Replication Attack Detection by Using Intrusion Detection System

M.Rajalakshmi[1] and Dr.C.Parthasarathy[2]
[1] Research scholar, Department of Computer science and Engineering, SCSVMV, Tamilnadu, India
[2]Assistant Professor, Department of Computer Science and Applications, SCSVMV, Tamilnadu, India
E-Mail: rajidmi@gmail.com , drsarathy45@gmail.com

Abstract

Wireless sensor networks are deployed in dense areas where intruders capture the sensor nodes physically. The captured nodes are replicated as many nodes take control of the entire network area. A solution has been introduced to rectify this attack. However, these solutions have low efficiency to detect the clone nodes fast due to the lack of changing with the network size. In order to discover the clone nodes fast, in this paper, an algorithm is developed in addition with the improved LEACH called NI-LEACH protocol which is used to minimize the cluster by taking the energy of each node and the minimum number of clusters. In addition to this protocol, an IDS (intrusion detection system) algorithm is designed and developed to detect the replication attacks by assigning monitor nodes in the wireless sensor network. Simulation results show that the new algorithm is simple and efficient to implement in wireless sensor networks. A malicious node can be continuously monitored and detected with high probability ratio and also achieving optimal throughput simultaneously. The capacity of the network is increased drastically by using this algorithm against the clone node attack by intruders.

Keywords: WSN, intruder, replication attack, energy consumption.

I. INRTODUCTION

Wireless sensor networks (WSNs) are collection of hundreds or thousands of sensor nodes which are deployed in dense or hostile environments to fulfill military or civil tasks.

The sensor nodes have many limitations due to its tiny nature. They are mostly deployed in dense and unattended areas to monitor and capture the data. The sensor nodes can be easily tampered and hence it is vulnerable to many types of attacks.

For example, an attacker captures some nodes called clone nodes which behave same way as legitimate node. By using this clone node the attacker receives the information stored in the legitimate node and replicates the data which is already transmitted over a period of time. It tampers the data so that it is not easy to detect such clone nodes. Thus it is very difficult to provide the security for wireless sensor networks against these attacks.

In practice, it is difficult and leads to high cost to protect the sensor nodes using physical shielding protection, so the sensor nodes are easily captured by the attackers. They are often unattended after deployment because it is not possible to attend some areas physically. The network will lead to a large number of internal attacks if we did not detect this replication attack as it is vulnerable to this type of attack.

The clone attack threat mechanism can be categorized using two features. First, a clone node usually acts as an original node to attract its surrounding nodes. There are thousands of nodes in each network and the legitimate nodes are not aware of the clone node surrounded by it. Secondly the clone node copied the information in which it is tampered. Once a node becomes clone node the data in it can be captured, compromised and copied. So it is easy to create further clone nodes in this network. The information stored in the original node is easily captured by intruders and the information is copied. The intruders again insert the captured clone nodes in the same network without performing any modifications.

There has been some work in the literature on node attack detection methods and detection of node replication in static WSNs. However, most of the existing clone detection methods cannot adapt to the change of the network size and have low detection efficiency for clone nodes. Moreover, although most of the methods are easy to implement in a centralized manner, they cannot handle the attack in which both the data transmission nodes and the cluster head nodes are captured at the same time.

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 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 paper, an improved LEACH (NILEACH) protocol to determine the optimal scale of the cluster and enhance the detection efficiency is proposed. Compared to the original LEACH protocol, the proposed NI-LEACH protocol has the following features. First, the optimal number of clusters in a network is taken into consideration which not only affects the energy consumption of data transmission, but also determines the efficiency of discovering clone nodes. Furthermore, to ensure energy balance, the residual energy of nodes in the NI-LEACH is introduced so that in each round a node with more energy should have higher probability to become a cluster head.

Furthermore, an intrusion detection algorithm is introduced to address the problem of replication attacks by quickly determining the replicated nodes in the clustered network. The intrusion detection algorithm consists of four steps: preprocessing, selecting monitor nodes, observing data transmission nodes, and monitoring cluster head nodes.

In order to improve the accuracy of detection, the concept of monitor nodes in the algorithm is introduced so that we can observe the message transmission and the behavior of cluster heads. Simulation results show that the introduced algorithm is effective to detect the replication attack of sensor nodes in WSN.

In Section II, there is the Introduction of the related work. Then in Section III, algorithm along with an improved LEACH protocol is discussed.

II. RELATED WORK

The base station which is centralized is used to detect clone nodes by replication attacks. A solution to this problem is sending a list of neighbor's node list to each and every node and the list includes the locations of each node to a BS. The base station compares the list stored in it. If the same ID is present in two lists, then the clone node is detected. Then the base station revokes the clone node by the replication attack.

This solution has few limitations; the first one is the presence of a single point of failure and high communication cost due to the large number of messages during transmission of data. Other solutions rely on local detection. A voting method is used within neighborhood nodes to check whether the neighboring node is legitimate. But this solution fails to find the clone nodes that are not within the same neighborhood in WSN.

III. SCOPE OF THE PAPER

In this paper, an improved LEACH (NILEACH) protocol is proposed to determine the optimal scale of the cluster and enhance the detection efficiency. Compared to the original LEACH protocol, the proposed NI-LEACH protocol has the following features:

First, it is considered the optimal number of clusters in a network, which not only affects the energy consumption of data transmission, but also determines the efficiency of discovering clone nodes. Furthermore, to ensure energy balance, it is introduced as the residual energy of nodes in the NI-LEACH so that in each round a node with more energy should have higher probability to become a cluster head.

IV. EXISTING SYTEM

There are many review works of the previous methods of detecting clone nodes in WSNs. The base station which is centralized is used to detect clone nodes by replication attacks. A solution to this problem is sending a list of neighbor's node list to each node and the list includes the locations of each node to a BS. The base station compares the list stored in it. If the same ID is present in two lists, the clone node is detected. Then the base station revokes the clone node by the replication attack.

This solution has few limitations; the first one is the presence of a single point of failure and high communication cost due to the large number of messages during transmission of data. Other solutions rely on local detection. A voting method is used within neighborhood nodes to check whether the neighbor node is legitimate. But this solution fails to find the clone nodes that are not within the same neighborhood in WSN.

DRAWBACKS

However, most of the existing clone detection methods cannot adapt to the change of the network size and have low detection efficiency for clone nodes.

V. PROPOSED SYSTEM

First, the proposed algorithm with an improved LEACH (NI LEACH) protocol is to determine the optimal scale of the cluster and enhance the detection efficiency. This paper has an algorithm and the design of an intrusion detection algorithm to address the problem of replication attacks, by quickly determining the replicated nodes in the clustered network.

ADVANTAGES

In order to improve the accuracy of detection, it is also introduced as the concept of monitor nodes in our algorithm so that it is possible to observe the message transmission and the behavior of cluster heads.

PROPOSED SYSTEM TECHNIQUE

In this section, we propose an improved LEACH protocol called NI-LEACH. Many researchers' works indicate that a node which consists of minimum ratio of probability cane be selected as cluster node to function in WSN. Such nodes are uniformly distributed in the network.

After assigning cluster nodes in the network, the monitor nodes are selected by intrusion detective algorithm. To detect the misbehavior of malicious nodes efficiently, many misbehavior detective algorithms were designed by many researchers for the honest or trust nodes where each cluster has one monitor node only to detect the presence of clone in the network.

But in practice there are multiple monitor nodes present in the network to reduce the probability of miss-detection and also the energy consumed by all the nodes.

The monitor nodes are responsible for observing the transmission of sending data between the nodes in the network and also to observe the behavior of cluster heads. So, the energy consumption is increased by multiple monitor nodes. The number of monitor nodes is an important factor to reduce the energy consumption.

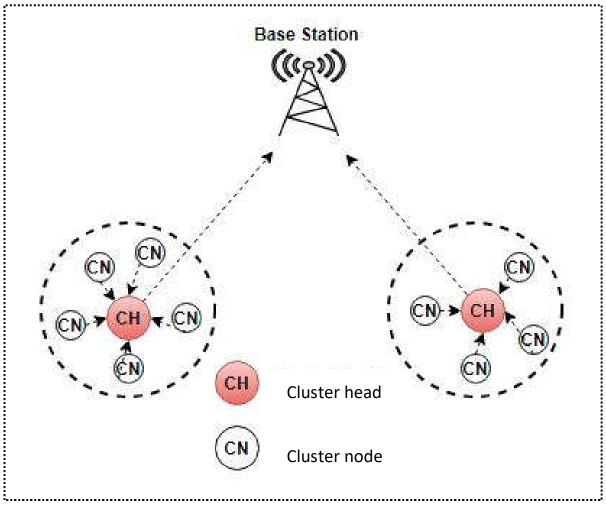

Fig 1: Cluster formation of network

In this paper, the algorithm is designed in such a way that energy consumption and detection range of each node is considered to select the monitor nodes. Each cluster has a separate monitor node to cover the cluster. Our objective is to find an appropriate set of monitor nodes, denoted by S, in each cluster so as to minimize the total energy consumption.

VI. LITERATURE SURVEY

Title Insider Attacker Detection in Wireless Sensor Networks

Authors Fang Liu & Xiu zhen Cheng

Year 2007

Descriptions Though dangerous to organize capacities, insider assailants are not discernible with just the great cryptography based methods. Numerous mission-faultfinder sensors organize applications that request a viable, light, adaptable calculation for the inner- enemy- recognizable- proof with just confined data accessible.

The insider assailant location plot proposed in this paper meets every one of the necessities by investigating the spatial connection existent among the systems administration practices of sensors in nearness. Our work is exploratory in that the proposed calculation considers various traits all the while in hub conducted assessment, with no prerequisite on an earlier learning about ordinary/malignant sensor exercises.

Also, it is application neighborly, which utilizes unique estimations from sensors and can be utilized to screen numerous parts of sensor organizing practices. Our calculation is absolutely limited, fitting great to the extensive scale sensor systems. Reenactment results demonstrate that inner enemies can be related to a high exactness and a low false alert rate when upwards of 25% sensors are getting out of hand.

Title Tour Planning for Mobile Data-Gathering Mechanisms in Wireless Sensor Networks

Authors Ming Ma, Yuanyuan Yang sue

Year 2013

Descriptions In this paper, we propose another information gathering instrument for substantial scale remote sensor organizes by bringing versatility into the system. A portable information authority, for accommodation called a M-gatherer in this paper, could be a versatile robot or a vehicle furnished with a ground-breaking handset and battery, working like a versatile base station and assembling information while traveling through the field.

An M-gatherer begins the information gathering visit occasionally from the static information sink, surveys every sensor while navigating its transmission go, at that point specifically gathers information from the sensor in single-bounce interchanges, lastly transports the information to the static sink. Since information parcels are straightforwardly accumulated without transfers and impacts, the lifetime of sensors is relied upon to be delayed. In this paper, we principally center around the issue of limiting the length of every datum gathering visit and allude to this as the single-bounce information gathering issue (SHDGP). We initially formalize the SHDGP into a blended whole number program and after that present a heuristic visit arranging calculation for the situation where a solitary M-gatherer is utilized. For the applications with strict separation/time imperatives, we consider using different M-authorities and propose an information gathering calculation where numerous M-gatherers cross through a few shorter subs visits simultaneously to fulfill the separation/time limitations.

Our single-bounce versatile information gathering plan can enhance the adaptability and equalization the vitality utilization among sensors. It very well may be utilized in both associated and detached systems.

Recreation results exhibit that the proposed information gathering calculation can enormously abbreviate the moving separation of the authorities contrasted and the covering line -guess calculation and are near the ideal calculation for little systems. Likewise, the proposed information gathering plan can fundamentally drag out the lifetime contrasted system and a system with static information sink or a system in which the portable gatherer can just move along straight lines.

Title Detection and Mitigation of Node Replication with Pulse Delay Attacks in Wireless Sensor Network

Authors Sachin Umarao

Year 2013

Descriptions Wireless sensor network (WSN) is made up of at least two interconnected sensor hubs remotely. These hubs might be conveyed either in open or shut condition. As these hubs convey remotely and sent in open condition there is dependably the danger of security of hubs and also information imparted. With a specific end goal to making secure correspondence over WSN there ought to be some security instrument. In this paper a typical security instrument is proposed to alleviate, beat, postpone, assault and hub replication. This component incorporates recognition and after that alleviation.

VII. MODULES

WSN Architecture

The following diagram is the network animator (NAM). The NAM window appears when the code is executed

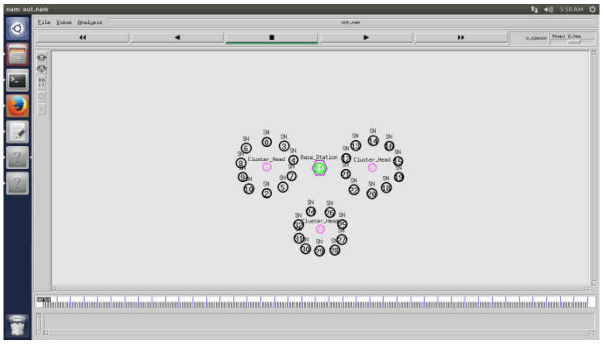

Fig 2: NS2 network creation

This is WSN architecture as shown by the NAM window; here the network has a group of nodes and each group has a cluster head which is the point of contact for all nodes in the cluster and all cluster heads communicate with the base station.

Node To Node Communication

Here the nodes communicate with each other, but this communication happens only within the cluster. The nodes cannot communicate with nodes in the other cluster group. The communication between nodes is denoted by the circles in the NAM diagram.

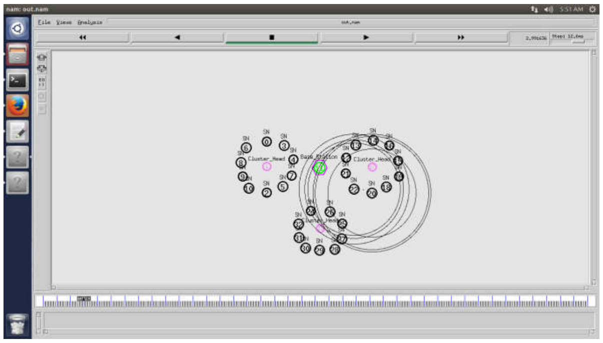

Fig 3: Data transmission between nodes

Capture Node

Capturing a node is the first step of a replication attack .First a node is captured and the data is copied and then only replicated.

The replicated node is the clone of the captured node.

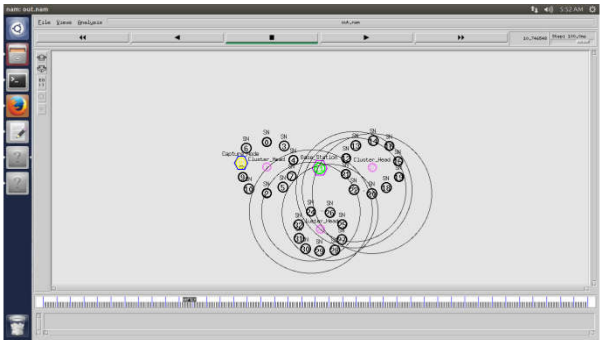

Fig 4: Finding replicating node in a network

Clone Node

After the node is captured and copied, the clone node is formed; the clone node is the replica of the captured node.

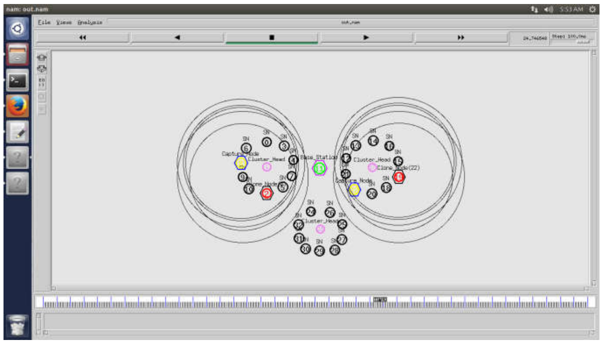

Fig 5: Formation of clone node

Energy Consumption

Since the nodes only communicate with the cluster heads and not with each other the node the transmission time is less and therefore the energy consumption is less. Hence they are energy efficient.

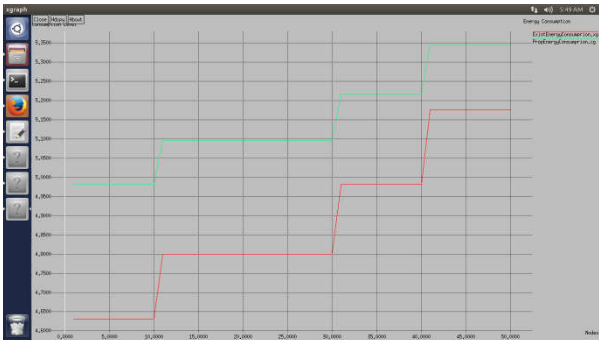

Fig 6: Graph for Energy consumption

Node Detection

Ordinary node detection is time consuming, but since it uses intrusion detection methodology, the time consumed to detect a node is less. The main aim of LEACH protocol is intrusion detection.

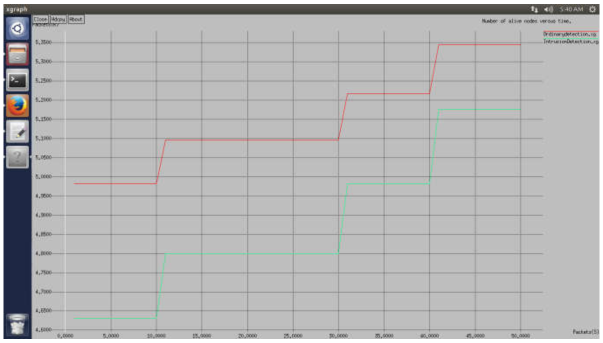

Fig 7: Graph for Number of live nodes

VIII. FUTURE ENHANCEMENTS

There are several challenging issues in our future work. First, we need to take into account how to detect the attack in the presence of multiple colluding adversaries. Second, we need to further study how the efficiency of detection can be affected when the monitor nodes have been captured.

IX. CONCLUSIONS

In this paper, the problem of clone nodes detection in wireless sensor networks is studied. Multiple monitor nodes are introduced into the detection process, where monitor nodes can observe the data transmission of all the nodes and the behavior of head clusters.

By choosing the encoder function properly, it shows that an attacker will be detected with high probability, and that the effective throughput provided by this detection algorithm can arbitrarily approach the optimum. Besides, along with the algorithm, an improved cluster protocol to cluster the network. The algorithm and improved leach protocol can improve the detection efficiency of the network and reduce the detection time. Meanwhile, the infected areas can be quickly isolated by our cluster protocol.

REFERENCES

[1] Guo S. et.al (2014) ‘Joint mobile data gathering and energy provisioning in wireless rechargeable sensor networks’, IEEE Transactions on Mobile Computing, pp. 2836–2852.

[2] Wang C. , Li J. and Yang Y. (2014) ‘Netwrap: An ndn based real time wireless recharging framework for wireless sensor networks’, IEEE Transactions on Mobile Computing, pp. 1283–1297.

[3] Ma M., Yang Y., and Zhao M. (2013) ‘Tour planning for mobile data gathering mechanisms in wireless sensor networks’, IEEE Transactions on Vehicular Technology, pp. 1472–1483.

[4] Akyildiz I., et.al (2002) ‘A survey on sensor networks’, IEEE Communications Magazine, Vol 40, No. 8, pp. 102–114.

[5] Becher A., et.al (2006) ‘Tampering with motes: Real-world physical attacks on wireless sensor networks’, Security in Pervasive Computing, Vol 3934, pp. 104–118.

[6] Parno B. ,et.al (2005) ‘Distributed detection of node replication attacks in sensor networks’, IEEE Symposium on Security and Privacy, pp. 49–63.

[7] Liu F., et.al (2007) ‘Insider attacker detection in wireless sensor networks’, IEEE International Conference on Computer Communications., pp. 1937–1945.

[8] Umarao S., et.al (2013) ‘Detection and mitigation of node replication with pulse delay attacks in wireless sensor network: A survey’, Proc. 2013 IEEE International Conference in MOOC Innovation and Technology in Education, pp. 390–392.

[9] Zhao yulan and Jiang chunfeng (2011) ‘Research about improvement of LEACH protocol’, The 2nd International conference on Information science and Engineering, IEEE.

[10] Sivakumar P. and Radhika M. (2017) ‘Performance analysis of LEACH-GA over LEACH and LEACH-C in WSN’, 6th International conference on smart computing and communications, Procedia computer science , Vol 125, pp 248-256.

[11] Deepika et al. (2016) ‘A Research paper on security enhancement in LEACH protocol’, International journal of Engineering development and research, Vol 4, ISSN: 2321-9939.