Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) – May 2015
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Detection of Diffusion in Attacks

R . Sakthi Bharathi

Dept. of Computer Applications, S.A Engineering College, Chennai
sakthibharathi100@gmail.com

Abstract— A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations [2]. Internal attackers (Insiders) that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures [3]. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks. This paper is on specific internal attack wormhole attack and a LOCALIZED FAULTY DETECTION ALGORITHM used to identify faulty nodes in sensor with the help of neighboring sensor and by using two predefined threshold values Θ1, Θ2 [4].

Keywords— *Sensor Security; Algorithm, Networking*

1. Introduction

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. A typical multi-hop wireless sensor network architecture will consist of hundreds or thousands of self-organization, lower-power, lower cost wireless nodes deployed en masse to monitor and affect the environment. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory space, sensors, a communication device and a power resource in form of a battery.

2. Common security schemes in wireless sensor networks

Applying any encryption scheme requires transmission of extra bits. Extra bits are used for beyond processing, memory and battery power which are very important resources for the ‘sensors ‘desire. Applying the security mechanisms such as encryption could also increases in delay, jitters and packet loss in wireless sensor networks.
Stenography: cryptography hides the contents of the message but the stenography hides the existence of the message, art of converting communication by embedding a message into a multimedia data (image, size video etc.).

2.1 Obstacle to sensor security

There are three constraints compared to a traditional computer network [1]. To make sensor networks economically viable. Sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. Sensor networks interact closely with their physical environments and with people, posing new security problems. So to develop useful security mechanisms from current security techniques it is necessary to understand the constraints first.

A. Very Limited Resources
1) Limited Memory and Storage Space.
2) Power Limitation.

B. Unreliable Communication
1) Unreliable Transfer.
2) Conflicts.
3) Latency.

C. Unattended Operations
1) Exposure to Physical Attacks.
2) Managed Remotely.
3) No Central Management Point.

3. Major Security Requirements

3.1 Data confidentiality

Data that passes over the network should be confidential. Cryptographic methods used to encrypt the sensor identities, and public keys which is considered to be the public sensor information. [5]

3.2 Data availability

Resources and the data should be easily available to the sensor nodes. Many approaches have been proposed to achieve this goal.

3.3 Data integrity

Since the data’s are traverse among sensor nodes the data’s are easily altered by the attackers. To avoid this integrity control should be implemented until it reaches its original recipients.

3.4 Data freshness

Data should be updated up to time; old messages should not be conveyed among sensor nodes, especially important

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

when shared key strategy is used in this design.

3.5 Authenticity

Required for many administrative tasks, various authentication mechanisms like cryptography, shared keys digital signatures and so on ensures that data used in decision making process is from legitimate and authorized node.

3.6 Self-organization

In any difficult situations nodes should be feasible to make it self-healing and self-organizing [4]. Based on the open system interconnect (OSI) model the attacks are listed below.

Table 1: OSI model attacks

S. no	Layer	Attacks	Counter measure
1.	Physical Layer	•Jamming •Node Tampering .Sybil •Eavesdropping	•RypassRestriction, •Encryption
2.	Data Link Layer	•Traffic Manipulation •Identity Spoofing Altering routing Replay attack	•Misbehavior Detection, •Identity Protection
3.	Network Layer	•Spoofed routing information •Sybil attack •Wormhole •Hello flood •Acknowledgment spoofing •Black Hole •False Routing • Packet Replication	•Routing Access Restriction •False Routing Information Detection • Wormhole Detection
4.	Transport Layer	•Floodingattack•De-synchronization	•Limiting Connection Numbers •Authentication
5.	Application Layer	• Malicious Code Attacks • Repudiation Attacks • Clock Skewing • SelectiveMessage Forwarding • Data Aggregation Distortion	•security,Protection, •Data Confidentiality Protection

4. Categorization of Attacks In Wireless Sensor Networks

Attack in WSN can be classified in two different levels

- Attack against security mechanisms.
- Attack against basic mechanisms.

In certain conditions when there is less security a false or malicious node could intercept private information, or could send false messages to nodes in the network.

5. Denial of Service Attack

Occurs due to unintentional failure of nodes or malicious action. Attack tries to exhaust the resources available to the victim node by sending extra unnecessary packets and thus prevents uers to access the legitimate node as shown in figure1.

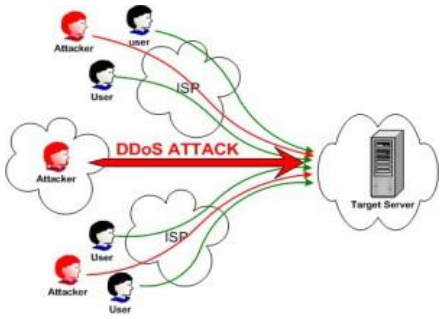

Fig.1: Denial of service

The basic types of attacks in different layers are [3] give below.

LAYER	ATTACKS
PHYSICAL LAYER	Jamming, tampering
DATA LINK LAYER	Collision, exhaustion
NETWORK LAYER	Misdirection
TRANSPORT LAYER	Desynchronisaton
APPLICATION LAYER	Path based dos

6. Selective Forwarding Packet

Packages are directly forwarded to the certain node by the attackers to remove the packages importance [5]. Random selection path and braided paths are not two consecutive links that are used for multi path routing.

7. Wormhole Attack

Considered to other most tedious attacks among the attacks in wireless sensor networks, this attack is the complicated to detect compared to other attacks. Literature survey on the wormhole attack says several ideas like,

1. Packet leashes (packets must be prevented from travelling farther than the radio transmission range. Drawback in this is need of highly synchronized clocks.
2. Distributed detection method (relies solely on network connectivity information, based on local topology) [6].

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Wormhole attack is poses three ways.

- Tunneling the messages above the network layer.
- Long range tunnel using high power transmitters.
- Creation of tunnel via wired infrastructure.

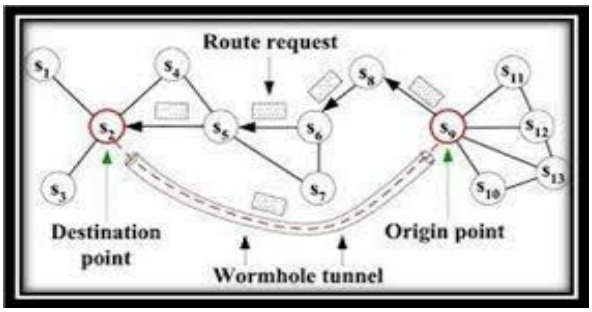

Fig.2: Wormhole architecture

Use of this attack is to exploit routing race conditions (refers that when a node take some actions based on the first instance of messages it receives and subsequently ignore later instances of that message). This attack is the combination of various attacks like black hole, sinkhole, eavesdropping.

8. Blackhole Attack

The Black hole attacks are one of the challenging attack in the security of WSN. [6]Black hole attacks occur when an adversary cap-tures and a set of nodes re-programs in the network to block/drop the packets they receive/generate instead of forwarding them towards the base station. [6]

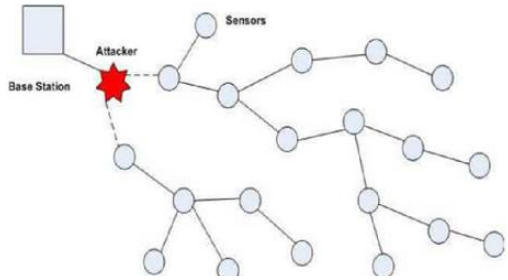

Fig.3 Black hole

9. Sinkhole Attack

Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to be verified. [7]

In this paper an algorithm to detect the wormhole attack known as Localized Faulty Detection Algorithm [4].The goal of the paper is to locate the faulty sensors in the wireless sensor networks. We propose and evaluate a localized fault detection algorithm to identify the faulty sensors. The implementation complexity is low and the probability of correct diagnosis is very high even in the existence of large fault sets.

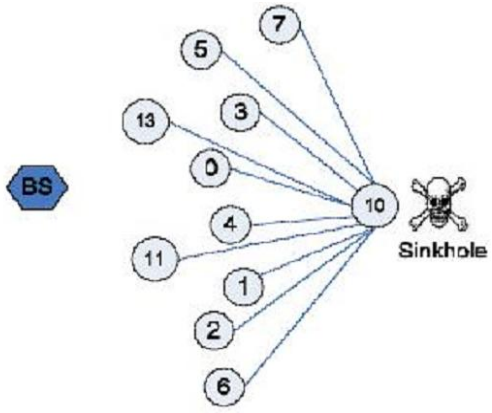

Fig.3: Sinkhole

We list the notations used in our algorithm and analysis below,

• n: total number of sensors;
• p: probability of failure of a sensor;
• k: number of neighbor sensors;
• S: set of all the sensors;
• N(Si): set of the neighbors of Si;
• xi: measurement of Si;
• d t ij : measurement difference between Si and Sj at time t, d t ij = x t i − x t j ; • Δtl = tl+1 − tl;
• Δd Δtl ij : measurement difference between Si and Sj from time tl to tl+1, Δd Δtl ij = d tl+1 ij −d tl ij = (x tl+1 i −x tl+1 j)−(x tl i − x tl j);
• cij : test between Si and Sj , cij ∈ {0, 1}, cij = cji;
• θ1 and θ2: two predefined threshold values;
• Ti: tendency value of a sensor, Ti ∈ {LG, LT, GD, FT};
• Maxd: an estimate of propagation distance from a set of identified good sensors in the first round of the algorithm iterations. The worst case is n, the best case is log n, and we take a reasonable √ n. Sensors are considered as neighboring sensors if they are within the transmission range of each other. Each node regularly sends its measured value to all its neighbors. We are interested in the history data if more than half of the sensor's neighbors have a significantly different value from it. We can use this Δd Δtl ij to find if the current measurement is different from previous measurement. If the measurements change over the time significantly, it is sure that the sensor is faulty. A test result cij is generated by sensor Si based on its neighbor Sj's measurements using two variables, dij and Δdij , and two predefined threshold value θ1 and θ2. If a sensor is faulty, it can generate arbitrary measurements. If cij is 0, most likely either both Si and Sj are good or both are faulty. Otherwise, if cij is 1, Si and Sj are most likely in different status.

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Algorithm The localized faulty sensor detection algorithm is summarized in the following:

Step 1: Each sensor Si tests every member of Sj ∈ N (Si) to generate test cij {0, 1} using the following method:

1: Each sensor Si, set cij = 0 and compute d t
2: IF |d t ij | > θ1 THEN
3: Calculate Δd Δtl ij ; 4: IF |Δd Δtl ij | > θ2 THEN cij = 1;

Step 2: Si generates a tendency value Ti related upon its neighboring sensors' test value: and also compare the number of Si's with its LG neighboring nodes with different test results to determine its status:

1: IF P Sj∈N(Si) cij < d|N(Si)|/2e, |N(Si)| is the number of the Si's neighboring nodes THEN
2: Ti = LG;
3: ELSE Ti = LF;
4: Communicate Ti to neighbors;
1: IF (P Sj∈N (Si) andTj=LG (1−2cij) ≥ d|N(Si)|/2e THEN
2: Tj = GD;
3: Communicate Ti to neighbors;

Step 3: For the remaining undetermined sensors, do the following steps in parallel for Maxd cycles:

1: FOR i = 1 to n
2: IF Ti = LG or Ti = LF THEN
3: IF Tj = GD ∀Sj ∈ N(Si), THEN
4: IF cji = 0 THEN
5: Ti = GD;
6: ELSE Ti = FT;
7: ELSE repeat
8: Communicate Ti to neighbors;

Step4: If ambiguity occurs, then the sensor's own tendency value determines its status:

1: FOR each Si, IF Tj = Tk = GD ∀Sj, Sk ∈ N(Si), where j 6= k, and IF cji 6= cki THEN
2: IF Ti = LG (or LF) THEN
3: Ti = GD (or FT)

10. Conclusion

Provisioning internal security is a significant task in WSN. This paper is presented about the wormhole attack and internal security requirements and characters. For future enhancements algorithm used in this paper to detect the wormhole attack (Localized Faulty Detection Algorithm).Can be tried to minimize the steps in this algorithm since it contains many modules in this algorithm more shortest algorithm can be found for reducing the risk factors and consume time.

Reference

[1] V.Sujathabai Assistant Prof. Dept. of MCA Vel Tech HighTechDr.Rangarajan Dr.Sakunthala Engineering collegeAvadiChennai
[2] http://searchdatacenter.techtarget.com/definition/sensor-network
[3] https:// www.google.co.in /? gws_rd p://www.techopedia.com / definition / 26217/insider-attack Jinran Chen, Shubha Kher, and Arun Somani Dependable Computing and Networking Lab
[4] Iowa State University Ames, Iowa 50010 jrchen, shubha, arun@iastate.edu
[5] Manisha, Gaurav Gupta Department of Computer Science Engineering Shoolini University, HP, India
[6] Ms. B .R. Baviskar, Mr. V. N. Patil1 PES's Modern College of Engineering Pune, India Electronics and Telecommunications Engineering Department bhagyashri.1424@gmail.com.
[7] Vinay Soni1, Pratik Modi2, Vishvash Chaudhr21, 2Department of Computer Engineering, LDRP -ITR, Gujarat Technological University,