An Efficient Clone Detection based on Witness Selection and Intrusion Detection System in Wireless Sensor Networks

Savan Kumar
M.Tech (IT), Dept. of ISE,
SDM College of Engineering & Technology,
(Affiliated to VTU, Belgavi), Dharwad-580002,
Karnataka, India

Dr. Rajashekarappa
Dept. of ISE,
SDM College of Engineering & Technology,
(Affiliated to VTU, Belgavi), Dharwad-580002,
Karnataka, India

***Abstract*:- As sensor nodes deployed for a variety of applications, cost effective and malicious user may compromise some sensors and acquire their private information. As the duplicated sensors have the same information they can easily participate in network operations and compromise of attacks. So we have proposed distributed energy-efficient clone detection protocol with random witness selection. ERCD protocol, which includes the witness selection and legitimacy verification stages. 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 randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection.**

Keywords:- Keywords are 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, sensors are usually not tamper-proof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks. Efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify. The private information of the source node, 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 full fill 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.

In this work, 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% clone detection probability with trustful witnesses.

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. 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. We further extend the clone detection performance with untruthful witnesses and show that the clone detection probability still approaches 98 percent when 10 percent of witnesses are compromised.

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) random selection, and iii) semi-random selection. The deterministic witness selection based clone detection protocols like RED 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.

3. METHODOLOGY

We have 2 main modules

Legitimacy verification Module
Clone Detection Module

Module Description:

3.1 Legitimacy verification:

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.

Clone Detection:

In distributed clone detection protocol with random witness selection, the clone detection probability generally refers to whether witnesses can successfully receive the verification message from the source node or not. Thus, the clone detection probability of ERCD protocol is the probability that the verification message can be successfully transmitted from the source node to its witnesses.

4. ERCD PROTOCOL

We proposed an energy-efficient ring based clone detection (ERCD) protocol to achieve high clone detection probability with random witness selection, while ensuring normal network operations with satisfactory network lifetime of WSNs. The ERCD protocol can be divided into two stages: witness selection and legitimacy verification. In witness selection, the source node sends its private information to a set of witnesses, which are randomly selected by the mapping function. In the legitimacy verification, verification message along the private information of the source node is transmitted to its witnesses. If any of witnesses successfully receives the message, it will forward the message to its witness header for verification. Upon receive the messages; the witness header compares the aggregated verification messages with stored records. If multiple copies of verification messages are received, the clone attack is detected and a revocation procedure will be triggered.
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.

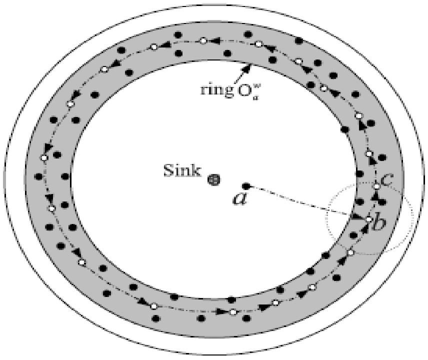
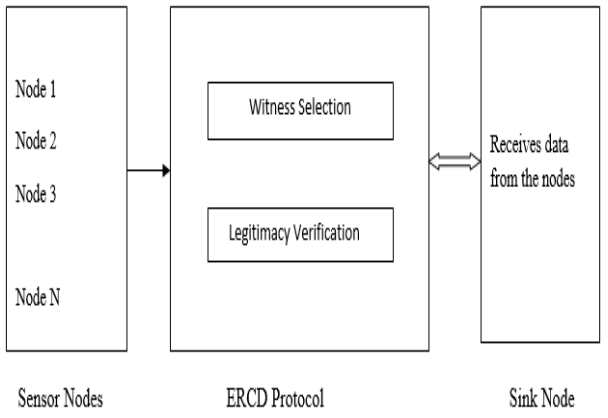


Fig.1 Ring structure of witnesses.

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 verification, 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 verification 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 Owa> 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 bstores the private information of node a and forwards the message to any node located in ring Owa 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 as shown in Fig. 1.

5. METHODOLOGY



6. CONCLUSION

We have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. 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 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 our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer clone detection probability, power consumption, network lifetime, and data buffer capacity is improved.

REFERENCES

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

[2] R. Lu, X. Lin, X. Liang, and X. Shen, “A dynamic privacy-preserving key management scheme for location based services in VANETs,” IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127–139, Jan. 2012.

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

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

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

[6] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, “Localized multicast: Efficient and distributed replica detection in large-scale sensor networks,” IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 913–926, Jul. 2010.

[7] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, “A trigger identification service for defending reactive jammers in WSN,” IEEE Transactions on Mobile Computing, vol. 11, no. 5, pp. 793–806, May. 2012.

[8] 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 Transactions on Parallel and Distributed Systems, vol. 23, no. 1, pp. 32–43, Jan. 2012.

[9] 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.

[10] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, “On the detection of clones in sensor networks using random key predistribution,” IEEE Transactions on Systems, Man, and Cybernetics, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[11] 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.