International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

ERCD: Energy and Memory Dynamic Clone Detection in Wireless Sensor Networks

Varadi Lakshmi
M.Tech, Department of Computer Science and Technology, SRKR Engineering College, Bhimavaram, West Godavari, Andhra Pradesh, India.

Abstract: In this scheme, an energy-efficient location-aware clone detection protocol is proposed in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and dynamically select witnesses located in a mesh area to verify the legitimacy of sensors and to report detected clone attacks. The mesh structure facilitates energy-efficient data forwarding along the path towards the source and the sink. We also propose the clone detection for mobile nodes in the mesh network using location estimation and simulation results are plotted for both static and dynamic network.

Keywords: Wireless sensor networks, clone detection protocol, energy efficiency, network lifetime.

1. INTRODUCTION

Wireless sensors have been widely deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, etc. For cost-effective sensor placement, sensors are usually not tamper-proof devices and are deployed in places with-out monitoring and protection, which makes them prone to different attacks. For example, a malicious user may compromise some sensors and acquire their private information. Then, it can duplicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks , which is referred to as the clone attack . As the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors, they can easily participate in network operations and launch attacks. Due to the low cost for sensor duplication and deployment, clone attacks have become one of the most critical security issues in WSNs. Thus, it is essential to effectively detect clone attacks in order to ensure efficient operation of WSNs. To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network.

The private information of the source node, i.e., identity and the location information, is shared with witnesses at the stage of witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification.

To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses should be dynamically selected; and

2) At least one of the witnesses can successfully receive all the verification message(s) for clone detection.

The first requirement is to make it difficult for malicious users eavesdrop the communication between current source node and its witnesses, so that malicious users cannot generate duplicate verification messages. The second requirement is to make sure that at least one of the witnesses can check the identity of the sensor nodes to determine whether there is a clone attack or not. To guarantee a high clone detection probability, i.e., the probability that clone attacks can be successfully detected, it is critical and challenging to fulfill these requirements in clone detection protocol design.

Different from wireless terminal devices, wireless sensors are usually of smaller size and lower price, and have limited battery and memory capacity. In the literature, some distributed clone detection protocols have been proposed, such as Dynamic and Distributed protocol (DDP) and Line-Select Multicast protocol (LSM) . However, most approaches mainly focus on improving clone detection probability without considering efficiency and balance of energy consumption in WSNs. Such requirement makes the existing protocols not so suitable for densely-deployed WSNs. Most existing approaches can improve the successful clone detection at the expense of energy consumption and memory storage, which may not be suitable for some sensor networks with limited energy resource and memory storage.

In this besides the clone detection probability, I also consider energy consumption and memory storage in the design of clone detection protocol, i.e., an energy-and memory-efficient distributed clone detection protocol with dynamic witness selection scheme in WSNs. Our protocol is applicable to general densely deployed multi-hop WSNs, where adversaries may compromise and clone sensor nodes to launch attacks and nodes are mobile in nature. A preliminary work is presented.

In that work, I proposed an energy-efficient mesh based clone detection (EMCD) protocol to achieve high clone detection probability with dynamic witness selection, while ensuring normal network operations with satisfactory network lifetime of WSNs. EMCD protocol is an enhancement of ERCD where nodes are static and follow ring structure, in EMCD nodes are mobile and dynamically select the witness. The EMCD protocol can be divided into two stages: witness selection and legitimacy verification.. If multiple copies of verification messages are received, the clone attack is detected and a revocation procedure will be triggered I find that the EMCD protocol can balance the energy consumption of sensors at different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings around the sink, which should not have witnesses. After that, we obtain the optimal number of non-witness rings based on the function of energy consumption. Extensive simulation results demonstrate that our proposed EMCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.

2. RELATED WORK

As one of the utmost important security issues, clone attack has attracted people's attention. There are

many works that studies clone detection protocols in the literature, which can be classified into two different categories, i.e., centralized and distributed clone detection protocols. In centralized protocols, the sink or witnesses generally locate in the center of each region, and store the private information of sensors. When the sink or witnesses receive the private information of the source node, they can determine whether there is a clone attack by comparing the private information with its pre-stored records. Normally, centralized clone detection protocols have low overhead and running complexity. However, the security of sensors' private information may not be guaranteed, because the malicious users can eavesdrop the transmission between the sink node and sensors. Moreover, the network lifetime may be dramatically decreased since the sensor nodes close to the sink will deplete their energy sooner than other nodes. Different from centralized protocols, in distributed clone detection protocols, a set of witnesses are selected to match with every sensor, which prevents the transmission between the sink and sensors from being eavesdropped by malicious users. There are three different types of witness selection schemes in distributed clone detection protocols: i) deterministic selection, ii) dynamic selection, and iii) semi-dynamic selection.

The deterministic witness selection based clone detection protocols like DDP choose the same set of witnesses for all sensor nodes. By using deterministic witness selection, a low communication overhead and a high clone detection probability can be achieved. In addition, the required buffer storage capacity of such protocols is very low, which is only related to the number of witnesses without considering network scale and node density. Nevertheless, due to the deterministic characteristic, the mapping function can be easily obtained and a variety of attacks may be launched by malicious users. To enhance the network security, the distributed clone detection protocols with dynamic witness selection like LSM are proposed, which are closely related to our work. In dynamic witness selection, it is difficult for malicious users to acquire the information of witnesses since the witnesses of each sensor are dynamically generated. However, the dynamisms of mapping function also increases the difficulty for the source node to reach its witnesses, which makes it challenging to achieve a high clone detection probability.

To ensure the clone detection probability, LSM lets all the nodes in the route between source and witnesses store the private information of the source node, which leads to a high requirement of data buffer and energy consumption. Thus, it is essential to guarantee the clone detection probability with low energy consumption and required buffer storage in clone detection protocols with dynamic witness selection approach. Other distributed clone detection protocols, such as Parallel Multiple Probabilistic Cells (P-MPC), proposed semi-dynamic witness selection approach trying to combine the advantages of both dynamic and deterministic witness selection approaches.

In this kind of witness selection scheme, a deterministic region is generated for the source node according to the mapping function, and then witnesses of the source node will be dynamically selected from the sensors in this region. However, the

two phases witness selection and dynamisms of the witnesses for each sensor leads to a high overhead and time complexity. The energy consumption and the required buffer storage of such protocols are lower than the dynamic witness selection approach but higher than the deterministic ones. Overall, most previous works aim at maximizing the clone detection probability without considering the impact of proposed clone detection protocol on the network lifetime and required data buffer storage. In this paper, we carefully design a distributed clone detection protocol with dynamic witness selection by jointly considering the clone detection probability, network lifetime and data buffer capacity.

3. Problem Definition

The problem in Wireless Sensor Network is that sensor nodes are deployed in open environment, thus the battery is the major console for all the sensor nodes. Existing approaches mainly focus on improving clone detection probability without considering efficiency and balance of energy consumption in WSNs. With such kind of approaches, some sensors may use up their batteries due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs. The limited memory or data buffer is another important feature of sensors which has significant impact on the design of clone detection protocols. Generally, to guarantee successful clone detection, witnesses need to record source nodes' private information and certify the legitimacy of sensors based on the stored private information. In most existing clone detection protocols, the required buffer storage size depends on the network node density, i.e., sensors need a large buffer to record the exchanged information among sensors in a high-density WSN, and thus the required buffer size scales with the network node density. Such requirement makes the existing protocols not suitable for densely-deployed WSNs and existing approaches consider static network where nodes are stationary not dynamic in nature and uses public key cryptography for key exchange.

4. Proposed Model

In this section we describe about the clone detection mechanism to find the energy efficient clone attack in WSN. The complete modules have been discussed below.

I. Network Module:

In this work, we consider a network region with one base station (BS) and an enormous number of wireless sensor nodes dynamically distributed in the network. We use the sink node as the origin of the system coordinator. The network model can be simply extended into the case of multiple BSs, where different BSs use orthogonal frequency-division multiple access (OFDMA) to communicate with its sensor nodes. For each sensor, it has to accomplish the tasks of data collection as well as clone detection. In every data collecting cycle, sensors send the collected data to the sink node through multi-hop paths. To be capable of conducting legitimacy verification, every sensor has the same buffer storage capacity to store the information. Buffer storage capacity should be sufficient to store the private information of source nodes, such that any node can be selected as a witness. When the buffer storage of

the sensor node is full, the oldest information will be dropped to accept the latest incoming information. As nodes are dynamic in nature in each sensor node GPS is adopted to collect the location information of that node. In our network, the link level security can be guaranteed by employing a conventional bootstrapping cryptography scheme, and the sink node uses a powerful cryptography scheme, which cannot be compromised by malicious users. A key pair (a,b) is assigned to each node, where a and b are the node ID and secret key, respectively. All nodes share their ID information with other nodes in the network. If either side of the link is compromised by malicious users, the link key is compromised. Each sensor node knows the physical information and the relative locations of its neighbor nodes.

II. Energy Module:

Energy Model, as implemented in, is a node attribute. The energy model represents level of energy in a mobile host. The energy model in a node has a initial value which is the level of energy the node has at the beginning of the simulation. This is known as initial Energy. It also has a given energy usage for every packet it transmits and receives.

These are called tx Power and tr Power.

Consumed Energy of node $E = E_{tx} + E_{tr}$

Residual Energy= Initial Energy – Consumed Energy

The most straightforward formulation is to look at the total energy required to transport a packet over a multihop path from source to destination. The goal is to minimize, for each packet the total amount of energy by selecting a good route and nearby witness node to legitimacy verification. In this scheme, we focus on designing a distributed clone detection protocol with dynamic witness selection by jointly considering clone detection probability, network lifetime and data buffer storage. Initially, a small set of nodes are compromised by the malicious users. Utilizing the clone detection protocol, we aim at maximizing the clone detection probability, i.e., the probability that cloned node can be successfully detected, to ensure the security of WSNs; meanwhile, the sufficient energy and buffer storage capacity for data collection and operating clone detection protocol should be guaranteed, which means that the network lifetime, i.e., the period from the start of network operation until the first outage occurs should not be impacted by the proposed clone detection protocol with sensors' buffer storage. Overall, our objective is to propose a distributed clone detection protocol with dynamic witness selection in order to maximize the clone detection probability while the negative impact of network lifetime.

III. Clone Detection

In this section, we introduce our distributed clone detection protocol, namely EMCD protocol, energy efficient mesh based clone detection protocol which can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity. The EMCD protocol consists of two stages: witness selection and legitimacy verification.

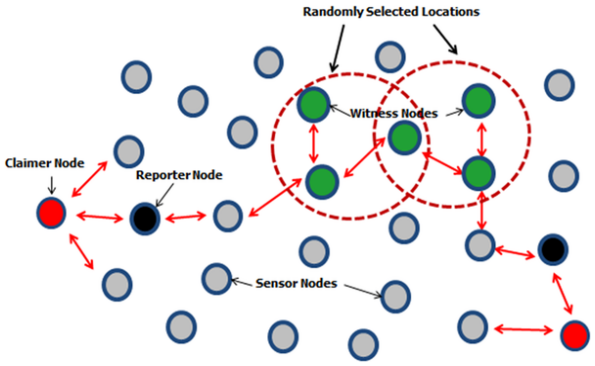

Fig:- Dynamically Selected witnesses in WSN

In witness selection, a dynamic mapping function is employed to help each source node dynamically select its witnesses. In the legitimacy verification, a verification request is sent from the source node to its witnesses, which contains the private information of the source node. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, where witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses. If the received messages are different from existing record or the messages are expired, the witness header will report a clone attack to the sink to trigger a revocation procedure.

Initially sensor node select nearby witness and collects location claims at witness nodes in each area and also in the center node to improve the probability of node replication detection while decrease the chance of dropping location claims by malicious nodes. A verification request is sent from the source node to its witnesses, which contains the private information of the source node. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, where witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses. If the received messages have same ID and key then witness header will report a clone attack to the sink to trigger a revocation procedure. In that revocation list information of clone nodes is presented.

5. Conclusion

In this scheme, we have proposed distributed energy-efficient clone detection protocol with dynamic witness selection. Specifically, we have proposed EMCD protocol, which includes the witness selection and legitimacy verification stages by considering different mobility patterns under various network scenarios. EMCD protocol use location information and private information for legitimacy verification. In addition our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.

6. References

[1] Z. Zheng, A. Liu, L. X. Cain, Z. Chen, and X. Sheen, “ERCD: An energy-efficient clone detection

protocol in WSNs," in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.

[2] M. Conti, R. D. Petro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans. Dependable. Secure Computer, vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[3] B. Par no, A. Per rig, and V. Gigot, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Sump. Security Privacy, Oakland, CA, USA, May. 8-11, 2005, pp. 49–63.

[4] Y. Zeng, J. Cao, S. Zhang, S. Goo, and L. Xian, "Dynamic-walk based approach to detect clone attacks in wireless sensor networks," IEEE J. Sel. Areas Common., vol. 28, no. 28, pp. 677–691, Jun. 2010.

[5] B. Zhu, S. Seta, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[6] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 793–806, May. 2012.

[7] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen., "BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 1, pp. 32–43, Jan. 2012.

[8] J. Li, J. Chen, and T. H. Lai, "Energy-efficient intrusion detection with a barrier of probabilistic sensors," in Proc. IEEE INFOCOM, Orlando, FL, USA, Mar. 25-30, 2012, pp. 118–126.

[9] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using dynamic key predistribution," IEEE Trans. Syst., Man, Cybern., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[10] W. Naruephiphat, Y. Ji, and C. Charnsripinyo, "An area-based approach for node replica detection in wireless sensor networks," in Proc. IEEE TrustCom, Liverpool, UK, Jun. 25-27, 2012, pp. 745–750.

[11] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in Proc. IEEE 17th Int. Conf. Netw. Protocols, Princeton, NJ, USA, Oct. 13-16, 2009, pp. 284–293.