isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 2 ,Apr,2023 ,ISSN_NO: 2321-3337

DETECTION OF MISBEHAVIORAL ACTIVITY AS COPY CAT NODES IN WIRELESS SENSOR NETWORKS TO ENHANCE THE NETWORK SECURITY

Brindha.P[1], Dhivya Bharathi.J[2], Sathya.S[3], Suresh S[4]
UG Scholar[1,2,3], –Department of Computer Science and Engineering,
GRT Institute of Engineering and Technology, Tiruttani, India.
Assistant Professor[4] -Department of Computer Science and Engineering,
GRT Institute of Engineering and Technology, Tiruttani, India.
brindhabean@gmail.com, dhivyab2002@gmail.com, sathyalakshmi2704@gmail.com,
surevitcahcet@gmail.com

Abstract - In the existing system, wireless sensor networks have security issues such as hacking private data and node failures. From the source node, sometimes message will not be reached the destination correctly. The receiver side system may also be affecteddue to fake message transmission by hackers. In the proposed system we use a chord algorithm. Chord is a protocol and algorithm for a peer-to-peer distributedhash table. The Chord is used to detect the cloned node in the wide network. Rivest-Shamir-Adelman (RSA) algorithm is used to encrypt and decrypt the data at both sender and receiver nodes. The chord is used as a location algorithm. A Group leader will allocate a random number with time stamp to the available nodes in the particular network location. We have a centralized server called witness node. If same key is given by another node, the witness node identifies clone node and it terminates the transmission whether it is a fake node. With the help of RSA and chord algorithm we ensure the double protection of data from mis behavioral activity and trust to use the data fairly and responsibly.

Keywords: Distributed Hash Table, chord algorithm, RSA algorithm, witness node, random number, timestamp, encryption.

1. INTRODUCTION

A wireless sensor network consists of sensors that have sensing, computation and wireless communication capabilities. Wireless sensor has been used in various fields such as military, health, environmental, home and other commercial areas.There is no practice of monitoring and maintaining the sensors so this may catch in many attacks. A malicious user may compromise some sensors and deploy clones by launching variety of attacks by duplicated the sensors to acquire the private information of the users. As the duplicated sensors having the same information captured from the legitimate sensors, the hackers can easily participate in network operations and launch attacks. So, there is a need to effectively detect theclone attacks in order to ensure healthy operations of WSNs. To detect the clone node a witness node is used to certify the legitimacy of the nodes in the network during the data transmission of any nodes in the networks. The source nodes will send the request to the witness node for verification and witnesses will report a detected attack if the node fails the certification. For successful clone detection there are two requirements:
i) witnesses should be randomly selected. ii) at least one of the witnesses can successfully receive all the verification messages for clone detection.

2. SECURITY POLICY

When it comes to clone detection using Wireless Sensor Networks (WSNs), there are several security policies that should be considered to ensure the integrity and confidentiality of the data being collected and transmitted.

2.1 Authentication: To ensure that only authorized nodes can access the WSN, it is important to implement authentication mechanisms. This can include using apre-shared key, digital certificates, or other authentication protocol to authenticate nodes before allowing them to join the network.

2.2. Encryption: To protect data being transmitted over the WSN, encryption mechanisms should be implemented. This can include using symmetric encryption, asymmetric encryption, or other encryption algorithms to protect the data from unauthorized access.

2.3. Access control: Access control mechanisms should be implemented to control who has access to the data collected by the WSN. This can include setting up permissions and roles for different users, as well as implementing access control lists to restrict access to sensitive data.

2.4. Physical Security: Physical security measures should be implemented to protect the WSN from physical attacks, theft, or tampering. This can include installing security cameras, using locks and key cards, and monitoring the physical environment around theWSN.

3. RELATED WORK

An energy-efficient clone detection protocol called ERCD to prevent clone attacks in wireless sensor networks (WSNs). The protocol uses a combination of a distributed hash table and a cluster-based approach to detect and report any clone nodes [1]. Although challenges of machine-to-machine (M2M) communications offers plenty, there need a solutions to which require green (energy-efficient), reliable, and secure communications [2]. Wireless sensor has been used in various fields such as military, health, environmental, home and other commercial areas [3]. Various protocols used in WSNs such as routing, data dissemination, time synchronization, and medium access control [4]. There is also a routing protocol called Energy-Aware Routing Protocol (EARP) that uses this cost function to select energy-efficient paths for data transmission [4]. A secure data collection is achieved by using randomized dispersive routes to avoid data interception and adversary attacks. It involves randomly dispersing data packets through multiple paths and ensuring their anonymity, which increases the difficulty of interception and reduces the probability of parasitic adversaries [5]. To detect and defend against parasitic adversaries, a randomized approach is used where nodes exchange a tokenbetween them, which is then used to detect any abnormal behavior. It is robust and efficient in detecting and defending against attackers [6]. Another method is the pseudonym changing strategy for preserving location privacy in vehicular ad hoc networks (VANETs). A current location privacy schemes based on pseudonyms fail to provide sufficient privacy protection because an adversary can linkpseudonyms of a vehicle and track its movement. The proposed scheme changes the pseudonym of a vehicle when it reaches a "social spot" such as a gas station or a shopping center, where many other vehicles alsochange their pseudonyms. By using simulations, it can effectively preserve the location privacy of vehicles without introducing significant communicationoverhead [7].

According to the smart grid system, an early warning system is used to detect and prevent cyber-attacks. It is done by the utilization of distributed anomaly detection techniques to identify and respond to anomalous behavior in the network[8].

4. METHODOLOGY

In the proposed system we use a chord algorithm. Chord is a protocol and algorithm for a peer-to-peer distributed hash table. The Chord is used to detect the cloned node in the wide network. Rivest-Shamir- Adelman (RSA) algorithm is used to encrypt and decrypt the data at both sender and receiver nodes. The chord is used as a location algorithm. Every group will have a group leader. A Group leader will allocate a random number with time stamp to the available nodes in the particular network location. We have a centralized server called witness node. If same key is given by another node, the witness node identifies clone node and it terminates the transmission whether it is a fake node.

With the help of RSA and chord algorithm we ensure the double protection of data from mis-behavioral activity and trust to use the data fairly and responsibly as shown in the fig 4.1.

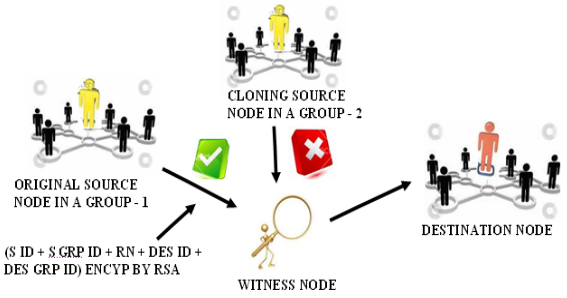

CLONING SOURCE NODE IN A GROUP - 2
ORIGINAL SOURCE NODE IN A GROUP - 1
DESTINATION NODE
(S ID + S GRP ID + RN + DES ID + DES GRP ID) ENCYP BY RSA
WITNESS NODE

Fig 4.1 Architecture Diagram

4.1 Network Construction

It is developed in order to create a dynamic network. In a network, nodes are interconnected withthe admin, which is monitoring all the other nodes. All nodes are sharing their information with each other.

4.2 Chord Algorithm

In this, we can verify the Neighbor nodes information of the Requested Node. So that by verifying the Id’s 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 nodes request.

Algorithm:

```
// ask node n to find the successor of id
n.find_successor(id)
// Yes, that should be a closing square bracket to
match the opening parenthesis.
// It is a half closed interval.
if id ∈ (n, successor] then
   return successor
else
   // forward the query around the circle
   n0 := closest_preceding_node(id)
   return n0.find_successor(id)
```

4.3 Witness node Distribution

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.

4.4 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 theRandom 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.

4.5 Verification of user id

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 UserInformation. If both the data are matched then theWitness node will confirm that this node with thatLocation is Genuine.

4.6 RSA Algorithm

The RSA (Rivest-Shamir-Adleman) algorithm is the most widely used public-key encryption algorithm which is used for both public-key encryption and digital signatures. RSA algorithm is mathematically infeasible to factor sufficiently large integers which are believed to be secure if its keys have a length of at least 1024-bits.

Key Generation steps:

1.Choose first two largest prime integers as p and q.
2.Compute n and Q(n) where n=pq and Q(n)=(p-1) (q-1).
3.Choose an integer e, 1<e<Q(n) where (greatest common denominator) gcd (e, Q(n)) =1.
4.Compute d,1<d<Q(n) where ed=1
The public key is (n, e) and the private key is (n,d).
The values of p, q and Q(n) are private.
E is the public or encryption exponent.
d is the private or decryption exponent.

4.7 Cloning detection and data transfer

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 Mal practice has occurred and the Packets are discarded by the witness node.

5. IMPLEMENTATION

5.1 Network Construction

The construction of a network for detecting clone nodes using WSN involves the deployment of a large number of sensor nodes and the implementation of specific algorithms to detect and identify clone nodes.

Here are the steps involved in constructing a network for detecting clone nodes using WSN:

Deployment: The first step is to deploy a large number of sensor nodes in the area of interest. The nodes should be distributed in such a way that they cover the entire area and are close enough to each other to form a communication network.

Node Identification: Each sensor node should have a unique identifier (ID) that cannot be easily duplicated. The ID can be based on the hardware of the node, such as its serial number or physical characteristics.

Detection Algorithm: A detection algorithm is implemented on the nodes and the base station to detect and identify clone nodes. The algorithm should be designed to compare the IDs of neighboring nodes and detect any duplicates.

Alert Mechanism: If a node detects a clone node, it should send an alert message to the base station. The base station can then take appropriate actions to isolate the clone node and prevent it from causing any harm to the network.

Security Measures: The network should be secured using appropriate security measures, such as encryption and authentication, to prevent unauthorized access and attacks.

Testing and Evaluation: The network should be tested and evaluated to ensure that it meets the requirements of the application. Testing can involve measuring the performance of the network, such as detection accuracy and false alarm rate, and evaluating the security of the network against various attacks.

5.2 Detection of clone

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 thatTime 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. Otherwise, it is clone node.

5.3 Network Security

Network-wide broadcast: The base station periodically broadcasts a message asking all nodes to report their ID. Each node responds with its unique ID, and the base station creates a list of active nodes in the network.

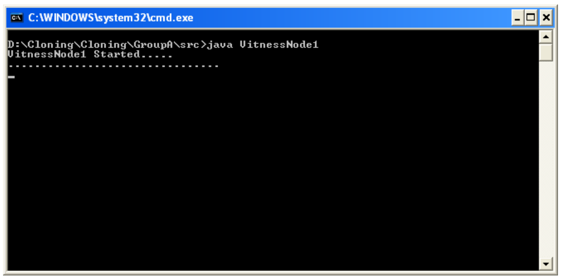
Neighbor discovery: Each node listens for messages from its neighbor and maintains a list of their IDs. If a node detects that two of its neighbor have the same ID,it sends an alert message to the base station.

Verification of node status: The base station verifies the status of the reported node by sending a challenge message to the node, which it must respond to correctly.

Deployment monitoring: The network administrator should monitor the deployment of the nodes to ensure that no additional nodes are introduced into the network without authorization.

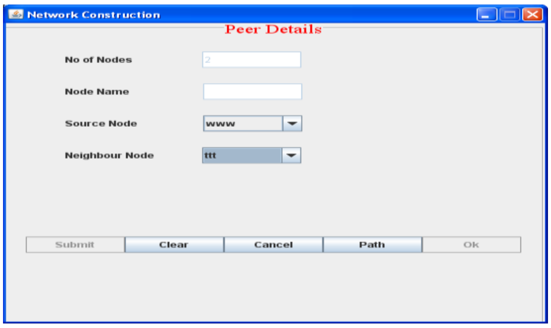
6. EXPERIMENTAL RESULTS

This paper discusses about the clone detection in WSNs demonstrate the effectiveness of these algorithms in enhancing the network security and detecting malicious activity.



```
D:\Cloning\Cloning\GroupA\src>java VitnessNode1
VitnessNode1 Started.....
...............................
_
```

Fig.6.1. Witness node



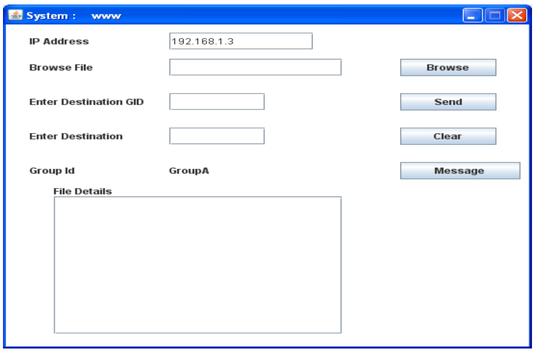
No of Nodes: 2

Node Name:

Source Node: www

Neighbour Node: ttt

Fig.6.2. Node path construction



IP Address: 192.168.1.3

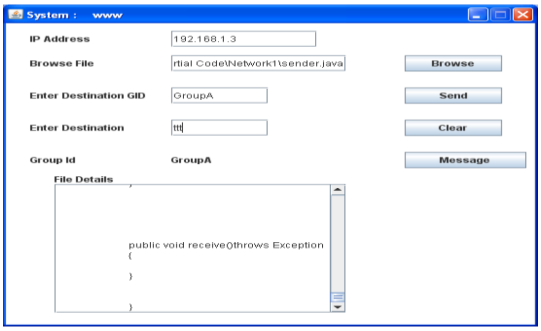
Browse File:

Enter Destination GID:

Enter Destination:

Group Id: GroupA

Fig.6.3. Node Windows


System : www

IP Address: 192.168.1.3

Browse File: rtial Code\Network1\sender.java

Enter Destination GID: GroupA

Enter Destination: ttt

Group Id: GroupA

File Details

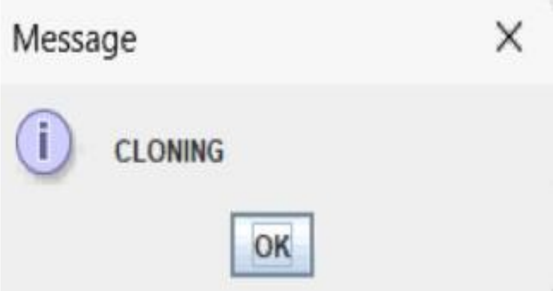
```
}
public void receive()throws Exception
{
}

}
```

Fig.6.4. File Sending

Message

Message sent successfully

Fig.6.5. Message sent successfully


Message

CLONING

Fig.6.6. Detection of cloning message

7. CONCLUSION & FUTURE WORK

In this paper, we have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message.

In addition, our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity ofdata buffer. This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.

Future enhancement:

The future work of this paper is we can use Machine learning techniques to enhance clone detection by providing more accurate detection and classification of cloned nodes. For example, deep learning models can be trained on large datasets of sensor data to improve the accuracy of clone detection.

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. IEEEINFOCOM, 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 Commun. Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] I. F. Akyildiz, W. Su, Y. Sankara Subramaniam, and E. Cayirci,“Wireless sensor networks: A survey,” Computer Network., 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 Network 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 Trans. Mobile Comput vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, “A randomized counter measure against parasitic adversaries in wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 28, no. 7,pp. 1036–1045, Sep.2010.

[7] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs, “IEEE Trans. Veh. Technol., vol.61, no. 1,pp.86-96,Jan. 2012.

[8] Z. M. Fadlullah, M. Fouda, N. Kato, X.Shen, and Y. Nozaki, " An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50-55, May. 2011.

About the Author

1. **Ms. Brindha P** is pursuing her B.E., in Computer Science and Engineering from Anna University.
2. **Ms. Dhivya Bharathi J** is pursuing her B.E., in Computer Science and Engineering from Anna University.
3**. Ms. Sathya S** is pursuing her B.E., in Computer Science and Engineering from Anna University.
4. **Mr. Suresh S, M.E.,** currently working as Assistant Professor in GRT Institute of Engineering and Technology, Tiruttani, Tamilnadu, India and pursuing Ph.D., Part-Time (External) in Anna University, Chennai, Tamilnadu, India. His research interest is Wireless Sensor Networks, Cognitive Radio Networks Data Mining, AI and NLP.,