ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 10, March 2017

STORAGE EFFICIENT DUPLICATE NODE DETECTION PROTOCOL FOR WSN

R.Shijimol[1],C.Naveen Raj[2],K.Rakesh[3],M.Manoj Prabhakaran[4]

Department of ECE, PSN College of Engineering and Technology, Tirunelveli.
Email:frshijimolme@gmail.com

Abstract:-Wireless Sensor Networks consists of sensors which are distributed in an ad hoc manner. Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. The existing system uses distributed Low-Storage Clone Detection protocol (LSCD) for WSNs. This protocol designs a detection route along the perpendicular direction of a witness path with witness nodes deployed in a ring path. However, in this a powerful adversary can also replicate node IDs, which leads to the need for improved clone detection. In order to overcome this, distributed hash table (DHT) based clone detection protocol is proposed that provides a checking system is constructed to catch cloned nodes. The protocol's performance on memory consumption and a critical security metric are theoretically deducted through a probability model. The DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.

Keywords:-wireless sensor network security,clone detection, network model, distributed route, DHT(Distributed Hash Table),withness path.

I. INTRODUCTION

To designs a Distributed Hash Table based protocol that can detect node clone with high security

level and holds strong resistance against adversary's attacks.To improve detection rate of the clone detectionWireless Sensor Networks (WSNs) are one of the most important compositions of Cyber-Physical Systems (CPSs) which monitor physical phenomena from surrounding environments to dynamically interact with human activities and/or machine systems such as surveillance systems, body health monitoring systems, and intelligent transportationsystems. Secure communication in WSNs is vital because information transferred through such networks can be easily stolen or replaced.For instance, an adversary could capture sensor nodes and acquire all the information stored therein—the nodes are commonly assumed to not be tamper proof. Therefore, an adversary may replicate captured nodes and deploy them in the network to perform a variety of malicious activities..This type of attack is referred to as a clone attack.A cloned node, because it has legitimate information, may participate in network operations in the same manner as a non-compromised node, and thus, the cloned node can launch a variety of attacks. It is not difficult to imagine that this may present a huge risk to users in many types of WSN applications (e.g., flood monitoring). Therefore, early detection and recognition of cloned nodes has important significance to network security.

II. DHT(Distributed Hash Table)

Distributed hash table (DHT), by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. The protocol's performance on memory consumption and a critical security metric are theoretically deducted through a probability model, and the resulting equations, with necessary adjustment for real application, are supported by the simulations. In accordance with our analysis, the comprehensive simulation results show that the DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 10, March 2017

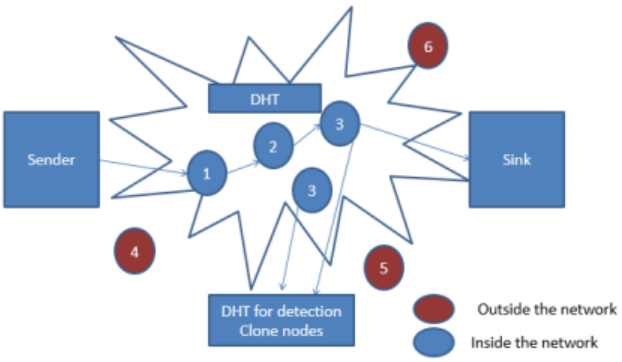
III. EXISTING SYSTEM

The existing system uses distributed Low-Storage Clone Detection protocol (LSCD) for WSNs. This protocol designs a detection route along the perpendicular direction of a witness path with witness nodes deployed in a ring path

Disadvantage of existing system

- As the compromising time decreases the number of clone nodes increases thus badly affects the security of the network.
- The powerful adversary can also replicate node IDs

Architecture



IV.PROPOSED SYSTEM

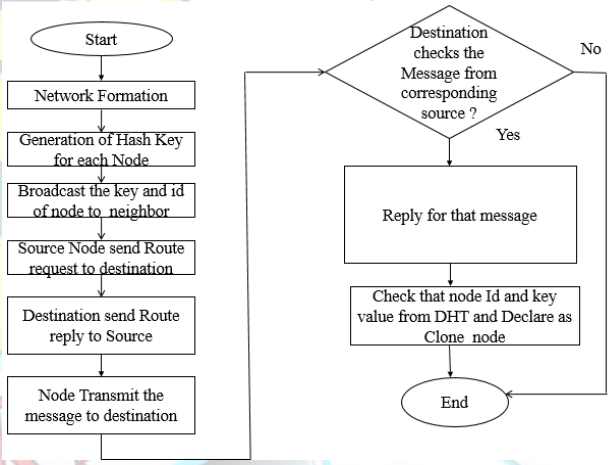
Distributed Hash Table is the node clone detection protocol

Distributed Hash Table is the node clone detection protocol which provides decentralization scheme with the key based caching and checking. Distributed Hash Table is based on a hash table of (key, record) pair which is already distributed.

The distributed hash table enables the sensor nodes to form an overlay network. The key plays vital role in distributed hash table and key determines where to send the message from source node i.e. the destination node is determined by the key and source doesn't know anything about the destination node.

The detection round initiated by initiator by sending an action message (involves nonce, seed, and time).

DFD(Data Flow Diagram)



Advantages of Proposed System

- Less communication overhead
- High detection probability of clone nodes
- Minimizes the delay

V.Modules

- Network model
- Witness path Detection
- Clone detection using DHT based clone detection protocol
- Performance Analysis

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 10, March 2017

VI .NETWORK MODEL

Number of nodes are deployed in network animator with a area 1500 x 1500 with the parameters such as transmission range, frequency, antenna type, routing protocol and security schemes.
The source and destination nodes are declared
The route between source and destination is calculated.

.

VII .WITNESSPATH

In the DHT based clone detection protocol, witness nodes form route paths along circles, with a sink serving as the center, because clone detection is processed along the centrifugal (or centripetal) direction, and the distance between any two detection routes is shorter than the witness path length. Thus, the witness path must encounter the detection route, ensuring high clone detection probability.

VIII. DHT based Clone Detection protocol

Distributed hash table (DHT) based clone detection is a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. The protocol's performance on memory consumption and a critical security metric are theoretically deducted through a probability model, and the resulting equations, with necessary adjustment for real application, are supported by the simulations.
In accordance with our analysis, the comprehensive simulation results show that the
DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.

IX .PERFORMANCE EVALUATION

Throughput:

- It measures the total rate of data sent over the network, including the rate of data sent from CHs to the sink and the rate of data sent from the nodes to their CHs.

Packet Drop Ratio:

- It measures the robustness of protocol and is calculated by dividing the total number of dropped packets by the total number of transmitted packets.

Delay:

- The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds.

Overhead:

- Overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal.

X .Conclusion

In this paper we present clone detection in WSN(wireless sensor networks)and to prevent nodes from adversary's attacks using DHT(Distributed Hash Table)One is based on a distributed hash table, which forms a Chord overlay network and provides the key-based routing, caching, and checking facilities for clone detection, and the other uses probabilistic directed technique to achieve efficient communication overhead for satisfactory detection probability. While the DHT-based protocol provides high security level for all kinds of sensor networks by one Deterministic witness and additional memory-efficient.

XI.References

[1]Y. Liu, A. Liu, and S. He, "A novel joint logging and migrating traceback scheme for achieving low storage requirement and long lifetime in WSNs," AEU Int. J. Electron. Commun., vol. 69, no. 10, pp. 1464–1482, Oct. 2015.
[2]J. Luo, L. Zhou, and H. Wen, "Lightweight and effective detection scheme for node clone attack in wireless sensor networks," IET Wireless Sensor Systems, vol. 1, no. 3, pp. 137-143, Sept. 2011.
[3] 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. Select. Areas Commun., vol. 28, no. 5, pp. 677-691Jun.2010.
[4] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans. Dependable and Secure Comput., vol. 8, no. 5, pp. 685-698,Sep.2011