EFFECTIVE IDENTIFICATION & REMOVAL OF CLONE NODES IN WSN USING CHORD ALGORITHM

S. Nida Fathima[1], S.N. NiyazFathima[2], E. Mahalakshmi[3], C. Jackulin

[1] *Student, Department of Computer Science, Panimalar Engineering College, Tamil Nadu, India*
[2] *Student, Department of Computer Science, Panimalar Engineering College, Tamil Nadu, India*
[3] *Student, Department of Computer Science, Panimalar Engineering College, Tamil Nadu, India*
[4] *Assistant Professor, Department of Computer Science, Panimalar Engineering College, Tamil Nadu, India*

ABSTRACT

Wireless sensor networks are vulnerable to the node clone attack, and several distributed protocols have been proposed to detect it. So too strong assumptions are required to be practical for large-scale, randomly deployed sensor networks. The main aim of the project is to identify the clone nodes and remove them. Thereby a distributed clone detection protocol namely ERCD (Energy-Efficient Ring Based Clone Detection) protocol having two stages: witness selection and legitimacy verification can be used for clone detection. The probability of clone detection can be increased by using the Chord algorithm which is based on the concept of Distributed Hash Table(DHT) where every node is assigned with a random key, before transmitting the data it has to give its key which would be verified by the witness node. The witness node identifies the cloned node if the same key is given by another node. Here every node only needs to know the neighbor-list containing all neighbor IDs and its locations. We are implementing Chord Algorithm, by location based nodes identification, where every region/location will have a group leader. The Group leader generates a random number with time stamp to the available nodes in that location. Witness node verifies the random number and time stamp to detect the cloned node. Those messages are encrypted for security purpose

Keyword *Wireless sensors network, energy-efficient ring based clone detection, chord algorithm, distributed hash table*

1. INTRODUCTION

Wireless sensors have been deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, etc. Sensors are usually not tamper-proof devices and are deployed in places without monitoring and protection, for cost-effective sensor placement which makes them prone to different attacks. For example, a malicious user can duplicate some sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks, which is referred to as the clone attack and acquire their private information. They can easily participate in network operations and launch attacks as the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors. Clone attacks have become one of the most critical security issues in WSNs due to the low cost for sensor duplication and deployment. Thus, it is essential to effectively detect clone attacks in order to ensure healthy operation of WSNs. In order to certify the legitimacy of the nodes in the network, a set of nodes are selected which are called witnesses nodes to perform efficient clone detection. The private information of the source node is shared with witnesses at the stage of witness selection i.e.,

identity and the location information. If any of the nodes in the network wants to transmit data, it first sends the request to the witness node for legitimacy verification, and witnesses node will report a detected attack if it fails the certification. Therefore to achieve successful clone detection, witness selection and legitimacy verification should fulfil two requirements: 1) witness nodes should be selected randomly; and 2) verification message(s) for clone detection should successfully receive by at least one of the witnesses. The first requirement is to make it difficult for malicious users to eavesdrop the communication between the 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 witness node 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 that the clone attacks can be successfully detected, is critical and challenging to fulfill these requirements in clone detection protocol design. Different from wireless devices, wireless sensors are usually of smaller size, lower price, limited battery consumption and memory capacity. Therefore, the design criteria of clone detection protocols should not only guarantee the high performance of clone detection but consider the memory efficiency and energy of sensors. Previous approaches mainly focus on improving clone detection probability without considering efficiency and balanced usage of energy consumption in WSNs where sensors may use up their batteries due to the unbalanced energy consumption. Network partition may occur in dead sensors which may further affect the normal operation of WSNs. To prolong network lifetime, i.e., duration from the starting time of network until the first occurrence of a sensor that runs out of energy, it is critical to minimize the energy consumption of each node and also to balance the energy consumption among sensors which is distributed and located in different areas of WSNs. The data buffer being another feature of sensors which has an impact on the clone detection protocols design .In General, to guarantee successful clone detection, witnesses have to record private information of source node and certify the sensors legitimacy based on the stored private information., The required buffer storage size in most existing clone detection protocols 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 such requirement makes the existing protocols not so suitable for densely-deployed WSNs, thus the required buffer size scales with the network node density. From the unlimited usage of energy consumption and memory storage, most existing approaches can improve the successful clone detection

2. RELATED WORK

Rongxing Lu et al [3] proposed a machine-to-machine communication in the year 2011 which faced challenges in energy efficiency, reliability and security(GRS). Without GRS, machine-to-machine communication cannot be accepted as communication paradigm. Although the requirements of GRS are fulfilled individually, they are considered to be complicated as a whole. Nodes interconnected in a wireless sensor network, communicate with each other and there is also a possibility of attacks to sensor nodes. Ramya Shivanagu and Deepti C [5] proposed a reactive jammer attack which acts as a major threat to WSN in terms of energy and range. Usually WSN consists of n sensor nodes and one base station where the base station calculates the estimated jammed area and range based on boundary node. Using trigger identification algorithm, trigger nodes are identified and eliminated where it(trigger nodes) acts only as receivers with the group testing technique. Panagiotis Papadimitratos et al [2] proposed a randomized key refreshing countermeasure to identify a typical attacker called parasitic adversary who seeks to exploit sensor networks in an unauthorized way, where RKR-GossiCrypt used for encryption and re encryption with random nodes and en routes to the sink. Therefore the amalgamation of randomized key refreshing and GossiCrypt protects data confidentiality with the probability 1 along with low cost mechanisms. Disadvantage of this paper ensures that it aims at confining the effects of adversary but not eliminating fully. Zubair Md. Fadlullah [4] proposed a scheme for forecasting those adversaries or malicious attacks with the help of smart power grids based on the probabilistic distribution which predicts the abnormal operations in the node. It results in warning about malicious Dos attacks, other malicious threats and anomalies. However small grids with background traffic have a need to establish a baseline for estimating error in order to avoid traffic among nodes Quanjun Chen et al [8] proposed an accurate model which confirms that the traffic load of a node increases with the proximity to the sink. Further the per-node energy consumption can be useful in identifying hotspots in the network. Additional sensors nodes can be deployed at those hotspots to extend the operational lifetime of the network. Yingpei Zeng et al [6] proposed that all replica- detection protocols must be a Non-Deterministic and Fully Distributed(NDFD) in order to identify replicated nodes and fulfills the witness selection than compromising the adversary nodes. Randomized multicast satisfies NDFD but has a drawback of very high communication overhead. So based on random walk two protocols named Random Walk(RAWL) and Table Assisted Random Walk which fulfills security requirements.

Ion Stoica et al [10] main contribution is an algorithm called chord algorithm which is a distributed peer-to-peer lookup protocol, helps in finding the nodes location which holds the data. It maps the key on to a node so that the data locations are implemented with a key and storing the node where the key maps. As every node in the network is mapped by a key, Haowen Chan et al [9] proposed a key establishment scheme where it represents the framework of pre-distributing a random set of keys to each node. Randomly selected pairwise keys serves the secrecy of the rest of the network when any node is captured and enables node-to-node authentication and revocations. Ming Zhang et al [7] proposed four replication detection protocols that have high detection probability, low memory requirement and balanced energy consumption which uses bloom filters to compress the information stored at the sensors with two new techniques called cell forwarding and cross forwarding with an average memory reduction up to 91%. These replication protocols are have efficient memory usage. E. Sujatha et al [1] proposed an ERCD (Energy-Efficient Ring Based Clone Detection) protocol maintains trustful witnesses in a ring structure, so that clone attack detection becomes easy with a probability 1. Extended network lifetime achieved by effectively distributing the traffic load across all the nodes in the network.

3. EXISTING SYSTEM

In the existing system, the main concentration is on the Energy-Efficient Ring Based Clone Detection(ERCD) protocol. Previous approaches/protocols only tried improving clone detection rate without considering the amount of energy consumption and memory usage, where Energy -Efficient Ring Based Clone Detection (ERCD) protocol limits energy consumption and memory usage as it has a ring structure and achieves high clone detection probability. Its divided into two stages 1. witness selection 2.legitimacy verification. In witness selection stage, source node sends its private information to a set of random witnesses which was selected by the mapping function. Verification message along with the private information of source node is transmitted to its witness node where witness header compares the verification message and records them. Clone attack was detected if multiple verification messages are received in the verification stage**.**

4. LIMITATIONS IN EXISTING SYSTEM

In the existing techniques, random witness nodes which are selected in witness selection stage can be compromised by the adversaries since the detection of clone probability is 1. Adversaries are detected only in the verification stage when multiple verification messages from the same source node arrive. Random selection of witness nodes makes time complexity with the existing system in order to detect the clone nodes or attacks. There is no random number distribution and no timestamp.

5. PROPOSED SYSTEM

In the proposed system, we have six modules namely network construction, chord algorithm, witness node distribution, verification of random number, verification of user id, cloning detection and data transfer

In fig1. Network construction module is developed in order to create a dynamic network. In a network, nodes are interconnected with the admin, which is monitoring all the other nodes. All nodes share their information with each other.

Chord algorithm is used to verify the neighbor nodes information of the Requested Node, so that by verifying the Ids and location we can detect the clone node. For this purpose, we have to create the list of the neighbor nodes information for each node so that the Server/ Witness Node can verify the node's request.

Witness node distribution has a major issue in designing a protocol to detect clone attacks is the selection of the witnesses. We will call 'Witness' as a node that detects the existence of a node in two different locations within the same protocol run. If the adversary knows the future witnesses before the detection protocol executes, the adversary could subvert these nodes so that the attack goes undetected. Here, we have identified two kinds of predictions:

1. ID-based prediction
2. Location-based prediction.

We say that a protocol for replica detection is ID-oblivious if the protocol does not provide any information on the ID of the sensors that will be the witnesses of the clone attack during the next protocol run. Similarly, a protocol is area-oblivious if probability does not depend on the geographical position of a node in the network. Clearly, when a protocol is neither ID-oblivious nor area-oblivious, then a smart adversary can have good chances of succeeding, since it is able to use this information to subvert the nodes that, most probably, will be the witnesses.

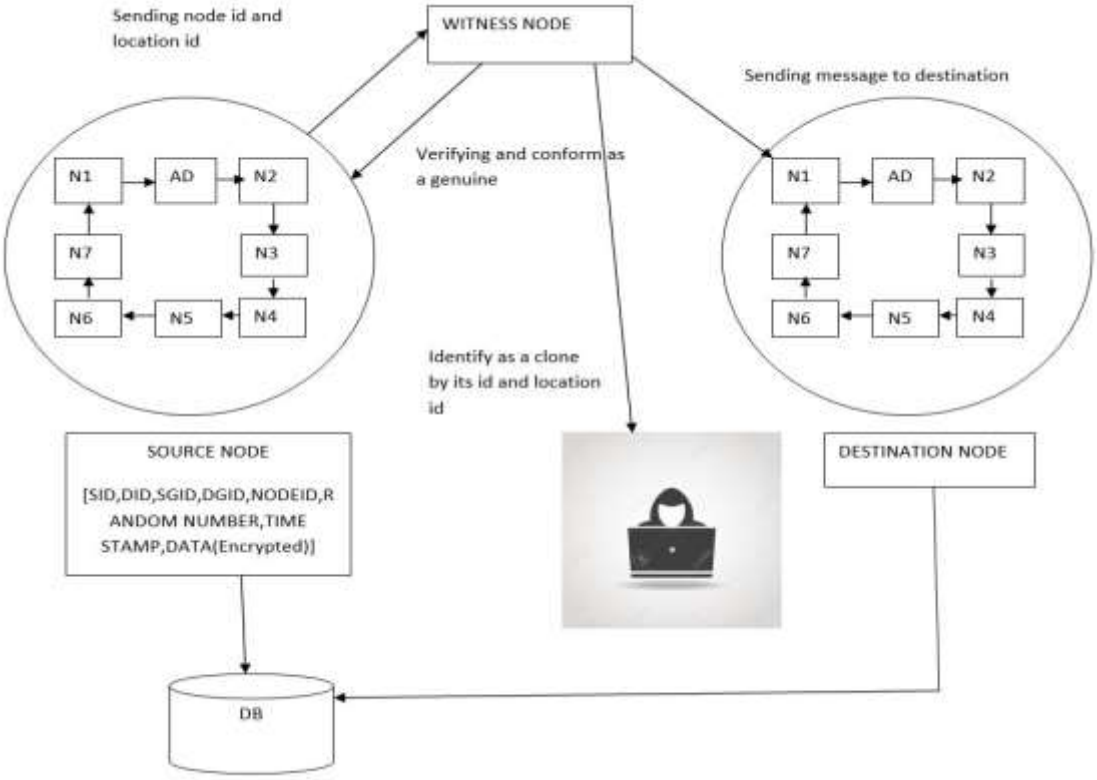

Fig -1: Architecture diagram

In the verification of random number, Random Key pre-distribution security scheme is implemented in the sensor network , that is each node is assigned a number randomly with Time Stamp from Group Leader. Then the Group Leader will transmit Random Number (Encrypted with RSA algorithm) which was generated with respect to that Time Stamp to the Witness node. Witness node will now check the Random number which is generated with the User information. If both the data are matched then the Witness node will confirm that this node is Genuine. User Id for verification of each node is assigned an ID as the individual once it is registered into the network and also an ID for the whole group (i.e) Location ID is generated for each and every Location.

That Node ID and Location ID are also appended with 1(Encrypted with RSA algorithm). Then the Witness node will now check the node ID + Location ID which is generated with the User Information. If both the data are matched then the Witness node will confirm that this node with that Location is Genuine.

Finally, in the clone detection module, Only the Witness node confirms the Sender node, the data is sent to the Destination, which is Genuine. If user specified information and the internal information are varied, then the Witness node will identify that Cloning or some Malpractice has occurred and the Packets are discarded by the witness node.

6. CONCLUSIONS

Security is an important requirement for WSN's. Thereby it is essential to identify and remove clone nodes to prevent data from being copied. Chord Algorithm's contribution of assigning a random key to every node helps in effectively finding which data item every node holds and in which location and every node is given a timestamp too. It helps in identifying the successor and predecessor of each node, which aids in better clone detection. ERCD protocol attains great network lifetime as well as consumption of total energy with satisfactory storage capacity of the buffered data.

7. 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] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE Journal on Selected Areas in Communications. vol. 28, no. 7, pp. 1036–1045, Sep. 2010.

[3] 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.

[4] 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

[5] 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

[6] 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

[7] 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 International Conference on Network Protocols, Princeton, NJ, USA, Oct. 13-16, 2009, pp. 284–293.

[8] Q. Chen, S. S. Kanhere, and M. Hassan, "Analysis of per-node traffic load in multi-hop wireless sensor networks," IEEE Transactions on Wireless Communications., vol. 8, no. 2, pp. 958–967, Feb. 2009.

[9] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symposium on Security and Privacy, Berkeley, CA, USA, May 11-14, 2003, pp. 197–213.

[10] Ion Stoica, Robert Morris, David Liben-Nowell, David R. Karger, M. Frans Kaashoek, Frank Dabek, and Hari Balakrishnan" Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications", IEEE/ACM Transactions on Networking, vol. 11, no 1, February 2003