Secure Localization: The Review on Possible Attacks of WSN and Their Remedy

Kalyani N Neve
Assistant Professor

Sweta G Phegade
Assistant Professor

Deepali Y Kirange
Assistant Professor

Abstract

The entire field of wireless network security is vast and in an evolutionary stage. Secure localization of nodes in a Wire- less Sensor Network (WSN) is an important research subject. When WSNs are deployed in hostile environments, many attacks happen, e.g., wormhole, sinkhole and Sybil attack. Some of them are attack on nodes and some of them are attack on information. So it is necessary to know about all possible attacks and their remedy. In this paper, we depict the attack model and talk about different types of node and doable common attacks against secure localization i.e. attacks on nodes and attacks on information. As well as we do the survey and try to find out the solutions on each attacks.

Keywords: *Wireless Sensor Network, Localization, attack on nodes, attacks on information*

1. Introduction

Localization is one of the most important topics in Wireless Sensor Networks (WSNs) .Before discussing secure localization problems, it is essential to take a look at some general concepts used in the localization process. Basically, there are two categories of sensor nodes: unknown nodes and anchor nodes. Unknown nodes in the network have no knowledge of their positions and no special hardware to acquire the positions. There are many fundamental techniques that are used to position the unknown nodes such as geographical routing, geographic key distribution, and location-based authentication. Anchor nodes, also called beacon nodes, in fact, their positions are obtained by manual placement or additional equipments such as GPS (Global Positioning System).

Therefore, unknown nodes can use localization information of anchor nodes to localize themselves.

2. Types of Localization

Usually, the localization process can be divided into two steps: 1) information acquisition and 2) position determination.

2.1. Information acquisition

Roughly speaking, existing localization schemes of WSNs are classified into two categories: range-based schemes, and range-free schemes. For range-based localization schemes, the distance or angle information is measured by RSSI (Received Signal Strength Indicator), TOA (Time of Arrival), Time Difference on Arrival (TDOA) and AOA (Angle of Arrival). For range-free localization schemes, the localization is realized based on network connectivity or other information, which can be obtained by DV-Hop, Convex Optimization and MDS-MAP.

2.2. Position determination

Location determination schemes have two categories: 1) terminal-based schemes and 2) infrastructure-based schemes. In terminal-based schemes, the unknown node localizes itself. After collecting available information about distances and positions of anchor nodes, the position of an unknown node can simply be computed by trilateration, multilateration, and triangulation. In infrastructure-based schemes, reference nodes including trusted neighbour nodes, mainly anchor nodes to localize the unknown node. Adversaries can attack localization in both two steps. The goal of the adversary is to make the unknown nodes obtain false positions, by compromising normal nodes to send false localization information, or pretend to be a legitimate node to forge, modify or replay signals. Thus, security measures are needed to make the estimated positions still correct under attacks.

Secure localization can be considered from two aspects. First, we discuss the attacks on nodes, since an attacker can compromise or pretend to be an unknown or an anchor node to interfere with localization process. Therefore, we need secure node authentication (SNA). Second, we discuss the attacks on information, since an attacker can forge, modify or replay localization information to make the estimated positions incorrect. Thus we need to detect the correctness of localization information.

3. Attack Model

Localization process can be attacked in a number of different ways. When an attacker attacks on victim's computer, the original connection is broken down and the new connection is established between server and victim's computer (victim is totally unaware about these connections) and all the information exchanged between them is passed through the attacker's PC (as shown in fig 1). Localization process can be attacked in a number of different ways Researchers have addressed a set of known attacks. Here we give the example to demonstrate the attacks. As an example fig (2) illustrates the how many ways the attacker attacks on e-mail system. The known attacks can be divided into two categories: external and internal attacks. The adversary is external if it is outside the WSN and implements malicious behaviours without right cryptographic key. Otherwise, the adversary is internal, in which case the adversary controls one or more fraudulent nodes. In this paper, the attacks are classified into two categories: A) attacks on nodes and B) attacks on information.

3.1. Attacks on Nodes

In this paper, malicious nodes contain attackers and compromised nodes. An attacker is an external node which intrudes into the WSN. A compromised node is normal node (an unknown or an anchor node) in the WSN compromised by the attacker. Attacks on nodes are listed as follows:

3.1.1. Compromise:
In many applications, sensor nodes are deployed in large numbering are as that cannot be constantly monitored. In these cases, the attackers can secretly enter the network and compromise individual nodes. Node compromise is the most fundamental attack in WSN that leads to other kinds of attacks. It occurs when an attacker gains control of a node in the WSN. Normally, compromised nodes can be obtained by the following methods: attacker scan extract cryptographic secrets, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker. These attacks are similar to physical attacks across some respects.

With compromised node, an attacker can alter the node to listen information in the WSN, revoke legitimate nodes, input malicious data, and cause internal attacks, e.g., DoS attack.

Remedy: Wood and Stankovic propose approaches to make the nodes' physical packaging tamper proof .The success of this strategy, however, depends on how accurately and completely designers consider potential threats at design time, the resources available for design, construction, testing, cost effectiveness, and attacker abilities among others.
Although such approaches are obviously welcome, there cannot be a panacea for defences against physical attacks.

The problem is arises because of the number of sensor nodes are in the network and we cannot monitor them at a time. If we place the some sensor nodes (which works like a monitors) in the network to keep the record of all nodes in the network then may be the problem of compromising of nodes will be overcome. It will keep the records like how many nodes in the network? Which information is going to exchange? And that information is received by the node in the network or by attacker.

3.1.2. Replication: If an adversary manages to capture a node and extract the authentication/encryption keys, it can produce a large number of replicas having the same identity (ID) from the captured node and integrate them into the WSN at chosen locations, which is called the node replication attack. Since the credentials of replicas are all the clones from the captured nodes, the replicas can be considered as legitimate members of the network. It is always assumed that the adversary cannot create new IDs for replicated nodes, since otherwise the attackers will have to create the corresponding security information (keys, codes, etc.), which is very difficult and even infeasible in most cases. Once the adversary replicates one or more sensor nodes, it can execute the malicious operations. For instance, the replicas may inject false localization information into the WSN.

Remedies: We proposed a neighbour based detection scheme to cope with replication attacks. The scheme features distributed detection and takes node mobility into account. It harnesses the dynamic observations of the neighbours of a claimer node and avoids the protocol iterations typically found in distributed detections.

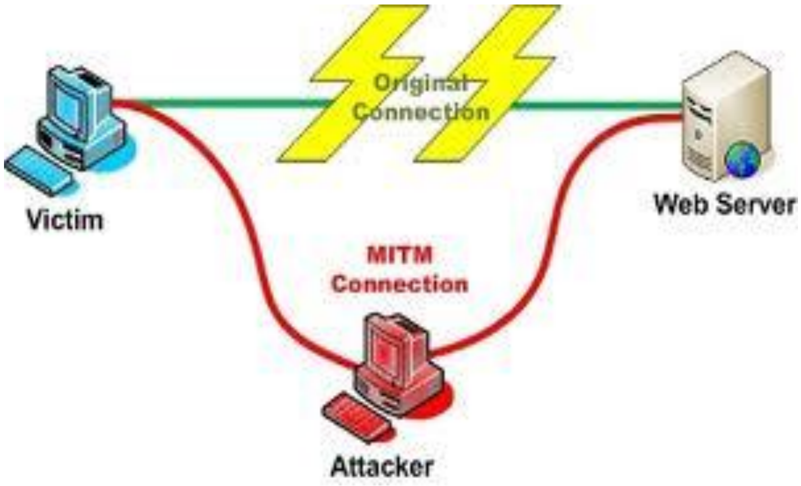

Fig 1: Attacker's attacks on victim's PC

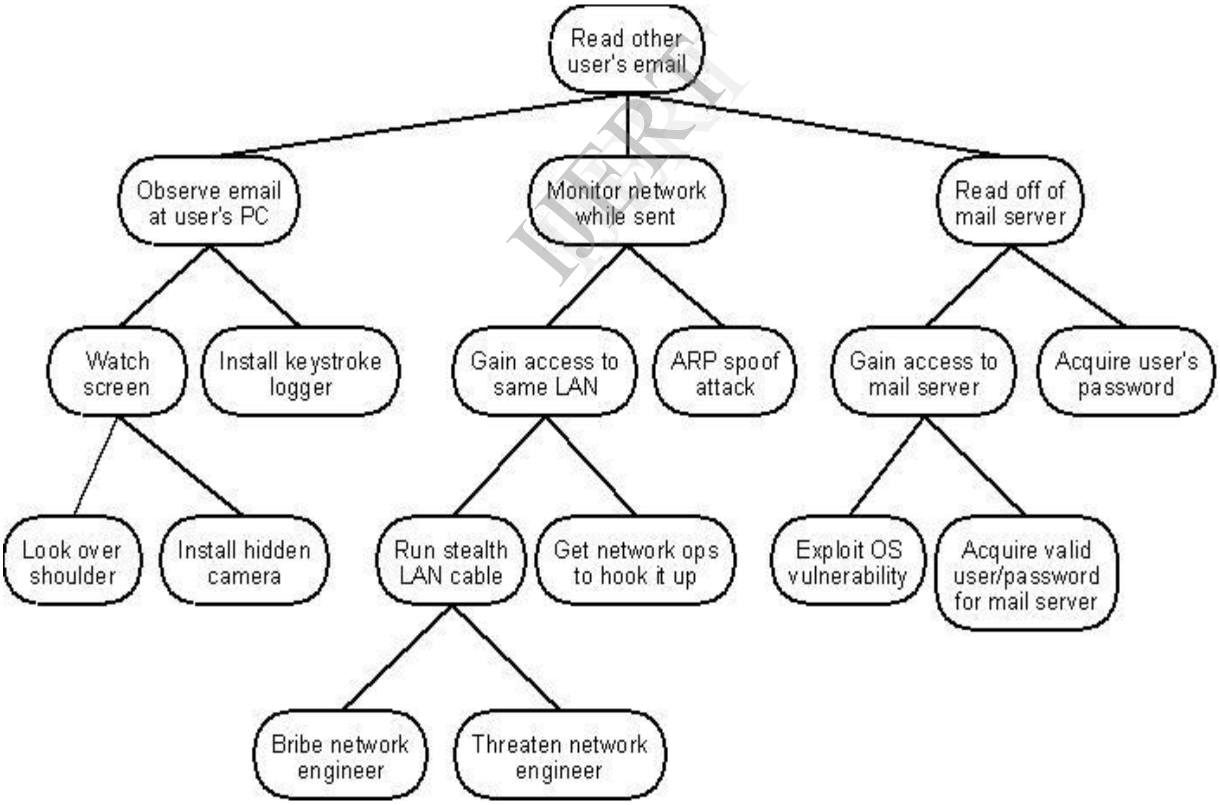

Fig 2: Many ways of attackers to attack on E-mail system.

3.1.3. Impersonation: An *impersonation attack* is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.

One form of node impersonation attack is the Invisible Node attack, and the other one is the Stolen Identity attack, as shown in Figure 3.

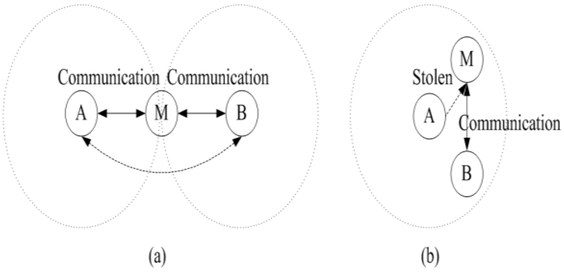

Fig 3. Node impersonation attack: (a) the Invisible Node attack. (b) the Stolen Identity attack.

The Invisible Node attack: Malicious node M simply stands between two nodes A and B that are not in direct range. The invisible node M silently repeats the communication between nodes A and B, which misleadingly assume that nodes A and B communicate directly. In this way, the malicious node succeeds in impersonating node A to node B and vice versa.

The Stolen Identity attack: The malicious node M succeeds in stealing all the authentication credentials from a legitimate node A, such as the certified signature keys. If the malicious node outraces the legitimate node in updating the stolen credentials, then the credentials of the legitimate node will not be valid anymore. Thus, only the malicious node will be able to communicate with node B. This kind of attack is not just a matter of stealing a nodes identity, but also a matter of abusing the trust relationships that other parties may have had established with the legitimate node.

3.1.4. Sybil attack: In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network. The incorrect information can be a variety of things, including position of nodes, signal strengths, making up nodes that do not exist. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but he should only be able to do so using the identities of the nodes he has compromised. Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor network.

Remedy: The mechanisms to prevent against Sybil attacks are to utilize identity certificates. The basic idea is very simple. The setup server, before deployment, assigns each sensor node some unique Information. The server then creates an identity certificate binding this node’s identity to the assigned unique information, and downloads this information into the node. To securely demonstrate its identity, a node first presents its identity certificate, and then proves that it possesses or matches the associated unique information. This process requires the exchange of several messages. Merkle hash tree can be used as basic means of computing identity certificates. The Merkle hash tree is a vertex-labeled binary tree, where the label of each non-leaf vertex is a hash of the concatenation of the labels of its two child vertexes. The primary path of a leaf vertex is the set of vertexes on the path from the leaf to the root of the tree. The authentication path consists of the siblings of the vertexes on this primary path. Given a vertex, its authentication path, and the hash function, the primary path can then be computed, up to and including the root of the tree. This computed value of the root can then be compared with a stored value, to verify the authenticity of the label of the leaf vertex.

3.1.5. Wormhole attack: In a wormhole attack, an attacker records a packet or individual bits of a packet at one location in the network. Then, it tunnels the packet (possibly selectively) to another location and replays it. The tunnel can be established in many different ways, for example, through an out-of-band channel, packet encapsulation, high-powered transmission, packet relay and protocol deviations. In localization process, the attack may tunnel totally different and erroneous localization information. One node in the network (sender) sends a message to the another node in the network (receiver node).Then the receiving node attempts to send the message to its neighbours. The neighbouring nodes think the message was sent from the sender node(which is usually out of range), so they attempt to send the message to the originating node, but it never arrives since it is too far away. Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover neighbouring information. Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

Remedy

The mechanism to combat the wormhole attack include, DAWWSEN , a proactive routing protocol based on the construction of a hierarchical tree where the base station is the root node, and the sensor nodes are the internal or the leaf nodes of the tree. A great advantage of DAWWSEN is that it doesn't require any geographical information about the sensor nodes, and doesn't take the time stamp of the packet as an approach for detecting a wormhole attack, which is very important for the resource constrained nature of the sensor nodes.

3.2. Attacks on Information

In the localization systems, unknown nodes always use the localization information of anchor nodes to localize themselves. The target of malicious nodes is usually to make localization information incorrect. Attacks on information are listed as follows:

3.2.1 Selective Forwarding attack

It is a situation when certain nodes do not forward many of the messages they receive. The sensor networks depend on repeated forwarding by broadcast for messages to propagate throughout the network.

Remedy: Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

3.2.2. False or Malicious Node

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network.

Remedy: This attack basically should be checked in the Routing layer itself. Details pertaining to the preventive measures for false node" attack are out of the scope of this paper.

3.2.3. Hello flood attacks

The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent. All messages now need to be routed multi-hop to this parent, which increases delay.

Remedy

This can be avoided by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop.

4. Conclusion

All of the previously mentioned security threats, the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, serve one common purpose that is to compromise the integrity of the network they attack. Also In the past, focus has not been on the security of WSNs, but with the various threats arising and the importance of data confidentiality, security has become a major issue. Although some solutions have already been proposed, there is no single solution to protect against every threat. In our paper we mainly focus on the attack models as well as different types of attacks. And various security threats in WSN and their remedies.

5. References

[1] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter State- less Routing for wireless networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Network, 2000, pp. 243–354.

[2] D. Liu and P. Ning, "Location-based pairwise key estab- lishments for static sensor networks," in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, pp. 72–82.

[3] S. U. Sastry, N. and D. Wagner, "Secure verification of location claims," in Proceedings of the 2nd ACM workshop on Wireless security, September 2003.

[4] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor networks: a survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, August 2008.

[5]http://www.google.co.in/search?q=attack+on+node&source=lnms&tbm=isch&sa=X&ei=2GQIUpvKE4jZrQeGqoGICQ&ved=0CAcQ_AUoAQ&biw=1025&bih=451

[6]http://www.springerreference.com/docs/html/chapterdbid/317115.html

[7] P. Bahl and V. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," in Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 21, 2000, pp. 755–784.

[8] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The anatomy of a context-aware application," in Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 1999, pp. 59–68.

[9] L. Girod and D. Estrin, "Robust range estimation using acoustic and multimodal sensing," in Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2001, pp. 1312–1320.

[10] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AoA," in Proceedings of the Twenty-Second

Annual Joint Conference of the IEEE Computer and Communications
Societies, vol. 3, April 2003, pp. 1734–1743.
[11] ——, "Ad hoc positioning system (APS)," in Proceedings
of the 2001 IEEE Global Telecommunications Conference
of the IEEE Communications Society, vol. 5, 2001, pp.
2926–2931.
[12] Wireless Sensor Networks: An Overview on its Security
Threats, *IJCA Special Issue on "Mobile Ad-hoc Networks"*
MANETs, 2010