Detection of Clone Attack in Wsn

Reyaz Ahmad sheikh[1], Rajeev kumar Arya[2], Mr.Shubhashish Goswami[3]
[1]M.tech Student, Department of CSE, Dev Bhoomi institute of Technolgy (Dehradun) India.
[2] M.tech Student, Department of CSE, Dev Bhoomi institute of Technolgy (Dehradun) India.
[3]Assistant Professor, Department of CSE, Dev Bhoomi institute of Technolgy (Dehradun) India.

***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.*

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

I. Introduction

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. 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.

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.

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.

II. Review Of Literature

One important physical attack is the introduction of cloned nodes into the network. When commodity hardware and operating systems are used, it is easy for an adversary to capture legitimate nodes, make clones by copying them and integrate these clones back into the network. Key preloading offers security to sensor networks with little overhead. Random key redistributions seems particularly well suited to this domain. The key usage probability distribution has been derived and showed how the false positive rate defines the key usage threshold. Keys whose use exceeds the threshold value ware considered cloned and erased from the network. WSNs ware expected to be the basic building block of pervasive computing environments, hence establishing secure pair-wise communications could be useful for many applications.

Wireless Sensor Network Security Visualization

by Eirini Karapistoli and Anastasios A. Economides (2012)

This paper explores the issues and concerns in visual analysis for wireless sensor network security purposes. This paper focuses on several distinct advantages offered by the information visualization and visual analytics in the security domain. The paper aims to consider the upper visualization layer in the security of WSNs due to the absence of this aspect in the existed security systems. Information visualization has been deployed in different fields and recently in visualizing network data. In addition, this paper reviews security visualization tools that are available to network security analysts. Finally, it concludes by identifying challenges for this new area of research.

Wireless Sensor Network: Security challenges

by Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI (2012)

The paper review several intelligent systems and concludes that the traditional security models and methods are not well sufficient for their deployment. The unique properties of sensor networks have been discussed and then an attack model has been proposed that addresses these unique properties. The paper outlines the security properties that must be considered while designing a secure sensor network and presents the security challenges along with the description of the attacker's goals. This paper proposes more appropriate attack taxonomy and looks at how the security model must be tailored for sensor networks.

Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey by WazirZada Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad, and Yang Xiang (2013)

In this paper, the demonstrated depiction about the node replication attack or clone node attack has been given. Distinguishing the node replication assault has turned into a basic research point in sensor system security, and designing detection schemes against node replication attack involves different threatening issues and challenges. A study has been introduced in this paper to characterize the existing discovery plans and different recommendations have been investigated in every class. The paper also highlights some technical details and comparisons to demonstrate limitations of the existent detections as well as effective contributions.

SET: Detecting node clones in Sensor Networks

by Heesook Choi, Sencun Zhu, Thomas F. La Porta

In this method, another adequate and effective plan, Set has been proposed, to locate the clone assaults. The key thought of Set is to distinguish clones by registering set operations (intersection and union) of restrictive subsets in the network. The reliability and resilience of SET has been shown by analyzing the probability that an adversary may effectively obstruct the set operations. Performance analysis and simulations also exhibit that the proposed plan is more proficient than existing plans from both correspondence and memory cost outlooks. A detailed security analysis has been given for several types of attacks in the paper. The probabilistic analysis done in the paper showed that SET provides a resilient and reliable detection. The performance and overhead of the proposed algorithm have been analyzed. The results showed that the proposed solution has low transmission overhead, while using reasonably small memory space. As described in the introduction, our solution is based on a set model of a sensor network in which exclusive subsets are formed and a report of each subset is transmitted to the base station. Due to the typical random deployment of sensors, it is challenging to construct exclusive subsets in the network. We first present an Exclusive Subset Maximal Independent Set (ESMIS) algorithm by which exclusive subsets are formed in a distributed way in the network (subsection III-A). To ensure secure subset construction in a network with compromised nodes, we propose to integrate the ESMIS algorithm with an authentication scheme. We optimize SET by applying randomization to the exclusive subset formation, without losing security and exclusiveness. To perform efficient and reliable set computation in the network, we propose a multiple tree based set computation scheme so that intersection and union of subsets can be efficiently computed. Finally, we present an interleaved authentication scheme, to preserve the reliability of set computation on a tree.

A Range-based Detection Method of Replication Attacks in Wireless Sensor Networks
by HuangJian, Xiong Yan, Li Ming-xi, Miao Fu you (2012)

In this paper, a range-based detection method (RBDM) has been proposed to detect replication attacks in wireless sensor networks. In this method, wireless ranging information between nodes is used to detect node replication attacks. The method can maintain a high probability of detection with Low accuracy ranging between nodes. The theoretical analysis and simulation results show that system is proficient and functional in discovery of replication strike in remote sensor systems.

III. Present Work

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. 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.

Proposed Method

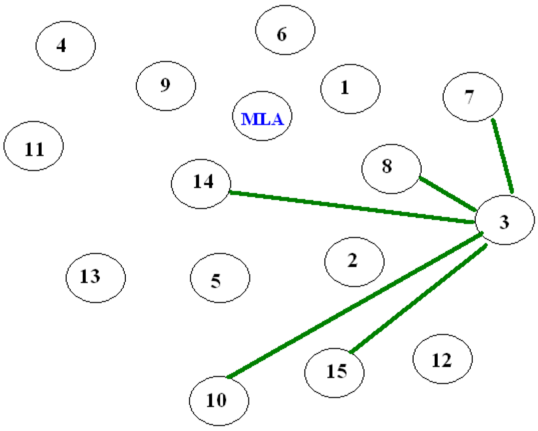
The fast utilization of unlimited advances in WSNs is increasing the potential of dangers and assaults to WSN. A common place risk called hub replication strike is an exceptionally intense issue in which a foe reproduces a sensor hub after physically catching it and afterward utilizes these copies to 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.

A majority of existing schemes adopt a witness finding strategy. In the witness finding strategy, nodes are required to sign and transmit a location claim to its witness nodes. Two conflicting location claims that claim the same node ID (signed by the same key) appear at different locations, implies a node clone attack. Yanxiang Lou et.al [8], explains that at any time, a physical cannot appear at different neighbourhood community otherwise there must be replicas in the network. Each node maintains a neighbour node list, which is readily available in a typical WSN since sensor nodes need to know their neighbours in order to communicate with each other. Whenever two nodes meet with each other, they exchange witness node lists with each other and check whether they are containing any node possessing same ID in both lists. If any such node occurs in both lists, then that node is detected as clone the reason being no node can be present at two different locations at a time.

The steps to be followed while implementing the proposed approach is:

- Clustering is done in network.
- Each node finds its two shortest neighbours.
- Shortest neighbour list will be forwarded to the C.Hs.
- If a clone is present in any cluster, shortest neighbour will be different.
- C.Hs will exchange the list with each other.
- In case if the clone is outside the cluster, C.H will exchange lists then they will identify the clone.
- C.Hs will send list to B.S.
- If two C.Hs possessing same ID but different list then B.S will detect the clones at C.H level.
- Two C.H's list cannot be same, so C.Hs will be detected.The proposed methodology is needed to be implemented in a tool. The tool opted for simulation of the proposed work is NS-2. The proposed clone attack detection technique is simple to implement and is based on network signatures. A digital signature algorithm is a cryptographic tool for generating non-repudiation evidence, authenticating the integrity as well as the origin of a signed message. In a digital signature algorithm, a signer keeps a private key secret and publishes the

corresponding public key. The private key is used by the signer to generate digital signatures on messages and the public key is used by anyone to verify signatures on messages.



WSN for proposed model

IV. Experimental Results

The proposed method is implemented using NS-2. NS2 is one of the most popular open source network simulators. Following are the steps to implement the proposed clone attack detection model on NS-2 and appropriate NS-2 functions have been used to implement these steps:

- Design the network on paper first
- Create the event scheduler
- Turn on tracing
- Create network
- Setup routing
- Setup used signature pattern
- Create Mac Layer Agent
- Create transport connection
- Create traffic
- Transmit application-level data
- Simulate and generate the trace and nam files
- Finish procedures.

The following result has been presented.

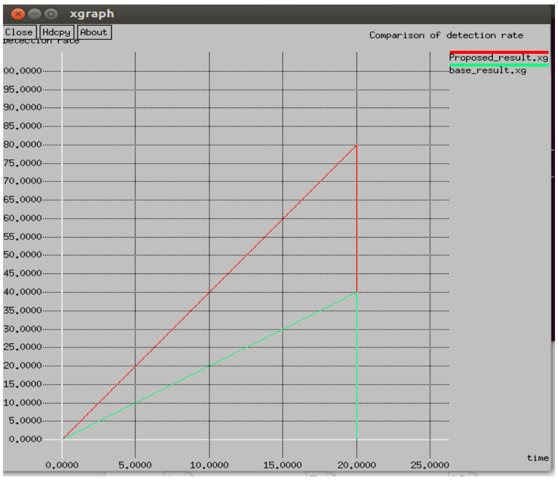


Fig. 12 Detection rate comparison

While simulating the proposed approach, 50 nodes were deployed randomly in the network. It as been observed 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 & Future Scope

The proposed method has been implemented using NS-2. The results of the implementation show that the proposed method is efficient to detect clone attack in the WSN efficiently. Further since the proposed method has signature of containing only four fields the system overheads are low, thereby reducing the energy consumption of the nodes. This further increases the throughput and reduces the delay as compared to methods proposed in the literature.

Future Scope:

• To combine the signature generated in this method with the cryptographic algorithms to further
Strengthen the security of the network along with the detection of cloning attack. • The proposed method can be modified to achieve simultaneous detection of Sybil and clone attack.

References

[1]. Maneesha V. Ramesh, Aswathy B. Raj and Hemalatha T, “Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks”, 2012 Fourth International Conference on Computational Intelligence and Communication Networks, IEEE

[2]. Chia-Mu Yu, Chun-Shien Lu, Sy-Yen Kuo, “CSI: Compressed Sensing-Based Clone Identification in Sensor Networks”, 8th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing 2012, Lugano

[3]. Yan-Xiao Li, Lian-Qin, Qian-Liang, “Research On Wireless Sensor Network Security”, 2010 International Conference on Computational Intelligence and Security, IEEE

[4]. Yilin Wang1 and Maosheng Qin, “Security for Wireless Sensor Networks”, International Conference on Control, Automation and Systems 2010Oct. 27-30, 2010

[5]. Heesook Choi, Sencun Zhu, Thomas F. La Porta, “SET: Detecting node clones in Sensor Networks”, [8] KuthadiVenuMadhav, Rajendra.CAnd Raja Lakshmi Selvaraj (2010), “A Study Of Security Challenges In Wireless Sensor Networks”, Journal of Theoretical and Applied Information Technology © 2005 - 2010 JATIT& LLS

[6]. Hero Modares, RosliSalleh, AmirhosseinMoravejosharieh (2011), “Overview of Security Issues in Wireless Sensor Networks”, 2011 Third International Conference on Computational Intelligence, Modelling& Simulation

[7]. EiriniKarapistoli and Anastasios A. Economides (2012), “Wireless Sensor Network Security Visualization”, 4th International Workshop on Mobile Computing and Networking Technologies 2012, IEEE

[8]. SunilGupta,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

[9]. Patrick Tague, David Slater, Jason Rogers, and RadhaPoovendran, “Evaluating the Vulnerability of Network TrafficUsing Joint Security and Routing Analysis”,1545-5971/09/2009 IEEE

[10]. 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

[11]. 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

[12]. 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

[13]. ChakibBekara and Maryline L aurent-Maknavicius, “Defending Against Nodes Replication Attacks on Wireless Sensor Networks”

[14]. Ahmad Salehi S., M.A. Razzaque, ParisaNaraei, Ali Farrokhtala, “Security in Wireless Sensor Networks: Issues and Challenges”, Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013