International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Low Priced And Efficient Energy Replica Detection In WSN

Miss.Sayali Ashok Bhoite[1] , Miss.Choudhar Sandhya Jalindar[2] , Miss. Gavali Vaishali Hanumant[3]
Miss. Salunkhe Swati Nandkumar[4] , Prof.Sirdeshpande S.A.[5]

Department of Computer Engineering,S. B. Patil Collage of Engineering Indapur, Dist-Pune, Savitribai Phule Pune University

---

Abstract—one of most challenging problem is the replica attack in static wireless sensor network. Also every sensor nodes are physically captured. These nodes are reprogramming and replicated in large number of replicas. Which may dynamically occupy the network Thus far different ways to detect the replicas? Most of the sensor nodes required high costs hardware like as:"Global Positioning System". In general, Sensor nodes are low price as compared to GPS hardware. On this paper, we proposed "Low Priced and Energy-Efficient Detection of Replicas in Static Wireless Sensor Network". On this proposed solution not required any internal hardware such as: GPS. Good performances as compared to exiting system. We show that the proposed solution saves the lot of energy than exiting system.

Introduction

Wireless sensor network are provides two different technologies such as: computation and communication. It consists of large number of sensing devices also support for : Physically and Environmental conditions like: Humidity,Tempreature,Pressure,Sound etc.Data collected by sensing devices and also transmitted to the destination .It also known as base station or sink.WSN's have various security challenges as compared to traditional network.The sensor nodes generally support for tamper resistances behind the hardware. It also spread in insecure enviornments.Where they are not grunted to capture and compromise attack. These replicas can be used for various launch stealth attack depending on the attackers motives. Such as listen secretly to private on network communication or controlling the source areas. This type of attack is also known as "Replica attack".

Accordingly, without using hardware like: GPS, we design low price replica detection solution for static wireless sensor network by using "Bloom Filter" and "Sequential delivery algorithm". Neighboring nodes IDs also presented with constant size by using Bloom Filter."Bloom Filter Output" (BFO): uses for proof. The in this methods slowly increase traffic between the neighboring node and randomly selected nodes ,then exiting system generates heavy traffic by transmitting proofs form the starting. The entire result shows that the proposed solution is more energy efficient than exiting system.

The contribution of purposed solution as follows:

- Low price solution: The proposed solution also reduces the cost of building wsns replica detection.
- Efficient - energy detection: Energy efficiency is important in wsn.we consider node in environment are often non rechargeable and hence availability depends on energy efficiency. Support for large scale.

.*A* Replica Attack and Detection Scenario

An attacker captures one or more nodes deployed in the network and then obtains secret information from them. Next, the attacker makes multiple replicas by using this information and then deploys them into targeted areas. Here, the neighboring nodes recognize replicas as newly deployed nodes. For obtaining useful information from the neighboring nodes in the target areas or controlling the neighboring nodes, replicas should prove that they are legitimate nodes with valid secret information. However, since replicas already know the secret information, they can prove it to the neighboring nodes without difficulty. Hence, before proving the legitimacy, all newly inserted nodes (some of which may be replicas) must pass the replica detection test more than once.

.RELATED WORK

- C.P.Mayer. In proposed:"security and privacy and privacy challenges in the Internet of Things. Problem of this proposed system is security and privacy is the key issues for IOT application and still faces some environment challenges. Solution of this paper is researched status of key technology including encryptions mechanism communication, security, protecting, sensor data and cryptographic algorithm and briefly outlines the challenges.

- B.Parno, A.Pemg and V.Gligar. On this proposed solution distributed detection or node replication attack in sensor network.

Architecture of WSN SYSTEM

Which Architecture Used for Architecture of wsn System are as follows

Architecture Used for Architecture of wsn system

Sensor networks are usually designed and deployed for a specific application. They are scalable with a minimal effort. Network topology changes frequently in WSN due to energy depletion, channel fading, node failure and damage. Sensor nodes are self configurable and they are densely deployed in the target area. Battery is the only source of energy for most of the sensing devices. Most of the applications of WSN are data centric and the data-flows within the network obey many-to-one traffic pattern. Due to higher node density, data redundancy may exist in the network.

Components of WSN system

Main components required for low price efficient energy replica detection in WSN , climatic sensors, wireless communication, Broadcast(network to node), and . [1] In our system design, climatic parameters are read from nearest automatic weather station and are interpolated to suit the local climate. For example wireless communication landslide from Private Key, Randomized key is used for which have has cover space up to 100 meters.

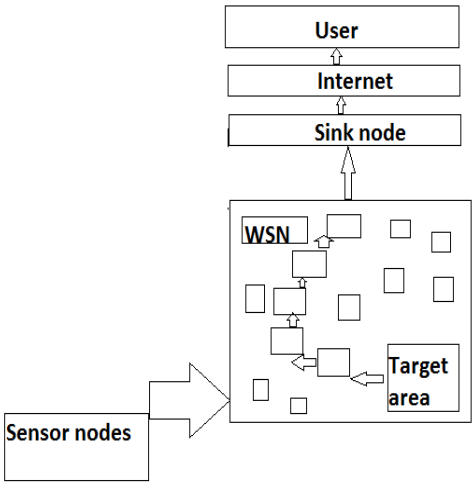

FIGURE 1: SYSTEM ARCHITECTURE OF WSN

THERE ARE FOUR MODULES

A] Node Formation

Neighboring node IDs are presented with a constant size using a Bloom filter. The Bloom filter output (BFO) is used as a proof. A newly deployed node generates different proofs according to the collected neighboring nodes ID's until collecting the entire neighboring node ID's. The proofs are delivered to a randomly selected node in the networkATmega168 Microcontroller[6]

B] Find Attacker

With regard to this attack, it is assumed that an attacker captures only a small fraction of nodes in the network because capturing a large fraction may not require replicas any more, and it may be more costly and detectable. It is reasonable to assume that an attacker captures only a few nodes and obtains secret information from the captured nodes.

c] **Replica Attack and Detection Using Bloom Filter**

An attacker captures one or more nodes deployed in the network and then obtains secret information from them. Next, the attacker makes multiple replicas by using this information and then deploys them into targeted areas. Here, the neighboring nodes recognize replicasaswly deployed nodes. For obtaining useful information from the neighboring nodes in the target areas.

D] Validation of Node

The RDB-R consists of three stages: proof generation, proof delivery, and proof validation. Henceforth, we explain the three stages with new deployment node A, the neighboring node C, and the witness node U. In the First Stage a proof for identifying a replica is created and updated in a newly added node.

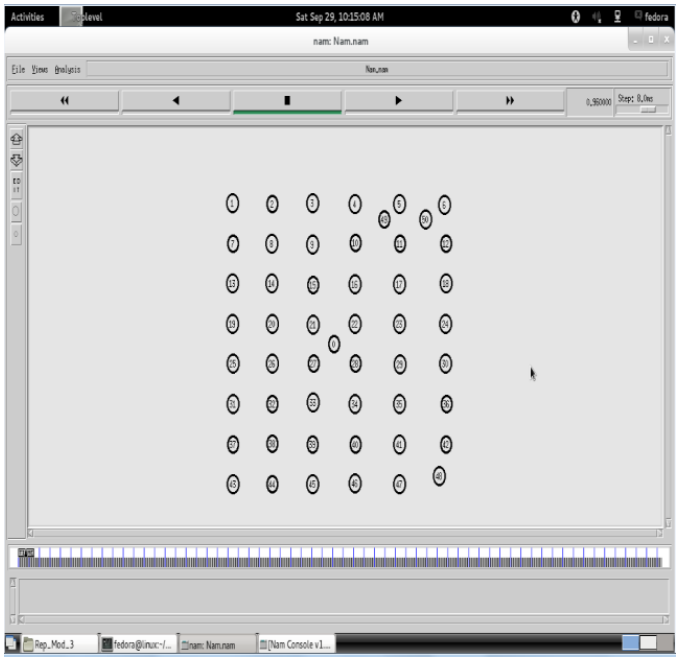

Fig. 1. Climatic Data extraction from IMD site

DUPLICATE NODE DETECTION :

The nodes which are captured by an adversary can compromise the sensor nodes and make many replicas of them. These compromised nodes all have the same ID are present in the network[6]. To understand the dangers of node compromise, we must first define what we mean by node compromise. Node compromise occurs when an attacker, though some subvert means, gains control of a node in the network after deployment.

Advantage:

Detects the replication with high probability using relatively limited number of witnesses.

Line Selected Multicast: This scheme uses the routing topology to detect the clones. In addition to the witness nodes, the intermediate nodes within the path can check for clones. Each node forwards the claims also saves the claims. For example, a node a and clone a ' in the network. Neighbor of a sends the location claim to r

Advantage:

- *Less communication cost*
- *High detection rate*
- *Less storage requirements*

.comparitive Study:

TABLE I. TABLE STYLES

	Time	Accuracy	Data Acquisition	Cost	Productivity
Existing System	More Time	Less Accurate	Sequential node	More Costly	Less
roposed System	Less Time	More Accurate	Random node	Less Costly	More

EXISTING SYSTEM :

- In existing system wireless sensor network have various type of security challenges or diffentiate to old network because the sensor hardware response for tamper resistance and are often spread in physically insecure environments .where they are vulnerable to get and settlement node with concessions by attacker's. A critical consequence of a sensor node settlement made with concessions attack is that once an attacker has required the

. Advantages

The strategy disperses traffic over the entire network, resulting in small packet loss and considerable energy saving.

We show that the proposed solution provides a high detection ratio as well as short detection time for detecting replicas without the use of GPS, as com-pared to existing schemes.

.Conclusion

In this paper, we proposed a low priced and energy-efficient solved to detect duplicate node for static wireless sensor network. Proposed does not use any additional hardware. Where existing system need of expensive hardware like as GPS receiver. Proposed solution use exhibits duplicate node or good performance than existing scheme. When one or more replicas detects within the short duration time and increase the high performance also gain the less energy.