IJRSET MARCH 2018 Volume 5, Issue 3 Pages: 11-17

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

REPLICATION ATTACK DETECTION IN WIRELESS SENSOR NETWORKS BY EFFICIENT NODE DEPLOYMENT

[1] A.C Charumathim, [2] M.VelumaniM.E., Ph.D.,
[1] Research Scholar, [2] Associate professor in computer science
[1, 2] Paavai Engineering College
[1, 2] Salem (DT), Tamilnadu.

ABSTRACT: Wireless sensor network is an emerging area in which multiple sensor nodes are deployed to perform monitoring tasks. Sensor nodes are deployed in an open environment or infrastructure which can be easily affected by number of mischievous attacks. Security is the important consideration in wireless sensor environment. Node replication attack is one of the dangerous types of attack in which attacker may generate the replica or clone of existing node in the same network by extracting all the credentials. In the node replication attacks the adversary captures the sensor node and extract the secret credentials. After extracting the secrets, duplicate the node and deploys in the duplicated node in the network. The duplicate node is called as clone nodes or replicated nodes. In Existing project LEACH (NI-LEACH) protocol to reduce the scale of the cluster by considering the residual energy of nodes and the optimal number of clusters. But need more security in this protocol. There may be case when the attacker replicates the whole cluster and attack the multiple nodes in one go. So, we use the Dynamic Secure Intrusion Detection Protocol model (DSIDP) detection method for defending against node replication attack. It is the intrusion detection process which is based on the monitoring nodes. The clustered network is taken into consideration in which clustering is done by underwater density based clustering sensor network (UWDBCSN) algorithm. The detection approach is integrated with sleep/wake scheduling algorithm to enhance the network performance.

KEY WORDS: [Wireless Sensor Networks (WSNs), Underwater Density Based Clustering Sensor Network (UWDBCSN), Dynamic Secure Intrusion Detection Protocol (DSIDP),Non-Deterministic And Fully Distributed (NDFD).]

1. INTRODUCTION

Wireless sensor networks (WSNs) are composed of a group of sensor nodes with limited resources. WSNs are usually deployed in harsh environments to fulfill military or civil tasks. Due to their operating nature, they are often unattended and generally lack effective ways against the tamper attack, hence they are vulnerable to most of new types of attacks. For example, an adversary could capture some network nodes, called clone nodes, to acquire the information stored there and replicate the messages transmitted by them, even tamper the local message such that it is difficult to find those clone nodes. Thus it is critical to ensure the security of wireless sensor networks.

In practice, sensor nodes can be easily captured, because they are usually unprotected by physical shielding due to cost considerations, and are often unattended after deployment. If we cannot detect these replicas, the network will be vulnerable to a large number of internal attacks. The threat of clone attack can be characterized from two aspects. First, a clone node is usually considered to be honest by its neighbors. In fact, without global countermeasures, honest nodes cannot be aware of the fact that there is a clone node among their neighbors. Second, besides the information of clone nodes can be copied, it can also be tampered with. Once a node has been captured and compromised, the attack will be sustained. It is very easy to make further clones of the same node. The node replication attack in a WSN. After the original node is captured by the attacker, all information is taken from the original node. The attacker then re-inserts this captured node to the network without any change.

LEACH (NI-LEACH) protocol to reduce the scale of the cluster by considering the residual energy of nodes and the optimal number of clusters. But some security issue in the existing protocol. In order to efficiently find the clone nodes, we need to reduce the scale of the cluster by appropriate clustering. However, most existing clustering protocols including LEACH select cluster heads in a random manner and do not consider the optimal number of clusters in large-scale WSNs.

In this Protocol having some Demeritsthe existing clone detection methods cannot adapt to the change of the network size and have low detection efficiency for clone nodes.For large-scale WSNs, it is difficult to find the positions of clone nodes since they may be at any position in the network.In existing System to implementing the anonymous communications to appropriate anonymous secure routing protocols.Lack of packet authentication.Difficult for the protocols to check whether a packet has been modified by a malicious node**.**In this attack the adversary access the internal state of the sensor node such as Secret information.

2. RELATED WORK

S. Guo, C. Wang, and Y. Yang says Joint mobile data gathering and energy provisioning in wireless rechargeable sensor networks the emerging wireless energy transfer technology enables charging sensor batteries in a wireless sensor network (WSN) and maintaining perpetual operation of the network. Recent breakthrough in this area has opened up a new dimension to the design of sensor network protocols. In the meanwhile, mobile data gathering has been considered as an efficient alternative to data relaying in WSNs. However, time variation of recharging rates in wireless rechargeable sensor networks imposes a great challenge in obtaining an optimal data gathering strategy. In this paper, we propose a framework of joint wireless energy replenishment and anchor-point based mobile data gathering (WerMDG) in WSNs by considering various sources of energy consumption and time-varying nature of energy replenishment.

C. Wang, J. Li, F. Ye, and Y. Yang says NETWRAP: An NDN Based Real-Time Wireless Recharging Framework for Wireless Sensor Networks Using vehicles equipped with wireless energy transmission technology to recharge sensor nodes over the air is a game-changer for traditional wireless sensor networks. The recharging policy regarding when to recharge which sensor nodes critically impacts the network performance. So far only a few works have studied such recharging policy for the case of using a single vehicle. In this paper, we propose NETWRAP, an NDN based Real Time Wireless Recharging Protocol for dynamic wireless recharging in sensor networks. The real-time recharging framework supports single or multiple mobile vehicles. Employing multiple mobile vehicles provides more scalability and robustness. To efficiently deliver sensor energy status information to vehicles in real-time, we leverage concepts

and mechanisms from NDN (Named Data Networking) and design energy monitoring and reporting protocols. We derive theoretical results on the energy neutral condition and the minimum number of mobile vehicles required for perpetual network operations. Then we study how to minimize the total traveling cost of vehicles while guaranteeing all the sensor nodes can be recharged before their batteries deplete.

M. Ma, Y. Yang, and M. Zhao, says Tour Planning For Mobile Data-Gathering Mechanisms In Wireless Sensor Networks In this paper we investigate the tour planning for mobile data gathering in wireless sensor node by introducing mobility into the network. An M-collector starts the data-gathering tour periodically from the static data sink, polls each sensor and then directly collects data from the sensor in single-hop communications, and transports it into the static sink. Our mobile data-gathering scheme improves the scalability and solves intrinsic problems. By introducing the M-collector, data gathering becomes more flexible and adaptable to the unexpected changes of the network topology. M-collector will separate each zone that will reduce the network faults. In addition, data gathering by Mcollectors is perfectly suitable for applications, where sensors are only partially connected. Proposed data-gathering scheme can greatly reduce the moving length compared with the covering line algorithm. In addition, it can prolong the network lifetime significantly compared with the scheme that has only a static data collector.

S. Umrao, D. Verma, and A. Tripathi, Says Detection and mitigation of node replication with pulse delay attacks in wireless sensor network: A survey Wireless Sensor Networks has collection of sensor nodes. The sensor nodes may be captured by the attacker because the nodes are spread out in unattended surroundings. The attacker collects all secret information such as key, secret credentials, etc. and replicates the node. This replicated node is also called as Clone node. In this paper, an attack called as node replication attack is discussed. The clone node or replicated node behaves as a legitimate node. The clone node can damage the network. In node replication attack, detecting the clone node is an important issue in Wireless Sensor Networks. In this survey, the existing detection schemes by researchers are discussed.

Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, says Random-walk based approach to detect clone attacks in wireless sensor networks Wireless sensor networks (WSNs) deployed in hostile environments are vulnerable to clone attacks. In such attack, an adversary compromises a few nodes, replicates them, and inserts arbitrary number of replicas into the network. Consequently, the adversary can carry out many internal attacks. Previous solutions on detecting clone attacks have several drawbacks. First, some of them require a central control, which introduces several inherent limits. Second, some of them are deterministic and vulnerable to simple witness compromising attacks. Third, in some solutions the adversary can easily learn the critical witness nodes to start smart attacks and protect replicas from being detected. In this paper, we first show that in order to avoid existing drawbacks, replica-detection protocols must be non-deterministic and fully distributed (NDFD), and fulfill three security requirements on witness selection. To our knowledge, only one existing protocol, Randomized Multicast, is NDFD and fulfills the requirements, but it has very high communication overhead. Then, based on random walk, we propose two new NDFD protocols, RAndomWaLk (RAWL) and Table-assisted RAndomWaLk (TRAWL), which fulfill the requirements while having only moderate communication and memory overheads.

Z. Li and G. Gong says Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks Wireless sensor networks are resource constrained and vulnerable to various kinds of attacks. In this

paper we study node clone attack. Many solutions came into existence and for detecting this attack. Many solutions need assumptions to have the problem solved in large-scale deployment of sensors. They have tradeoffs between the solutions provided and network conditions. Recently Li and Gong proposed two protocols for node clone detection with different tradeoffs with network conditions. Distributed Hash Table (DHT) was used to have distributed mechanisms for node clone detection. Due to the overhead caused by DHT, they proposed another protocol that overcomes this problem. In this paper, we implement a novel mechanism that can detect node clone attack in wireless sensor networks. We made simulations in NS2 to demonstrate the proof of concept.

3. PROBLEM DESCRIPTION

Wireless Sensor Networks has collection of Sensor Nodes. It is used in more applications such as environmental monitoring, habitat monitoring and object tracking. The sensor nodes may be captured by an adversary because the sensor nodes are spread out in unattended surroundings. The main common attacks in sensor network are clone attack, man in the middle attack, Sinkhole, Jamming, tampering, flooding, wormhole attack, routing attack, sybil attack, Denial of Service attack.

The replication attacks injurious in many parts of the networks such as misbehavior activities, extra resource allocation, falsifying sensor data etc.

The duplicated node can be inserted into any location in the network. If the replicated node is not detected, then it leads to different attacks. The clones extract information from the network and collects all the secret information. And also it disconnects the network or jamming the network

Detecting Replicated node is a difficult task. For detecting the node replication attacks a few schemes have been proposed. The proposed detection technique should be energetic and memory demanding because the sensor nodes are resource constrained.

In this paper the node replication attacks is organized.

4. SYSTEM MODEL

Wireless sensor network (WSN) consists of large number of tiny sensor nodes randomly distributed in some regions. Each node has a limited energy supply and generates information. It has been proved that the nodes closer to the sink node will use up their energy more quickly, as a result, the network lifetime will be affected. Due to inhospitable conditions these sensors are not always deployed uniformly in the area of interest. Therefore, how to optimize the network lifetime and keeping energy efficiency improving becomes an important problem. Here we use the **Dynamic Secure Intrusion Detection Protocol** model **(DSIDP)** detection method for defending against node replication attack. This model improves the lifetime of the network with enhanced energy efficiency and improved communication. Here we also propose a Energy saving data gathering method for wsn with less energy consumption and faster data transmission. In this paper performance has been analyzed for the above Clustering protocols in WSN. So the sensor nodes have to be more energy efficient and timely work done method. In complex time critical application, the need of improved energy efficient routing technique is an important issue. At the same time we have to design a model with lower energy budget and also increase the network life time to a significant level.

Data aggregation protocols aims at eliminating redundant data transmission and thus improve the lifetime of energy constrained wireless sensor network. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks (WSN) offer an increasingly attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity.

The proposed detection technique should be energetic and memory demanding because the sensor nodes are resource constrained. This project proposed Random Key distribution for node replication detection attack. Data aggregation protocols aims at eliminating redundant data transmission. Trouble-free for the protocols to check whether a packet has been modified by a malicious node. If the usage of keys exceeds the criteria or threshold value, then it is assigned as a replicated node. The verification is with base station and the nearest sensors, which has high detection rate.

5. SYSTEM MODULES

1. **Node Creation**
2. **Creating Base Node**
3. **Cluster Node**
4. **Trusted Node**

6. PROJECT DESCRIPTION

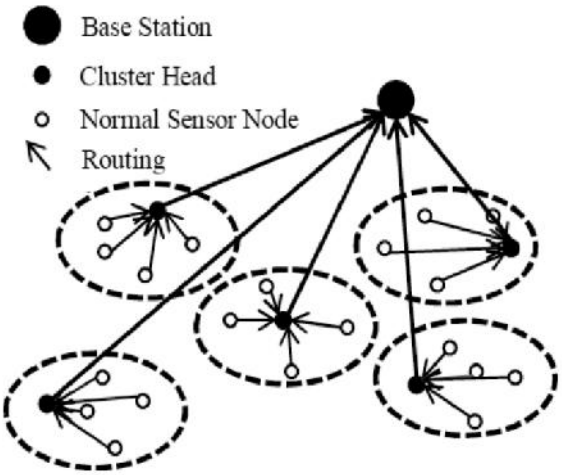
1. Node Creation

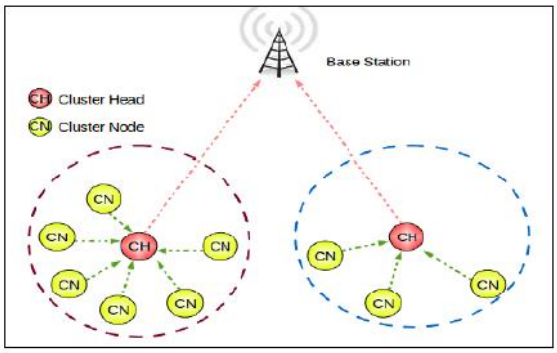
In a network, a node is a connection point, either a redistribution point or an end point for data transmissions. In general, a node has programmed or engineered capability to recognize and process or forward transmissions to other nodes.

2. Creating Base Node

A **node** is a basic unit used in computer science. Nodes are devices or data points on a larger network. Devices such as a personal computer, cell phone, or printer are nodes. When defining nodes on the internet, a node is anything that has an IP address. Nodes are individual parts of a larger data structure, such as linked lists and tree data structures. Nodes contain data and also may link to other nodes. Links between nodes are often implemented by pointers.

Architecture Diagram





3.Cluster Node

Beyond the basic definition of a node, the administrator can also describe the node's attributes, such as how much RAM, disk, what OS or kernel version it has, perhaps even its physical location. This information can then be used by the cluster when deciding where to place resources. The cluster node command is used to administer a node in a server cluster or to view its status. Used without parameters, **cluster node** defaults to the **/status** command-line option and displays the status for all nodes is displayed.

4.Trusted Node

The Trusted Node feature enables you to enforce more restrictive security parameters when dealing with specific nodes in your network, enabling you to define each adjacent node in the network map as internal or external in its relationship to the local node of

that network map. When a Process begins execution, the security exit gets control and a bit in the Security Control. If the adjacent node is defined, the bit turns off. Based on this information, the administrator can code the security exit to take the appropriate action.

7. TECHNIQUES AND ALGORITHM

Dynamic Secure Intrusion Detection Protocol model (DSIDP) and UWDBCSN

Step 1: Initial setup is to design the network as less hop count transmission.

Step 2: Design a CH(ClusterHead) from the sensor devices (here we are setting ClusterHead(CH) which can receive the data from number of nodes).

Step3: if sensor having the data, then sensor finding the CH, which is near to that sensor.

Step 4: if sensor found any CH point node is available then transfers data to CH

Step 5: if CH has more data then it informs to Base station.

Step 6: Base station receives the number of control information from different CH's.

Step 7: Node can be dedicated to a particular special function such as relaying, sensing and aggregation helps in reducing number of communications by using some aggregate functions like suppression (eliminating duplicates), min, max and average.

Step 8: after collecting the control message, BS makes the shortest route to collect the data from CH's.

Step 9: BS moves towards each CH's and collects the info and returns back to CH.

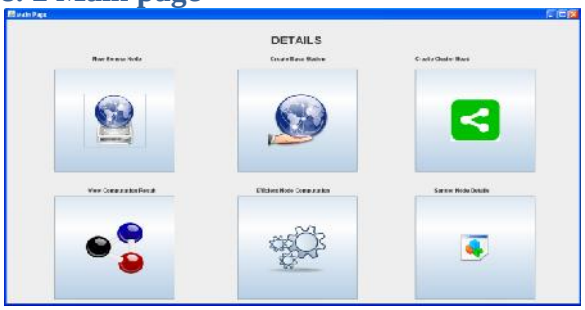
Implement cluster based technique to detect and eliminate malicious node from the network

8. PARTIAL RESULTS

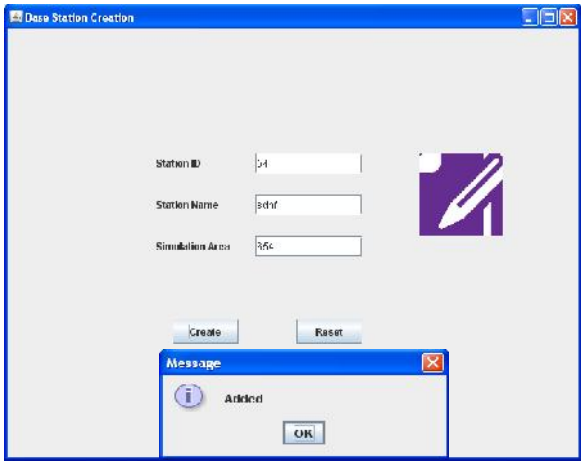
Sample Screen Shots

8. 1 Login

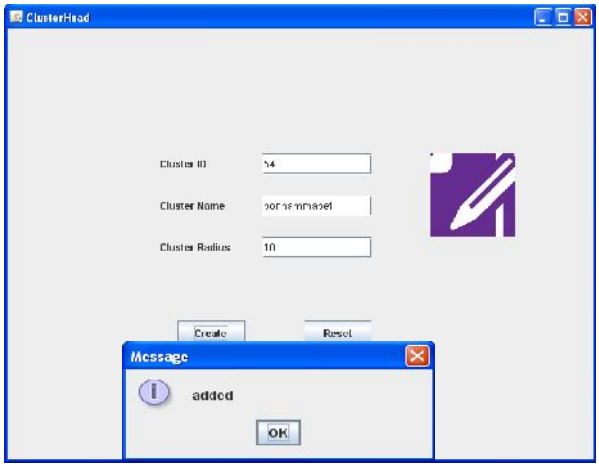
8. 2 Main page



8. 3 Base Station Creation



8. 4 Cluster Head



CONCLUSION

Detecting node replication attack is a very important issue in sensor networks. This paper reviews about the scheme which is discussed by the researchers for detecting node replication attack. There should be some more identification schemes in addition to the various algorithms produced by researchers related to node replication attack detection. An efficient solution should be developed to defend against this attack.

REFERENCES

[1]. S. Guo, C. Wang, and Y. Yang, "Joint mobile data gathering and energy provisioning in wireless rechargeable sensor networks," IEEETransactions on Mobile Computing, pp. 2836–2852, 2014.

[2]. C. Wang, J. Li, F. Ye, and Y. Yang, "Netwrap: An ndn based realtime wireless recharging framework for wireless sensor networks," IEEE Transactions on Mobile Computing, pp. 1283–1297, 2014.

[3]. M. Ma, Y. Yang, and M. Zhao, "Tour planning for mobile datagathering mechanisms in wireless sensor networks," IEEE Transactionson Vehicular Technology, pp. 1472–1483, 2013.

[4]H. Choi, S. Zhu, and T. r. La Porta, "Set: Detecting node clones in sensor networks," Proc. 3th International Conference on Security andPrivacy in Communications Networks and the Workshops, pp. 341–350, Sept 2007.

[5]. Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," Proc.IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, pp. 677–691, June 2010.

[6]. Z. Li and G. Gong, "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks," Proc. 6th IEEEInternational Conference on Mobile Adhoc and Sensor Systems, pp. 1030–1035, Oct 2009.

[7]. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," Proc. 9th ACM Conference on Computerand Communications Security, pp. 41–47, 2002.

[8]. A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," Proc. 1th Inthernational Workshop on Quality of Service &Secutity in Wireless and Mobile Networks, pp. 16–23, 2005.

[9]. H. Choi, S. Zhu, and T. r. La Porta, "Set: Detecting node clones in sensor networks," Proc. 3th International Conference on Security andPrivacy in Communications Networks and the Workshops, pp. 341–350, Sept 2007.

[10]. K. Xing, F. Liu, X. Cheng, and D. Du, "Real-time detection of clone attacks in wireless sensor networks," Proc. 28th InternationalConference on Distributed Computing Systems, pp. 3–10, June 2008.

[11]. X. Wang and J. Wong, "An end-to-end detection of wormhole attack in wireless ad-hoc networks," Proc. 31th Annual IEEE InternationalConference on Computer Software and Applications, vol. 1, pp. 39–48, July 2007.

[12]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proc.6th Annual InternationalConference on Mobile Computing and Networking, pp. 255–265, 2000.