CLONE ATTACK IN WIRELESS SENSOR NETWORK

Mr.Wajahat Gh Mohd[1], Ms Sakshi Gautam[2], Mr. Mohammad Anis[3]

[1,2,3]Dept. of Computer Science and Engineering,JB Institute Of Technology Dehradun.

[1]Wajahat.jbit@gmail.Com

Abstract: One of the most vexing problems in wireless sensor network security is the node Clone attack. In this attack, an adversary breaks into a sensor node, reprograms it, and inserts several copies of the node back into the sensor network. Cloning gives the adversary an easy way to build an army of malicious nodes that can cripple the sensor network. A few distributed solutions to address this fundamental problem have been recently proposed. However, these solutions are not satisfactory. Therefore first, the desirable properties of a distributed mechanism for the detection of node Clone attacks have been analyzed. Second, the known solutions for this problem do not completely meet our requirements. Third, a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node Clone attacks has been proposed, and it satisfies the intended requirements. Wireless Sensor Networks (WSNs) are often deployed in hostile environments where an adversary can physically capture some of the nodes, first can reprogram, and then, can replicate them in a large number of clones, easily taking control over the network. A few distributed solutions to address this fundamental problem have been recently proposed. However, these solutions are not satisfactory. First, they are energy and memory demanding: A serious drawback for any protocol to be used in the WSN-resource-constrained environment. Further, they are vulnerable to the specific adversary models introduced in this paper. The contributions of this work are threefold. First, we analyze the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, we show that the known solutions for this problem do not completely meet our requirements. Third, we propose a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks, and we show that it satisfies the introduced requirements. Finally, extensive simulations show that our protocol is highly efficient in communication, memory, and computation; is much more effective than competing solutions in the literature; and is resistant to the new kind of attacks introduced in this paper, while other solutions are not”

***Index Terms* -** Index Terms: - clone attack, RED, witness distribution, oblivious, performance, WSN.

I. INTRODUCTION

As the world business is becoming more portable and computational provisions are coming to be broadly appropriated, wireless sensor networks are crossing over any barrier by making distance and movement consistent. As the computing and communications devices continue to prolife rate, wireless networks require some creative medium access procedures to share the limited broadcast bandwidth in a fair and efficient manner. The magnetic characteristics of the wireless sensor networks pulled in numerous analysts to work on various issues related to these types of networks. Wireless Sensor Networks (WSN) are developing as both a vital new domain in the IT environment and a hot research including system design, networking, distributed algorithms, programming models, data management, security and social components. Wireless sensor networks are rapidly picking up the popularity as they are potentially low cost solutions. The fundamental thought of sensor network is to scatter minor sensing gadgets over a particular geographic zone for some specific purposes like target tracking, surveillance, environmental screening and so on. These tiny devices are equipped for sensing a few progressions of parameters and communicating with different units. A wireless sensor network (WSN) is a remote system comprising of an extensive number of geologically dispersed sensor nodes. These sensor nodes could be effectively conveyed at vital districts easily at a low cost. Sensor nodes collaborate with one another to screen physical or ecological conditions, for example, temperature, sound, picture, vibration, weight, movement or contaminations with the assistance of different sorts of sensors. However, while much consideration is constantly paid to the routing strategies and wireless sensor network modeling, the security issues are yet to receive extensive focus [1]. Essentially the utilization of any effective security conspire in wireless sensor systems is encouraged by the span of sensors, the processing power, memory and kind of functions anticipated from the sensors. Sensor networks are not universally traditional computing devices; subsequently the existing security models and strategies are lacking to run with them. In sensors, the geographic dissemination of the units allows an attacker to physically have control of nodes and study mystery key material, or to capture messages. The hierarchical nature of sensor networks and their route maintenance protocols permit the attacker to confirm where the root node is placed [2].WSNs are picking up interest in the research community due to their unique qualities. WSNs are very little watched. Consequently it is effectively conceivable for an assaulter to catch a hub physically, altering its code and getting private data like cryptographic keys. Wireless medium is inherently broadcast in nature which makes them vulnerable to attacks. These attacks can disturb the operation of WSN and can even kill the purpose of their deployment [3].Wireless networks can be recognized of two sorts: infrastructure network and ad-hoc (infrastructure less) network. Infrastructure network is a sort of a network with fixed and wired gateways. A mobile host interacts with a bridge in the network within its communication radius. The mobile unit can mobile geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This phenomenon is termed as handoff. On the other hand, Mobile ad hoc network is an aggregation of wireless mobile nodes in which nodes team up by sending packets for each other to permit them to communicate outside range of direct wireless transmission. Ad hoc networks require no fixed network infrastructure such as base stations or access points, and could be rapidly and economically set up as required.

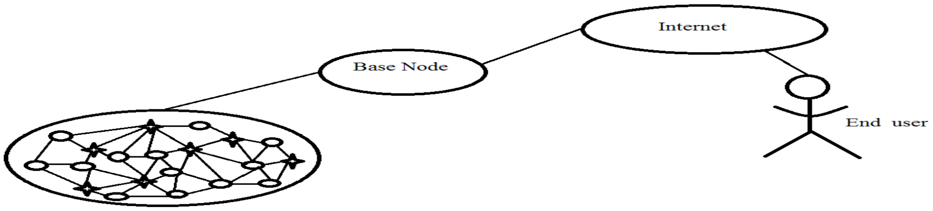


Figure1: WSN Overview

II.REVIEW OF LITERATURE

The wireless sensor network is an open research field. All the components of this network are still in developing phase. The security of WSNs has been extensively studied by the research community and while there are several open problems that remain to be solved. Several approaches have been proposed for avoiding the attacks in WSNs and for ensuring the security. There exist several analysis papers on wireless sensor networks, more specifically, on security. This existing literature presents a valuable categorization of attacks and practical security considerations. Some of the papers have been considered that has been taken as a motivation towards my study.

Security in Wireless Sensor Networks: Issues and Challenges by Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong (2006)

The paper aims to investigate the security issues and challenges in wireless sensor networks. The paper aims to identify security threat and throw a light on the proposed security mechanisms for wireless sensor networks. The paper explains that the WSNs have a great scope in applications like mass public and military purposes. The network security fundamentals and the techniques meant for wireless sensor networks are being discussed in the paper. The various possible attacks in WSNs and the holistic view of security to ensure robust security in wireless sensor networks have been reviewed.

Wireless Sensor Network Security: A Survey by John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary (2006)

The need of effective security mechanisms has been emphasized in the study. The reason is the interaction of the sensor networks with the sensitive data. Holding the security concerns, this paper surveys the major topics in wireless sensor network security and highlights the hurdles and the requirements in the sensor security. Many of the current attacks have been classified in the paper along with their corresponding defensive measures. It is more challenging to achieve security in sensor networks due to inherent resources and computing constraints than traditional network security. The paper aims to provide a general overview of the wireless sensor network security along with enlightening the direction in which further review of the relevant literature can be completed.

Detection of Masquerade Attacks on Wireless Sensor Networks by Vijay Bhuse, Ajay Gupta and Ala Al-Fuqaha (2007)

Considering the important WSN properties, two lightweight techniques have been proposed in this paper to detect masquerade attacks on wireless sensor networks (WSN). These two proposed techniques- MG (Mutual Guarding) and SRP complement each other when used concurrently. In this paper, the proposed techniques have been presented and their performance has been analyzed in terms of success rate of detection, overhead and its effect on the network lifetime. The drawbacks of MG technique over SRP are explored.

A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks by Mauro Conti, Roberto Di Pietro, Luigi V. Mancini (2007)

The paper emphasizes on the fundamental problem of node replication attack detection. The paper has presented and justified a few of the basic requirements for an ideal protocol to detect node replicas. This work presents a three step protocol. This paper is the proposal of a Randomized, Efficient, and Distributed(RED) protocol that is able for detecting node replication attacks and the analysis shows that it is completely satisfactory with respect to the requirements. The simulation results also show that the proposed protocol is highly efficient in communication, memory, and computation ,an sets out an improved attack detection probability compared to the best solutions in the literature, and that it is resistant to the new kind of attacks introduced in this paper.

III.PRESENT WORK

3.1 Scope of Work

Wireless sensor networks have pulled in a ton of consideration throughout the most recent decade in wireless and mobile computing research community. Requisitions of these systems are various and developing running from indoor arrangement situations to open air organization. However, due to distributed nature and their deployment in remote areas, systems are helpless to various security dangers that can unfavorably influence their execution. As the current sensor nodes lack hardware support for tamper-resistance and are often deployed in unattended environments where they are susceptible to catch and trade off by a foe, new security tests emerge in sensor systems [4]. Thus, that makes us to accept that existing security instruments are deficient, and new thoughts are required. Luckily, the new issues likewise move new research and speak to a chance to fittingly address sensor organize security from the begin.

3.2 Problem Formulation

With the expanding advancement of Internet computing, there is additionally potential in the harm created by malicious attack. In the field of intrusion detection, masquerade attacks a standout amongst the most unsafe and challenging to discover. A masquerade strike is an unapproved endeavor to mimic a genuine client. As masquerade systems development, it is basic to improve vigorous and correct methods to identify these attacks. As a research problem, masquerade detection is a subset of the inconsistency recognition ideal model for general interruption identification frameworks (IDS). Right away security has been seen as a standalone part of a system architecture, where a differentiate module gives security. This separation is not usually appreciable approach to network security .To accomplish a safe framework, security must be reconciled into each segment. By and large not mixing security to parts throughout framework improvement plan, part has turned to be a purpose of strike. As a result, security must be associated with every aspect of system design.

In this work, a very severe and important physical attack on WSN which is called node replication attack or clone attack has been taken into consideration. It is also known as identity attack. In this attack, an adversary first physically catches genuine nodes, then replicates them fabricating those replicas having the same identity (ID) with the captured node, and finally deploys a number of clones throughout the network. In WSN, a variety of insider attacks can be launched by an adversary by replicating the captured sensors and deploy them in the network[4]. Relying on the Centralized base station is one of the first solutions for the detection of node replication attacks. In this solution, each node sends a list of its neighbors and the geographic coordinates to a Base Station (BS).The same entrance in two records sent by hubs that are not "close" to one another will bring about clone recognition. At that point, the BS repudiates the clones. This result is not exceptionally productive as it has a few hindrances, for example, the base station goes about as a solitary purpose of disappointment and high correspondence takes because of the substantial number of messages. Further, nodes close to the BS will be required to route far more messages than other nodes, hence shortening their operational life .In the event that these duplicated nodes or clones remain undetected or unattended for quite a while, they can further begin the progressions in convention conduct and interruption into the frameworks security [4]. It is simple for an adversary to start such assaults because of the way that the clones have real data and they may be recognized as authentic nodes.

3.3 Objectives

The goal of confidentiality is needed in WSN environment to avoid the divulgence of the data going around the sensor nodes of the system or between the sensors and the base station. Authentication in sensor systems is fundamental for every sensor node and base station to confirm that the information gained was truly sent by a trusted sender or not. While clustering of nodes in WSNs, authentication is needed. We can trust the data sent by the nodes in that group after clustering. Integrity controls must be executed to guarantee that data won't be adjusted in any surprising way. Secure administration is required at base station, clustered nodes, and protocol layer in WSN. Because security issues like key distribution to sensor nodes with a specific end goal to create encryption and tracking data require secure administration.

3.4 Research Methodology

3.4.1 Methodology

The fast utilization of unlimited advances in WSNs is increasing the potential of dangers and assaults to WSN. A commonplace risk called hub replication strike is an exceptionally intense issue in which a foe reproduces a sensor hub after physically catching it and afterward utilizes these copies to disturb the system operations by redeploying them at key positions of the system. Hence the exploration identified with hub replication strike in WSNs has been accompanied with much engage in recent years. The research of authentication and security techniques is now very develop yet such results neglect to recognize hub replication attack and in this way no more furnish WSN with satisfactory security from this assault. Moreover, the discovery of node replication attack in portable WSN is far distinctive and more challenging than in static WSNs.

RSD protocol (Randomization, Selection, and Detection) is a new protocol for detection of node replication attacks. RSD executes at fixed intervals of time. RSD is stationary centralized technique, where Base Station is responsible for overall functionality of nodes in Wireless Sensor Network (WSN). In stationary centralized technique, nodes are deployed at initial stage by base station will not change their location in future. Only base station can change nodes’ location at the time of redeployment. In RSD, we have taken three kinds of nodes.

- Base Station node

- Sensor Nodes: which send and receive messages to each other over the network.
- Witness Nodes: are responsible for secure transmission of messages between sensor (sender and receiver) nodes.

1. Randomization: At the first step, a random value rand is shared among all the nodes by Base Station using centralized broadcasting (for example from a satellite).

2. Selection:

a) In the second step, a sensor node or sender who wants to send message to another sensor node (receiver), asks Base Station to select a witness node, which is close to receiver node, for secure transmission of message.

b.) Base Station takes in input the current rand value, sensor node (sender) ID location and total number of witness node g of location to apply pseudo-random function to select a witness node randomly.

3. Detection: Base station acknowledges both sensor node (sender) and witness node about each other. Base station also sends a list of all the sensor nodes' ID Location(the list of the deployment of sensor node at initial stage) to selected witness node. So witness node compares this list with current ID Location of sender node and sender node's neighbor nodes.

a.) If sensor nodes are present with different location having same ID, it means a clone node having ID of the real node has been forwarded by an adversary. So witness node will detect this clone node/replicated node and inform about this to base station and base station will revoke clone node and inform other nodes about revoking through broadcasting.

b.) If a sensor node is captured by an adversary, it will be absent at current time and selected witness node will tell about this to base station that a sensor node at the time of deployment is not present currently.

c.) In case, if witness node may be get captured by an adversary, base station can ensure about it using the same detection procedure. BS will ask its neighbor witness node to compare captured witness node's current ID Location with the ID Location at the time of deployment. And if witness node is really captured or replicated, neighbor witness node will inform about this to base station and base station will revoke captured witness node.

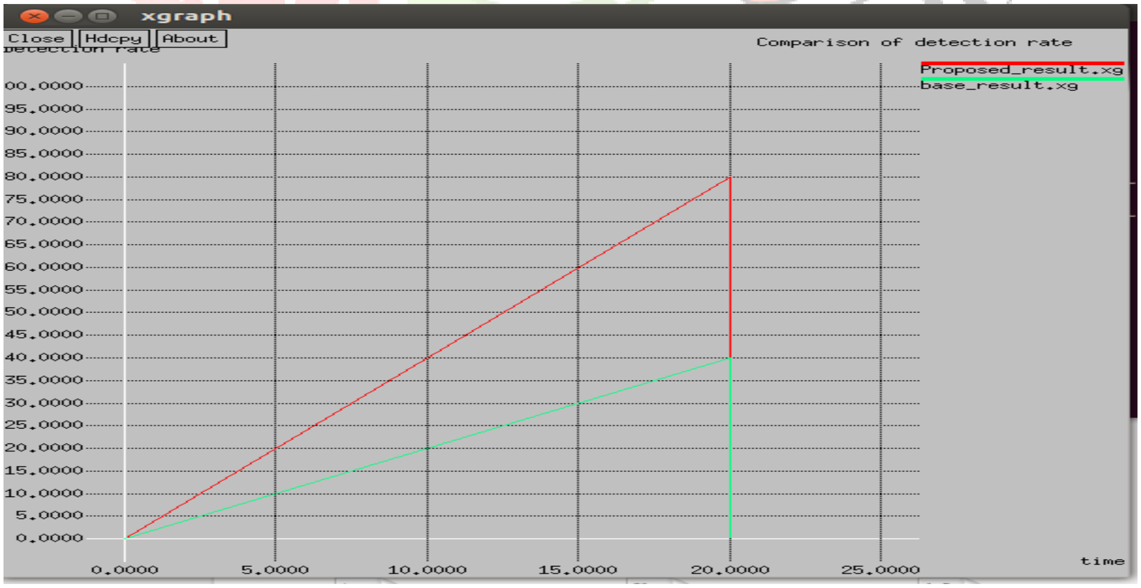
3.4.2 Tool Used for Simulation

These days, there are numerous system network simulators that can mimic the WSNs. Ns2 is an open-source event-driven test system designed particularly for research in computer communication networks. Network Simulator Ns-2 is a discrete event simulator that is focused at network research. It furnishes underpin for simulation of TCP, steering and multicast protocols over wired and remote sensor networks.NS-2 fully simulates a layered network from physical radio transmission channel to high level applications.

NS-2 simulator has several features that make it suitable for our simulation.

- A network environment for ad-hoc networks
- Wireless channel modules
- Routing along multiple paths

IV. RESULTS AND DISCUSSION:



While simulating the proposed approach, 50 nodes were deployed randomly in the network. It as beenobserved that the clone detection rate in the existing RED approach was 40% while in proposed approach the detection rate is 80%. Hence the proposed approach shows better results.

V.CONCLUSION AND FUTURE WORK

I. The first and foremost work is to choose the Domain of interest and finalize the name of the research topic to work on.In the month of September- October 2017, I had finalized my Domain and the name of the research topic on which I was supposed to work. I have read the research papers and gone through various web articles to find the "Problem Definition" and to develop the approach to be proposed. The most important part is the selection of the tool that will be needed for the realization of the proposal.
II. In November 2017, I decided my problem definition. November onwards the simulation work will be started. Since I have already gone a long way in studying the theoretical algorithms, I am in process to simulate the proposed solution in NS-2.
III.In addition to this, I began to make the documentation of my proposal.

REFERENCES.

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

[2] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI (2012), "*Wireless Sensor Network: Security challenges",* 978-1-4673-1053-6/12/2012 IEEE

[3] Vijay Bhuse, Ajay Gupta and Ala Al-Fuqaha (2007), "*Detection of Masquerade Attacks on Wireless Sensor Networks*", 4244-0353-7/07/2007 IEEE

[4] Wazir Zada Khan, Mohammed Y. Aal salem, Mohammed Naufal Bin Mohammed Saad, and Yang Xiang (2013), "*Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey",* International Journal of Distributed Sensor Networks Volume 2013, Article ID 149023, 22 pages

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary (2006), "*Wireless Sensor Network Security: A Survey",* Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.)c©2006 Auerbach Publications, CRC Pres

[6] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini (2007), "*A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks*", MobiHoc'07, September 9-14, 2007, Montréal, Québec, Canada Copyright 2007 ACM 978-1-59593-684-4/07/0009

[7] Luis E. Palafox and J. Antonio Garcia-Macias (2008), "*Security in Wireless Sensor Networks",* 2008, IGI Global

[8] Kutha di Venu Madhav, Rajendra.C And Raja Lakshmi Selvaraj (2010), "*A Study Of Security Challenges In Wireless Sensor Networks",* Journal of Theoretical and Applied Information Technology © 2005 - 2010 JATIT& LLS

[9] Hero Modares, RosliSalleh, Amirhossein Moravejosharieh (2011), "*Overview of Security Issues in Wireless Sensor Networks",* 2011 Third International Conference on Computational Intelligence, Modelling & Simulation

[10] Eirini Karapistoli and Anastasios A. Economides (2012), "*Wireless Sensor Network Security Visualization",* 4th International Workshop on Mobile Computing and Networking Technologies 2012, IEEE

[11] Sunil Gupta,Harsh K Verma, AL Sangal, "*Analysis and Removal of Vulnerabilities in Masquerading Attack in Wireless Sensor Networks*", ISSN 2249-6343International Journal of Computer Technology and Electronics Engineering (IJCTEE)Volume 2, Issue 3, June 2012

[12] Patrick Tague, David Slater, Jason Rogers, and Radha Poovendran*, "Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis"*,1545-5971/09/2009 IEEE

[13] Ravi Kumar,Sunil Kumar,Prabhat Singh, "*Enhanced Approach for Reliable & Secure Wireless Sensor Network",* Volume 3, Issue 7 July 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[14] Md. Safiqul Islam, Syed AshiqurRahman, "*Anomaly Intrusion Detection System in Wireless Sensor Networks:Security Threats and Existing Approaches",* International Journal of Advanced Science and Technology Vol.36, November, 2011

[15] BabliKumari,JyotiShukla, *"Secure Routing in Wireless Sensor Network",* Page |746 Volume 3, Issue 8, August 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[16] ChakibBekara and Maryline Laurent-Maknavicius, "*Defending Against Nodes Replication Attacks on Wireless Sensor Networks"*