Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 06, June -2018

MEMORY AND ENERGY EFFICIENT CLONE DETECTION IN WIRELESS NETWORK

[1]Snehalkumar Wakale, [2]Ajinkya Kotambe, [3]Savita Nilakh, [4]Sumit Rathod
[5]B.L.Dhotes

[#]*Computer Department, Sinhgad Institute of Technology*

Abstract - *Wireless ad-hoc Systems are vulnerable to replica occurrences or node replication doses as they are deployed in hostile and unattended situations where they are rundown of physical protection, needed physical tamper-resistance of device nodes. As a result, an attacker can easily capture and compromise sensor nodes and after replicating them, he inserts arbitrary number of clones/replicas into the network. If these clones are not simply detected, an attacker can be further capable to mount a wide variety of internal attacks which can emasculate the various protocols and device applications. Certain solutions have been proposed in the literature to address the crucial problem of clone detection, which are not satisfactory as they suffer from some serious drawbacks. In this paper we propose an Energy-Efficient Distributed Star Based Clone Detection (ESCD) protocol which includes observer selection for verification stage. Our protocol can also achieve better efficiency as well as it becomes trustful system.*

Keywords- *Additional Key Words and Phrases: Clone Detection Protocol, Energy Efficiency*

I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of sensor nodes with powerful sensing capabilities but limited resources. They consist of advanced network architectures and thus are used in a wide variety of applications. These sensors lack tamper resistance hardware because of cost considerations and are often deployed in tough and rough settings and vicinities, hostile scenarios and unattended environments. Thus, they antagonize the extortions from the invaders and muggers which can launch many attacks including the intention to acquire critical information from the WSN or to debilitate and enervate the tasks of the WSNs. Here, we particularly focus on more harmful attack which is known as *node replication attack* or *clone attack*. In this attack an adversary physically captures one or more sensor nodes and compromise all its secret credentials. The node cooperation so allows an opponent to be capable of making clones or replicas of the compromised nodes and then secretly deploying them at strategic positions of the network.

II. LITERATURE SURVEY

Sr. No.	Paper Name	Authors	Published Year	Advantages	Disadvantages
1	ERCD: An Energy-efficient Clone Detection Protocol in WSNs	: ZhongmingZheng , Anfeng Liu , Lin X. Cai , Zhigang Chen , and Xuemin (Sherman) Shen	2013	Location-aware clone detection protocol for clone attack detection	Attacker uses the replica node to insert fake data and disturb the whole operations in the network.
2	Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive	Routes Tao Shu, Sisi Liu, and Marwan Krunz	2010	Generate randomized multipath routes	Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs)
3	Distributed Detection of Clone Attacks in Wireless Sensor Networks	Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei	2011	Replicate them in a large number of clones.	Not secured

4	Distributed Detection of Node Replication Attacks in Sensor Networks	Bryan Parno, Adrian Perrig, Virgil Gligor	2011	Used to detect replicated nodes	Node replication detection schemes depend primarily on centralized mechanisms with single points of failure
5	Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks	YingpeiZeng, Jiannong Cao, Shigeng Zhang, ShanqingGuo and Li Xie	2014	Randomized Multicast, is NDFD and fulfills the requirements of clone detection	It has very high communication overhead

III. EXISTING SYSTEM

To allow well-organized clone recognition, usually, a set of nodes are selected, which are called observe, to help confirm the validity of the nodes in the system. The private information of the source node, i.e., identity and the position information are 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 complete successful clone detection, witness collection and legitimacy verification should fulfil two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully take delivery of all the confirmation communication(s) for clone detection.

Disadvantages of Existing System

- Is to make it difficult for malicious users listen in the communication between current source node and its witness, so that malicious users cannot generate duplicate verification messages.
- The existing system does not make sure that at least one of the witness can check the individuality of the sensor nodes to determine whether there is a clone attack or not.

IV. PROPOSED SYSTEM

Our procedure is appropriate to general densely deployed multi-hop WSNs, where opponents may compromise and replica sensor nodes to launch attacks. We spread the analytical model by assessing the required data barrier of ESCD protocol and by including experimental consequences to provision our theoretical analysis. Energy-Efficient Distributed Star Based Clone Detection (ESCD) protocol.

Advantages of Proposed System

- Extensive simulation results demonstrate that our proposed ESCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.
- The experiment results demonstrate that the clone detection probability can closely approach 100 percent with untruthful witnesses.
- By using ESCD protocol, energy consumption of sensors close to the sink has lower traffic of witness selection and legitimacy verification, which helps to balance the uneven energy consumption of data collection.
-

V. MATHEMATICAL MODEL

Let S be the whole System:

S= {N, CH, W, C}

Where,

1. N is the number of nodes
   N= {n1, n2, n3….n}

2. CH be the Cluster head
   CH= {ch1}

3. W be the Witness messages
   W= {w1, w2….wn}

4. C be the Clone nodes
   C= {c1, c2, c3….cn}

Step 1: Node N will login into the system through ID and Password.

Step 2: After Login system S will authenticate the node.

Step 3: The Node will send the file to the database. When Node is sending file to database then at that time another node i.e. Clone node will also send the file.

Step 4: After receiving the files from Node and Clone node the system is requesting for Witness message.

Step 5: If the node will able to send the witness message then it is a valid node otherwise the clone is detected.

Output: Finally detected clone and saves energy into node.

VI. CONCLUSION

We have deliberate circulated vitality well-organized replica discovery protocol with random witness selection. Specifically, we have proposed the ESCD protocol, which includes the witness selection and legality corroboration stages. In addition, our protocol can achieve better network lifetime and total energy ingesting with sensible storage capacity of data buffer. The energy feeding and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.

REFFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, “ERCD: Anenergy-efficient clone detection protocol in wsns,” in Proc. IEEE INFOCOM, Turin, IT, 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 Communications Magazine, 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,” Computer Networks, 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,” Computer Networks, 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 Transactions on Mobile Computing, vol. 9, no. 7, pp. 941–954, Jul. 2010.