© 2016 IJSRSET | Volume 2 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

An Efficient Cloning Detection Protocol Using Distributed Hash Table for Cyber-Physical System in WSN

K. Sindhukavi*[1], P. Brundha[2], P. J. Beslin Pajila[3]

*[1]PG Student, CSE, Anna University, Tirunelveli, Tamil Nadu, India
[2,3]CSE, Anna University, Tirunelveli, Tamil Nadu, India

ABSTRACT

Wireless Sensor Networks consists of sensors which are distributed in an ad hoc manner. Various security mechanisms such as cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as 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 known path with known 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 completion on memory consumption and a critical security metric are theoretically deduced through a probability model. The DHT-based protocol can catch node clone with the high-security level and holds strong resistance against adversary's attacks.

Keywords: Wireless Sensor Network Security, Clone Detection Protocol, Distributed Hash Table

I. INTRODUCTION

Wireless sensor network is one of the most important compositions of cyber-physical systems. Secure communication in WSN is vital because information transferred through such networks can be easily replaced. For instance, an adversary could capture sensor nodes and acquire all the information stored. 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 cloned attack. Witness-based clone detection methods that allow resource-constrained sensor nodes to mitigate node capture and clone attacks have been developed. In such methods, each node forwards its identity to a set of coordinates that act as a witness node. Such methods use that fact that clone has the same ID as a captured node but are at different locations. Hence clone is detected when two nodes report same ID but different locations. 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.

In the LSCD 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 that the LSCD theoretically has a 100% clone detection probability. Moreover, witness routes and clone detection routes are randomly generated. Thus, even if the adversary knows the LSCD algorithm, the locations of witness nodes and detection route information cannot be obtained. Therefore, the LSCD protocol has fully distributed characteristics and strong robustness to compromise attacks.

To overcome the problem occurred in the Low Storage Clone Detection Protocol new technique called Distributed hash table (DHT) is introduced DHT is a class of a dissolution distributed system that provides a lookup service similar to a hashtable(key, value) pairs are stored in DHT & any participating node can efficiently retrieve the value associated with given key. Responsibility for controlling the mapping from keys to values is distributed among the nodes, in such a way that change in the set of participant's origin a minimal amount of disruption. This allows a DHT to scale to a huge numbers of nodes and to handle continual node arrivals, failures.

The DHT-based protocol can catch node clone with high- security level and influence strong resistance against adversary's attacks.

II. METHODS AND MATERIAL

A. Related Works

A Logging joint marking (LM) traceback scheme [1] is proposed. The LM scheme requires less storage capacity, and storage among the nodes is equity. It is a fair storage system. This technique is helpful to improve storage utilization. Due to high overhead, this technique fails.

A Lightweight method for clone nodes attack detection [2] in WSNs. This scheme aims at achieving fast detection and decrease the data transmission cost by taking advantage of temporal and spatial uniqueness in physical layer channel responses. This technique is helpful to minimizing the packet transmission overhead. Due to low security, this technique fails. A new self-healing, Randomized, Efficient, and Distributed (RED) protocol [3] is used for the detection of node replication attacks .this technique is used for high efficient in communication. Due to low robustness among compromise attacks, this technique fails.

Localized Multicast [4], the witness nodes for a node identity is randomly selected from the nodes that are located within a geographically limited region. This technique is used for High probability detection of replica attacks. Due to higher communication costs, this technique fails.

Clone detection protocol [11], this protocol designs a detection route along the horizontal direction of a witness path with witness nodes expanded in a ring path. This ensures that the detection route must encounter the witness path because the distance between any two detection paths must be smaller than the witness path length. In the LSCD protocol, clone detection is processed in a non-hotspot region where a large amount of energy remains, which can improve energy efficiency as well as network lifetime. This technique is helpful to improve energy efficiency. Due to lower security, this technique fails.

B. Proposed Detection Scheme

To overcome the problem occurred in the Low Storage Clone Detection Protocol new technique called Distributed Hash Table (DHT) is introduced. DHT is a class of a decentralized distributed system that provides a lookup service similar to a hashtable(key, value) pairs are stored in DHT & any participating node can efficiently retrieve the value associated with given key. Responsibility for maintaining the mapping from keys to values is distributed among the nodes, in such a way that change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely huge numbers of nodes and to handle continual node arrivals, failures. The DHT-based protocol can catch node clone with high-security level and influence strong resistance against adversary's attacks.

C. System Design

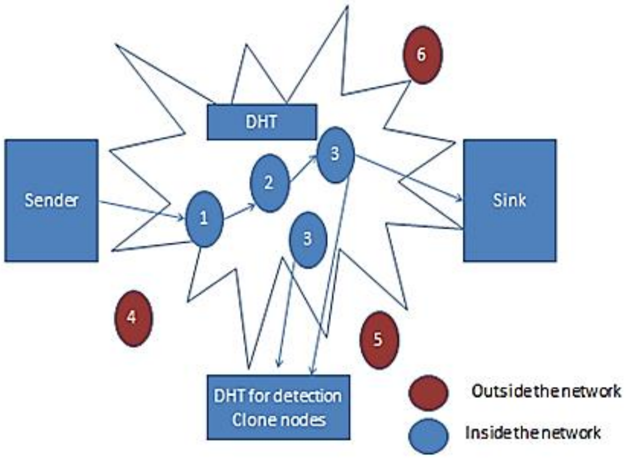

Figure 1.1 System Design

Figure 1 describes the data transformation from sender to sink. There are a number of nodes in an inner network and outer network. The sensor nodes are assumed to know their relative locations, the sink node location and the hops to the sink. assume that each sensor node has knowledge of its adjacent neighboring nodes. The sender sends a data to the first node and the first node sends its data to the nearby node. If two nodes have a same ID then it detects that node using Cloned detection protocol based on Distributed Hash Table (DHT) and finally send data to sink.

D. Algorithm1 Building Witness Path

```
$X$x ← Encrypt ($ID$x , $l$x )
 k = PseudoRand ($ID$x , $l$x , $h$)
Random walk $\varepsilon$1 hops to node $y$, i ← y. hop, y'=y;
while i≠ k do
    if i < k then
        y′ ← NeighborNodeOnMaxHop (y′), i ← i + 1;
    else
        y′ ← NeighborNodeOnMinHop (y′), i ← i − 1;
    end if;
end while;
 node y' Random walk $\varepsilon$2 hops to node y″, where each
node's hop count is the same as the route path;
 i ← 1
while i < ⌈$\Psi/r$⌉ do
    Let y″record $X$x;
    y″ ← NeighborNodeOnSameHop(y″), i ← i + 1;
end while;
```

E. Algorithm2 Clone Detection

```
 Random walk hops to node x′; x′. tag = true 3 □
 node x′ routing reverse sink to x‴ with broadcast $X$x;
while x′. hop ≠ 2 do
    x′ ← NeighborNodeOnMinHop(x′); Broadcast $X$x;
end while;
$\partial$ ←The hops need for routing to build the next clone
route
    x′. tag = false
routing $\partial$ hops to node $z$ with same-hop routing;
z. tag = true, $z$ route reverse to sink;
for each clone detection route reverse to the sink;
z′ ← NeighborNodeOnMaxHop(z′); Broadcast $X$x;
    if z′. tag = true then
        compute $\partial$ using formula 9;
        if $\partial$ ≠ 0 then
            along both left- and right-hand directions,
same-  hop routing hop to nodes z″, z‴; □
            z′. tag = false;
            nodes z″, z‴ route reverse to the sink;
        end if;
    end if;
end for;
for each node $S$ that hears $X$x do
        if ($ID$x, $l$x) of $S$ ≠ ($ID$x , $l$x ) in $X$x then
            trigger the revocation procedure;
        end if
end for
```

III. RESULTS AND DISCUSSION

A. System Modules

1. **Network model**

- The number of nodes are deployed in network animator with an 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.

2. **Witness path**

- In the LSCD 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 that the LSCD theoretically has a 100% clone detection probability.

3. **Cloned detection protocol based on DHT**

- LSCD based Distributed Hash Table (DHT) is a fully decentralized, key-based caching and checking system is constructed to catch replicate nodes.
- The protocol's performance on memory consumption and a critical security metric are theoretically deduced through a probability model**,** and the resulting equations, with necessary adjustment for real application, are supported by the simulations.

In an analysis, the comprehensive simulation results show that the DHT-based protocol can detect node replicate with high-security level and holds strong resistance against adversary's attacks.

B. Performance Analysis and Result

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

Overhead:

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

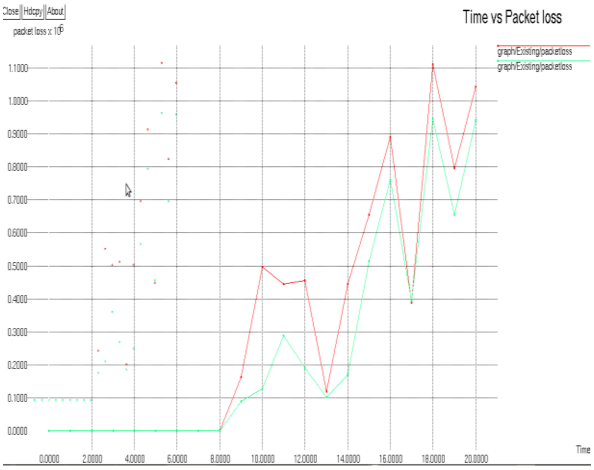

Figure 1. Packet loss

In figure 1 represents the comparison of packet loss with the existing system. Time is plotted along x-axis and packet loss is plotted along the y-axis. The packet loss gets decreased when compared with the existing system.

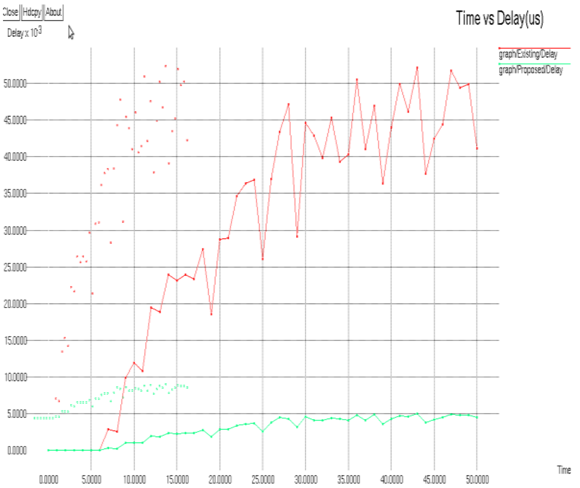

Figure 2. Delay

In figure 2 describes the comparison of delay with the existing system. Time is plotted along x-axis and delay is plotted along the y-axis. The delay gets decreased when compared with the existing system.

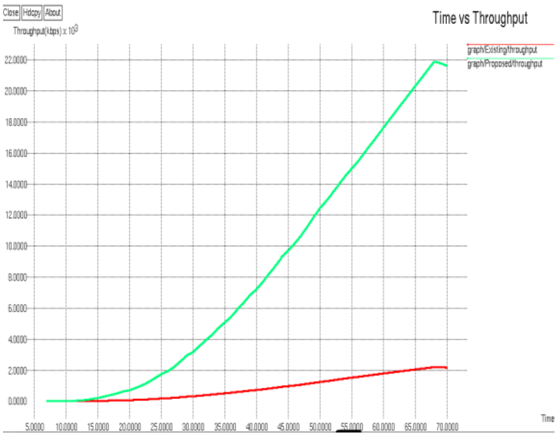

Figure 3. Throughput

In figure 3 represents the comparison of packet loss with the existing system. Time is plotted along x-axis and throughput is plotted along y-axis. The throughput gets decreased when compared with the existing system.

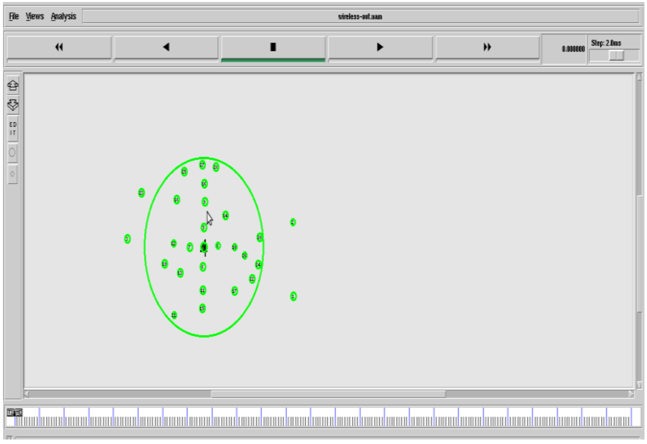

Figure 4. Node formation

In figure 4 designs a detection route along the horizontal direction of a witness path with witness nodes deployed in a ring path. This ensures that the detection path must encounter the witness path because the distance between any two detection routes must be smaller than the witness path length.

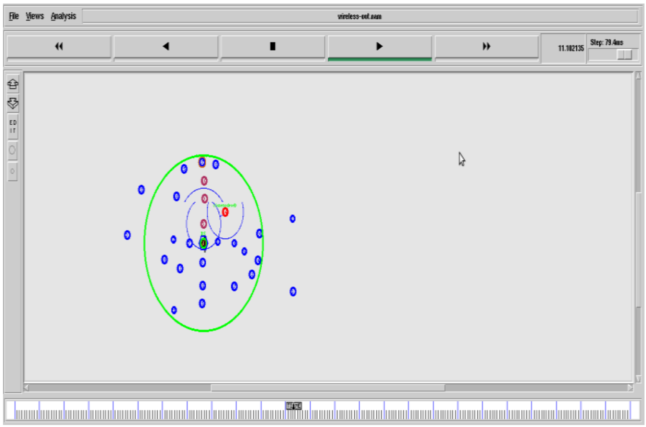

Figure 5. Data transfer with clone node

In figure 5 data can be transfer from one to the nearby node. each node forwards its identity to a set of coordinates that act as a witness node. Such methods use that fact that clone has the same ID as a captured node but are at different locations. Hence clone is detected when two nodes report same ID but different locations.

In figure 6 data can be transfer from one to the nearby node. No two nodes have same ID and location. Therefore there is a no clone node.

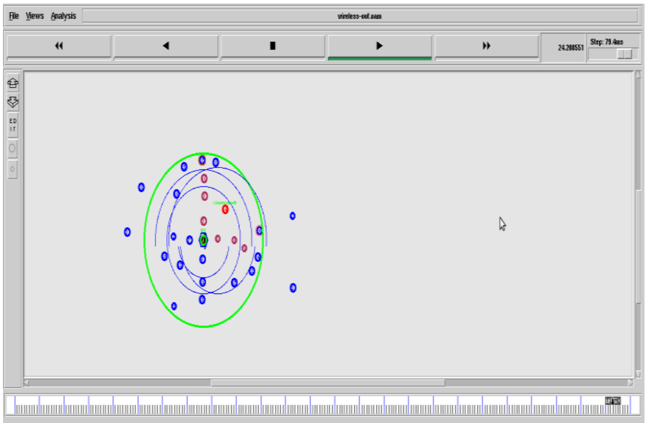

Figure 6. Data transfer without clone node

IV. CONCLUSION AND FUTURE WORK

Distributed Hash Table based on cloned detection protocol for WSN whose storage requirement is only a small constant. Thus protocol successfully achieving a small constant storage requirement. Based on the theoretical analysis and experimental results, the DHT protocol is proven to improve various performance indicators namely, the network lifetime is increased by 20, the Detection probability is increased by 50%, and storage requirements are only 1/5 those of the LSM protocol.

FUTURE WORK:

Enhanced Random walk method is used. In this each node broadcast a signed location claim. Each of the node's neighbors probabilistically forwards claim to some randomly selected nodes. Each randomly selected node sends a message containing the claim to initiate a random walk in the network. The passed nodes are selected as witness nodes and it will store the claim. If any witness collects different location claims for the same node ID. This will result in the detection of the replicated node.

V. 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

[4] J. Select. Areas Commun., vol. 28, no. 5, pp. 677-691, Jun. 2010.

[5] 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.

[6] B. Zhu, S. Setia, S. Jojodia, S. Roy, and L. Wang, "Localized multicast: efficient and distributed replica detection in large-scale sensor networks," IEEE Transactions Mobile Comput., vol. 9, no. 7, pp. 913-926, Jul. 2012.

[7] L. Jiang, A. Liu, Y. Hu, and Z. Chen, "Lifetime maximization through dynamic Ring-based routing scheme for correlated data collecting in WSNs," Comput. Electr. Eng., vol. 41, pp. 191–215, Jan. 2015.

[8] W. T. Zhu, "Node replication attacks in wireless sensor networks: bypassing the neighbor-based

detection scheme," in NCIS Int. Conf., 2011, pp. 156-160.

[9] J. Ho, M. Wright, and S. K. Das, "Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing," IEEE Trans. on Mobile Comput., vol. 10, no. 6, pp. 767-782, Jun. 2011.

[10] J. Ho, M. Wright, and S. K. Das, "Distributed detection of mobile malicious node attacks in wireless sensor networks," Ad Hoc Netw., vol. 10, no. 3, pp. 512–523, May. 2012.

[11] Z. Zheng, A. Liu, L. Cai, Z. Chen, and X. Shen, "Energy and memory efficient clone detection in wireless sensor networks," IEEE Transactions Mobile Comput. 2015.

[12] Mianxiong Dong, Kaoru Ota, Laurence T.Yang,Miyi Guo, "A low storage clone detection protocol for cyber physical system" IEEE Transaction computer aided design., 2015.

[13] W. Naruephiphat, Y. S. Ji, and C. Charnsripinyo, "An area-based approach for node replica detection in wireless sensor networks," in TrustCom Int. Conf., 2012, pp 745-750.

[14] A. Liu, X. Jin, G. Cui, and Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Inf. Sci., vol. 230, pp. 197-226, May 2013.

[15] M. Dong, K. Ota, A. Liu, and M. Guo, "Joint optimization of lifetime and transport delay under reliability constraint wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 1, pp. 225-236, 2016.

[16] W. Huo, S. Mohammed, J. C. Moreno, and Y. Amirat, "Mobile target detection in wireless sensor networks with adjustable sensing frequency," IEEE Systems Journal, pp. 1–14, 2014.