ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DETECTION OF CLONE NODE USING CHORD ALGORITHM FOR SECURE DATA TRANSMISSION AND PREVENTION OF COLLUSION ATTACKS IN WSN

S. Divya*, Mr. D. Duraikumar, Prof VP. Manikandan
* Mtech It Ganadipathy Tulsi's Jain Engineering College Vellore
HOD Ganadipathy Tulsi's Jain Engineering College Vellore
Guided Ganadipathy Tulsi's Jain Engineering College Vellore

DOI: 10.5281/zenodo.54786

ABSTRACT

At present due to limitation and computing power and energy resources of sensor node the data is aggregated by extremely simple algorithm such as averaging data from multiple sensors is aggregated at aggregation node which is done at base station only the aggregate values. Such algorithm is very vulnerable to false and more important malicious attack since WSNR usually un attend without tamper resistance network they are highly susceptible to such attacks. This cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus better and more sophisticated algorithm are needed for data aggregation in further WSNR Iterative filtering algorithm are attractive option for WSN because they solve both problem data aggregates data trustworthiness assessment using a single iterative procedure such algorithm simultaneously aggregated data from multiple sources.

KEYWORDS: Wireless sensor network, robust data aggregation, collusion attacks.

INTRODUCTION

Is to detect and prevent the clone node while transferring the data from source to destination and transfer the data in secure manner. There are immediate needs for clone node detection systems in commercial, law enforcement and military applications and any government and private organization sector for providing security. A trustworthiness assessment at any given moment represents an aggregate of the behavior of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behavior. The main target of malicious attackers are aggregation of trust, defect and reputation system.

In addition to the obvious security applications A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. A WSN can be deployed in harsh environments to fulfill both military and civil applications. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. For instance, an adversary could eavesdrop on all network communications and could capture nodes there by acquiring all the information stored within (sensors are commonly assumed not to be tamper proof). Note that once a sensor is compromised, the information inside is easily accessible.

An adversary may replicate captured sensors and deploy them in the network to launch a variety of insider attacks. This attack process is referred to as clone attack. A few Attacks that may be launched by cloned nodes. Since a cloned node has legitimate information (codes and key materials), it may participate in network operations in the same way as a non-compromised node; hence cloned nodes can launch a variety of attacks. For instance, a cloned node may create an aggregate data in such a way to bias the result. Further, if data confidentiality is an issue, cloned nodes can violate this requirement leaking data.

To the best of our knowledge, with the exception of the proposal in discussed in the following, only centralized or local protocols have been proposed so far to tackle with clone detection attack. While centralized protocols have a single point of failure, local protocols do not detect replicated nodes that are distributed in different area of the network.

The properties of distributed mechanisms for detection of node replication attack. And also analyze the first protocol for distributed detection, which was recently proposed and show that this protocol is not completely satisfactory. Finally, to propose a new algorithm called chord algorithms for the detection of node replication attacks and prove that our algorithm actually does meet all the requirements. It is highly efficient with regards to required communications, more energy, memory, and computationally efficient, and that it detects node replication attacks with higher probability.

In this solution, each node sends a list of its neighbors and their claimed locations (i.e., the geographic coordinates of each node) to a Base Station (BS). The same entry in two lists sent by nodes that are not "close" to each other will result in clone detection. Then, the BS revokes the clones. This solution has several drawbacks, such as the presence of a single point of failure (the BS), and high communication costs due to the large number of messages. Further, nodes close to the BS will be required to route far more messages than other nodes, hence shortening their operational life.

Other solutions rely on local detection. For example, in [7, 18, 2 and 29] a voting mechanism is used within a neighborhood to agree on the legitimacy of a given node. However, applying this kind of method to the problem of replica detection. Fails to detect clones that are not within the same neighborhood. With this solution each node floods the network with a message containing its location information and compares the received location information with that of its neighbors. If a neighbors of nodes receives a location claim that the same nodes is in a position not coherent with the position of detected by, this will result in the detection of a clone. However, this method is very energy consuming since it requires n flooding's per iteration, where n is the number of nodes in the WSN. Note that clone attacks are based on identity theft however the attacks are orthogonal. Further, while the former can be efficiently addressed with mechanism with authentication based on the knowledge of a fixed key set efficient detection of clone attacks is actually an open issue.

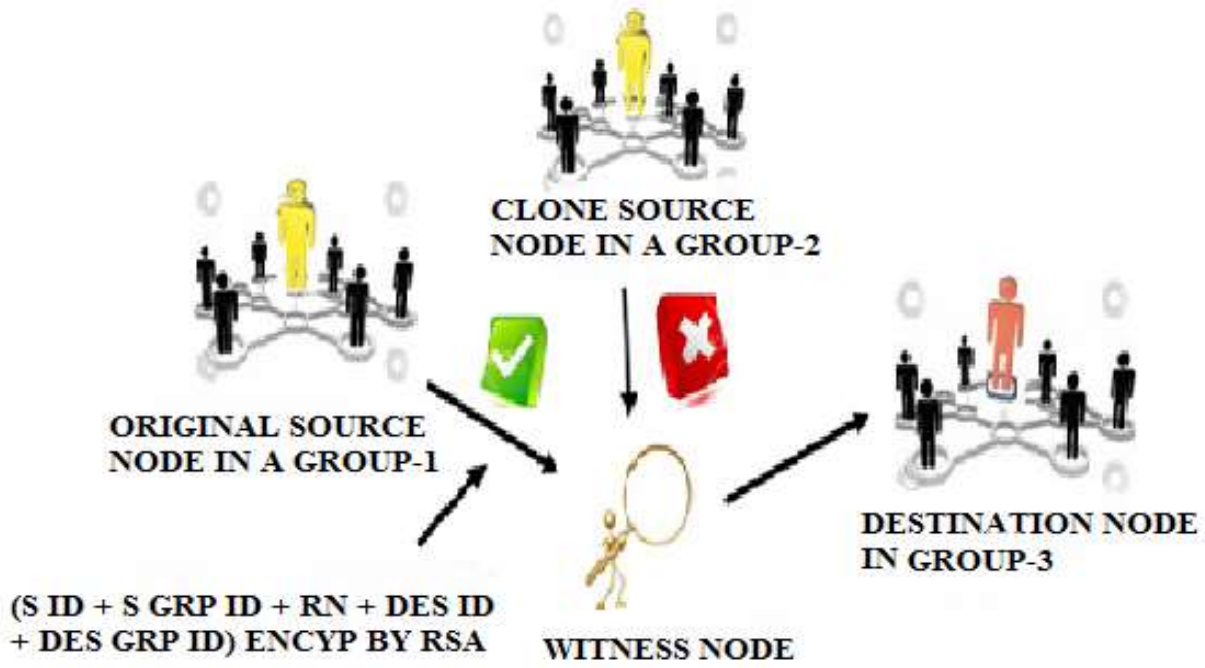
The node that detects the existence of another node in two different locations within the same time-frame will be called *witness*. When a node announces its location, every neighbor locally checks the signature of the claim and then it forwards this location claim with probability p. If the neighbor forwards the claim, it randomly selects a fixed number $g \geq 1$ of destination nodes and sends the signed claim to all the destination nodes.

In order for a location claim to travel from source to destination node, it must pass through several intermediate nodes: thus defining a claim message path. Moreover, every node that routes this claim message will check the signature, store the message, and check for coherence with the other location claims received within the same iteration of the detection protocol. Node replication is eventually detected by the node (called witness) on the intersection of two paths that originate from different network positions by the same node ID. In fact, if during a check the same node *sa* is present with two non-coherent locations, the witness will trigger a revocation protocol for node *sa*. In what follows, the generic term "witness" will be used to refer to an actual witness.

SYSTEM ARCHITECTURE

The group leader sends a unique id and time stamp to all the nodes in the network. A source node sends a message to destination node, which will cache ID, location and check for replica node detection. Then, some intermediate nodes behave as an inspector to improve toughness against the adversary in an efficient way. An inspector or witness node is used to verify the message.

ISSN: 2277-9655
Impact Factor: 4.116



- Network construction
- Witness node
- Verification and Clone node detection

Network construction
This 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 are sharing their information with each other's.

Witness node
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.

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 node in the network.

Verification and clone node detection
Here, we have identified two kinds of predictions:

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

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.

Each node is assigned an ID as 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.

The witness node extracts the information (ID and location) and it checks: Whether this is the first received claim carrying ID, then it simply stores the message. If other claims from ID have been received, the witness checks whether the claimed location is the same of the stored claim for this ID). If it is not, the witness node triggers a revocation procedure for the given ID Only the Witness node confirms the Sender node, the data is send 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 Mal practice has occurred and the Packets are discarded by the witness node.of location-based keys (LBKs) by binding private keys of individual nodes to both their IDs and geographic locations.

CONCLUSION

The paper present and justified a few of the basic requirements that an ideal protocol for distributed detection of node replicas should have. In present work introduce the preliminary notion of ID-obliviousness and area-obliviousness that conveys a measure of the quality of the node identity replica detection protocol, i.e., its resilience to an active attacker. Moreover, That the overhead of such a protocol should not only be small, but also evenly distribute among the nodes, both in computation and memory. Furthermore, an introducing new model for the adversary. However, the main contribution of this project is the proposal of a Chord algorithm that is able for detecting node replication attacks. This is prove that the overhead introduce by Chord is low and almost evenly balanced among the nodes, while these properties are not provided by IF (Iterative filtering) LSM and RED. Finally, both ID-oblivious and area-oblivious and also shows a dramatic improvement in detection capability.

REFERENCES

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.
[2] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference. New York, NY, USA: Springer,.
[3] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in Proc. 5th Int. Workshop Security Trust Manage., Saint Malo, France, 2009, pp. 253–262.
[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.
[5] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, "Trust and reputation systems for wireless sensor networks," in Security and Privacy in Mobile and Wireless Networking, S. Gritzalis, T. Karygiannis, and C. Skianis, eds.,Leicester, U.K.: Troubador Publishing Ltd, 2009 pp. 105–128,.
[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.