERENCES

[1] Pooja1, Manisha, Dr. Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks," International Journal of P2P Network Trends and Technology- Volume3Issue1- 2013, ISSN: 2249-2615.

[2] S.Sharmila, G Umamaheswari, "Detection of Sybil Attack in Mobile Wireless Sensor Networks," International Journal of Engineering Science & Advanced Technology, Volume-2, Issue-2, 256 – 262, ISSN: 2250–3676.

[3] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," 1570-8705/$ - see front matter 2003 Elsevier B.V. All rights reserved. doi:10.1016/S1570-8705(03)00008-8.

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges ", Feb. 20-22, 2006 ICACT2006, ISBN 89-5519-129-4.

[5] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, ISSN 1947-5500.

[6] Abirami.K, Santhi.B, Sybil attack in Wireless Sensor Network, Abirami.K et al., International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013, ISSN: 0975-4024.

[7] Manjunatha T. N1, Sushma M. D2, Shivakumar K. M3, "Security Concepts and Sybil Attack Detection in Wireless Sensor Networks," Volume 2, Issue 2, March – April 2013, ISSN-2278-6856.