USE OF CLONE DETECTION PROTOCOL IN WIRELESS SENSOR NETWORKS

Dheeraj Kumar Sikhwal
Assistant Professor, Department Of Computer Science Engineering
Shekhawati Institute Of Engineering And Technology, Sikar, Rajasthan, India

ABSTRACT: In this paper, we propose an energy-efficient location-aware clone detection protocol 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 randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. We theoretically prove that the proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98 percent when 10 percent of witnesses are compromised. Moreover, in most existing clone detection protocols with random witness selection scheme, the required buffer storage of sensors is usually dependent on the node density, i.e $O(\sqrt{n})$***, while in our proposed protocol, the required buffer storage of sensors is independent of n but a function of the hop length of the network radius h, i.e., O(h). Extensive simulations demonstrate that our proposed protocol can achieve long network lifetime by effectively distributing the traffic load across the network.***

I. INTRODUCTION

WIRELESS sensors have been widely deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, etc. [2], [3], [4]. For cost-effective sensor placement, sensors are usually not tamper-proof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks [5], [6], [7], [8], [9]. 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 [10], which is referred to as the clone attack [11], [12], [13]. 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 healthy 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 verifi- cation should fulfill two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection [11]. The first requirement is to make it diffi- cult 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. Therefore, the design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors. In the literature, some distributed clone detection protocols have been proposed, such as Randomized Efficient and Distributed protocol (RED) [10] and LineSelect Multicast protocol (LSM) [11]. However, most 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. To prolong network lifetime, i.e., time duration from the start of network until the first occurrence of a sensor that runs out of energy, it is critical to not only minimize the energy consumption of each node but also balance the energy consumption among sensors distributively located in different areas 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 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.

II. ERCD PROTOCOL

In this section, we introduce our distributed clone detection protocol, namely ERCD protocol, which can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity. The ERCD protocol consists of two stages: witness selection and legitimacy verification. In witness selection, a random mapping function is employed to help each source node randomly 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, network region is virtually divided into h adjacent rings, where each ring has a sufficiently large number of sensor nodes to forward along the ring and the width of each ring is r. To simplify the description, we use hop length to represent the minimal number of hops in the paper. Since we consider a densely deployed WSN, hop length of the network is the quotient of the distance from the sink to the sensor at the border of network region over the transmission range of each sensor, i.e., the distance of each hop refers to the transmission range of sensor nodes. Table 1 shows the mathematical symbols utilized in this section.

The ERCD protocol starts with a breadth-first search by the sink node to initiate the ring index, and all neighboring sensors periodically exchange the relative location and ID information. After that, whenever a sensor node establishes a data transmission to others, it has to run the ERCD protocol, i.e., witness selection and legitimacy verifi- cation, to verify its legitimacy. In witness selection, a ring index is randomly selected by the mapping function as the witness ring of node a. To help relieve the traffic load in hot spot, the area around the sink cannot be selected by the mapping function. After that, node a sends its private information to the node located in witness ring, and then the node forwards the information along the witness ring to form a ring structure. In the legitimacy verification, a verifi- cation message of the source node is forwarded to its witnesses. The ring index of node a, denoted Oa, is compared with its witness ring index Owa to determine the next forwarding node. If Ow a >Oa, the message will be forwarded to any node located in ring Oa þ 1; otherwise, the message will be forwarded to any node in ring Oa 1. This step can forward the message toward the witness ring of node a. The ERCD protocol repeats above operations until a node, denoted b, located in the witness ring Owa is reached. Node b stores the private information of node a and forwards the message to any node located in ring Ow a within its transmission range, denoted as c. Then, node c stores the information and forwards the message to the node d, where link ðc; dÞ has longest projection on the extension line of the directional link from b to c. The procedure will be repeated until node b reappears in the transmission range. Therefore, the witnesses of node a have a ring structure, consisting of b; c; :::b as shown in Fig. 1.

In the legitimacy verification, node a sends a verification message including its private information following the same path towards the witness ring as in witness selection. To enhance the probability that witnesses can successfully receive the verification message for clone detection, the message will be broadcast when it is very close to the witness ring, namely three-ring broadcasts, i.e., the message will be broadcast in Ow a 1, Ow a and Ow a þ 1 as shown in Fig. 2. In Theorem 1, we prove that the three-ring broadcasts can ensure the network security, i.e., the clone detection probability is one, under the assumption that all witnesses are trustful. To determine whether there exists a clone attack or not, all the verification messages received by witnesses are forwarded to the witness header along the same route in witness selection. The sensor nodes in the transmission route but not located in the witness ring are called the transmitters.

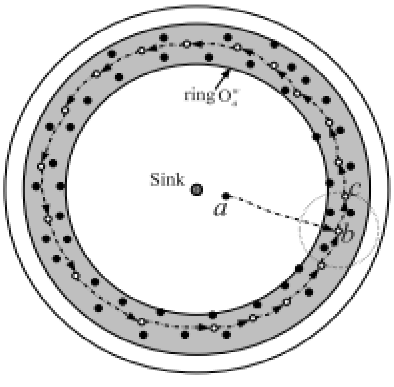

Fig. 1. Ring structure of witnesses.

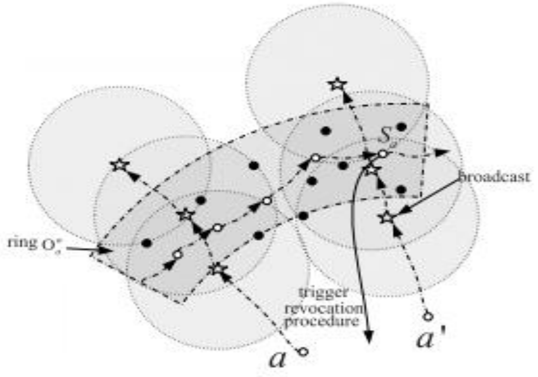

Fig. 2.Legitimacy verification.

The witness header of the source node a, denoted by Sa, is a sensor located in witness ring Ow a , meanwhile it is also in the communication range of the transmitter located in ring index $O_a^w - 1 \text{ or } O_a^w + 1$. The witness header Sa is randomly selected by the transmitter in the neighboring witness ring, i.e., the ring of $O_a^w - 1 \text{ or } O_a^w + 1$. If more than one copies or incorrect copies or expired copies are received by the witness header, the ERCD protocol will trigger a revocation procedure; if no copy is received from the source node due to packet loss or silent cloned node, transmissions from the source node will not be permitted.

Energy Consumption and Network Lifetime
In WSNs, since wireless sensor nodes are usually powered by batteries, it is critical to evaluate the energy consumption of sensor nodes and to ensure that normal network operations will not be broken down by node outage. Therefore, we define the network lifetime as the period from the start of network operation until any node outage occurs to evaluate the performance of the ERCD protocol. We only consider the transmission power consumption, as the reception power consumption occupies little percentage of total power consumption. Since witness sets in our ERCD protocol are generated based on ring structure, sensor nodes in the same ring have similar tasks. To simplify the analysis, we suppose that all sensor nodes in the same ring have same traffic load. Our analysis in this work is generic, which can be applied to various energy models. Let "1 and 1 denote the bit size of each collected data and the frequency of data collection, respectively. A node inside (outside) ring k refers to the node which locates in the ring with index smaller than (larger than) k. First, we analyze the traffic load of each sensor node, such that the energy consumption and network lifetime can be derived based on it. By using the ERCD protocol, traffic load of each sensor node consists of normal data collection, witness selection and legitimacy verification. We can derive the expression for the traffic load of normal data collection as follows.

III. CONCLUSION

In this paper, we have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. 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. In our future work, we will consider different mobility patterns under various network scenarios.

REFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, “ERCD: An energy-efficient clone detection protocol in WSNs,” in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.

[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, “GRS: The green, reliability, and security of emerging machine to machine communications,” IEEE Commun. Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[4] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, “Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks,” Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.

[5] T. Shu, M. Krunz, and S. Liu, “Secure data collection in wireless sensor networks using randomized dispersive routes,” IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, “A randomized countermeasure against parasitic adversaries in wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 28, no. 7, pp. 1036–1045, Sep. 2010.

[7] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs,” IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

[8] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, “An early warning system against malicious activities for smart grid communications,” IEEE Netw., vol. 25, no. 5, pp. 50–55, May. 2011.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, “A dynamic privacy-preserving key management scheme for location based services in VANETs,” IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.

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

[11] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symp. Security Privacy, Oakland, CA, USA, May. 8-11, 2005, pp. 49–63.

[12] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-walk based approach to detect clone attacks in wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 28, no. 28, pp. 677–691, Jun. 2010.

[13] B. Zhu, S. Setia, 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.