Research Article

Replica Node Detection Using Enhanced Single Hop Detection with Clonal Selection Algorithm in Mobile Wireless Sensor Networks

L. S. Sindhuja and G. Padmavathi

Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women University, Bharathi Park Road, Mettupalayam Road, Coimbatore, Tamil Nadu 641043, India

Correspondence should be addressed to L. S. Sindhuja; sindhuja.karthick2011@gmail.com

Received 7 July 2015; Revised 12 November 2015; Accepted 19 November 2015

1. Introduction

Wireless Sensor Network (WSN) comprises a group of wireless sensor nodes that form a communication network. These nodes collect the sensitive information from the region and send these contents as a message to the base station where it checks the data and ID sent by the sensor nodes. These sensor nodes are normally low priced hardware components with constraints on memory size and computation capabilities. The Mobile Wireless Sensor Networks are similar to WSN except that the sensor nodes are mobile in nature. The various applications of Mobile Wireless Sensor Networks include robotics, transportation system, surveillance, and tracking. Researchers focus to integrate Mobile Wireless Sensor Networks into “the Internet of Things (IoT)” [1]. However, a huge amount of security issue arises in the form of attacks due to lack of hardware support and insecure sensor nodes. One such attack is the node replication attack.

In sensor networks, attackers capture and compromise nodes to inject fake data into the network that affect the network communication and operations. Such type of attack is known as replica node attack [2–5]. The adversary captures secret keys from the compromised nodes and spreads them as replicas in the network. Replicas are reflected as honest by its neighbors and normal nodes are not aware of replicas present as their neighbors. It also colludes and acts as legitimate node that provides firmness to the network.

The replica nodes are controlled by the adversary. The problem is the replica nodes also contain the key that is required for secured communication in the network. In addition to these problems, mobility of nodes, the collusion of replica, and sideway attacks are the main difficulty while detecting and controlling these replica nodes. When the replicas are not detected, then the network will be open to attackers and the network becomes more vulnerable.
The detection of replica node in the Mobile Wireless Sensor Networks is a crucial task. So far, only few detection schemes have been proposed [6–9]. Since the adversary distributes replica nodes everywhere in the network, the mobility-assisted detection scheme is required to detect the replicas in the network.

In the earlier works, mobility assisted technique, Single Hop Detection (SHD), was proposed. In SHD, each node broadcasts its location claim to its single hop neighbors and selects the witness node. The selected witness node detects replicas by performing the verification process. As a result, it reduces communication overhead. However, when the replicas collude with each other, they select replica as a witness node. Hence, the detection accuracy is low.

The main objective of the proposed work is to improve the detection accuracy by selecting the appropriate witness node with reduced overheads during the detection of replica nodes in the mobile wireless sensor networks. To meet the objective, SHD is enhanced using the Artificial Immune System.

Artificial Immune System (AIS) is a branch of Artificial Intelligence based on the principles of Human Immune System. It provides various solutions to the real world problems due to its characteristic features. The characteristic features include learning ability to the new conditions, adaptability and distributed nature to the diverse environment, limited resources, survivability even in the harsh environments. The enhancement of SHD with AIS improves the detection accuracy.

The contribution of the paper includes the enhancement of the SHD method by applying the Clonal Selection algorithm for selecting the witness nodes that is another contribution. Due to this, the detection ratio is increased by selecting the appropriate witness nodes and thereby, the replica node detection process incurs minimum control overheads.

This paper is organized as follows: In Section 2, various related works towards this technique implemented by different authors are discussed. In Section 3, the system model is discussed. In Section 4, proposed CSSHD method is briefly explained and in Section 5, the performance of the proposed technique is compared with the existing technique based on certain performance metrics and finally Section 6 concludes the paper.

2. Previous Works

Identifying the replicas in mobile wireless sensor networks is an enforcing task under hostile environments. The existing node replication attack detection methods are either centralized or distributed [6–12]. The centralized detection method has distinct points where it can fail and also can be captured by the adversary. As a result, distributed detection methods are proposed in the literature. The distributed replica detection methods are of different types [13], namely,

(i) information exchange based method,
(ii) node meeting based method,
(iii) mobility assisted based detection method.

Of the detection methods, only the distributed detection methods are discussed below.

Yu et al. [6, 12] in 2013 present the eXtremely Efficient Detection (XED) method. This is a distributed detection algorithm for mobile networks in which the detection is based on the information exchanged between the nodes in the network. It detects the replica based on the random number exchanged between each other of the two nodes. The detection capability is degraded when the replicas exchange the exact random value.

Ho et al. [7] in 2009 presents the Sequential Probability Ratio Test (SPRT); at each periodic time, the sensor node travels to the new position; it signs the claim and sends this claim to its neighbors and to the base station. The base station calculates the speed depending on the probability ratio test and matches it with the observed speed. If the observed speed is higher than the computed maximum speed, then the detected node is a replica node.

Conti et al. [8] in 2008 introduced a clone detection mechanism called Simple and Co-operative Distributed Detection (SDD & CDD). To duplicate a node, it must be isolated from the network and then its information must be extracted. This information earns some periodic time and the Simple Distributed Detection [8] uses that time period for detecting the replica. The detection capability of Simple Distributed Detection (SDD) does not provide much accuracy to detect the replica nodes and thus improved to develop a Co-operative Distributed Detection (CDD) procedure. The CDD [8] use the nodes cooperation to improve the replica node detection rate. The nodes interchange the information when nodes are in the same communication radius. This method increases the detection probability.

Zhu et al. [9] in 2007 proposed an Efficient and Distributed Detection (EDD), a node meeting based distributed detection method. The EDD method computes the number of encountering times between nodes in a given time period “T” with higher probability. If a node with a higher threshold value is encountered, then it is considered as a replica node.

Lou et al. [14] in 2012 proposed Single Hop Detection (SHD) method. It is a mobility assisted based distributed detection method. In SHD method, when a node appears at different neighborhood community, replica is detected. This method improves the communication overhead.

All the above methods discussed are compared and Table 1 presents the comparison.

The parameters used by various detection methods for evaluation are the number of claims, overheads, detection rate, and false detection rates. From the literature it is observed that SHD method is efficient when compared to other detection methods in terms of control overheads but the detection accuracy is low when the replica is selected as a witness node. Hence an attempt is made to enhance the SHD method using Artificial Immune System in terms of detection accuracy with minimum number of control overheads. The system model of the proposed work is explained in the next section.
### Table 1: Comparison of node replication attack detection techniques in Mobile Wireless Sensor Networks.

<table>
<thead>
<tr>
<th>Year</th>
<th>Author(s)</th>
<th>Technique(s)</th>
<th>Replica detection mechanism</th>
<th>Parameters used</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>Zhu et al. [9]</td>
<td>Efficient and Distributed Detection (EDD)</td>
<td>When a node exceeds the predefined threshold value, then it is detected as replica</td>
<td>Detection accuracy, detection time, storage overhead, computation overhead, and communication overhead</td>
</tr>
<tr>
<td>2008</td>
<td>Yu et al. [12]</td>
<td>Extremely Efficient Detection (XED)</td>
<td>Based on the random value exchanged between the two nodes, replicas are detected</td>
<td>Detection accuracy, detection time, storage overhead, computation overhead, and communication overhead</td>
</tr>
<tr>
<td>2008</td>
<td>Conti et al. [8]</td>
<td>Simple and Co-operative Distributed Detection (SDD &amp; CDD)</td>
<td>Replicas are detected based on the periodic time of the nodes in the network</td>
<td>Detection probability, false positive, and false negative</td>
</tr>
<tr>
<td>2009</td>
<td>Ho et al. [5, 7, 11]</td>
<td>Sequential Probability Ratio Test (SPRT)</td>
<td>Detects the replica, when the node appears at distinct locations exceeding the predefined velocity</td>
<td>Number of claims, false positive, and false negative</td>
</tr>
<tr>
<td>2012</td>
<td>Lou et al. [14]</td>
<td>Single Hop Detection</td>
<td>When a node appears at different neighborhood community, replica is detected</td>
<td>Detection time and communication overhead</td>
</tr>
</tbody>
</table>

### 3. System Model

Before the application of the enhanced SHD method for detecting node replication attack, the system model used by the study must be discussed. The system model is further discussed in terms of the network model and the threat model.

#### 3.1. Network Model

Mobile Wireless Sensor Network is built up of several sensor nodes which have distinct identity ID from 1 to \( n \). It uses symmetric routing that refers to the identical path of the data transfer between the source and the destination and vice versa. Every node sends beacon message periodically in the format (ID, neighbor ID) and supports equal time interval period. Each node in the network is considered to be mobile. It uses random way point (RWP) mobility model [15–17] for the mobility. The other mobility models available are Random Mobility model, Random Waypoint Mobility model, Random Direction Mobility model, a boundless simulation area mobility model, Gauss-Markov Mobility model, probabilistic random walk mobility model, and city section mobility model [18], out of which the random way point mobility model is very important for the problem area due to the flexibility and the reasonable patterns created to appear in real-life.

Each node knows its own location and aims to reach the destination point with its velocity in a predefined interval randomly in the sensing field. When a node reaches the destination point in a network, it remains static for a random amount of time. Each time, the node uses the same mobility rule again. For minimizing the complexity in the mobility, each node has \( k \) average neighbors per each move in the network. The value of \( k \) varies within \( [1, 2, \ldots, p] \) where \( p < N \). \( “N” \) is the number of nodes in the Mobile Wireless Sensor Networks. The network uses identity-based public key system for data protection during packet transmission [15]. Each node stores its own private key and a master public key. The private key is used to sign claim messages.

In consolidation, the following are the assumptions made in the creation of a network model:

1. Movement of nodes according to Random Waypoint Mobility model.
2. Identity-based public key system that is used to protect the data.

#### 3.2. Threat Model

Nodes in the Mobile Wireless Sensor Networks are not resistant proof. An active adversary may compromise sensor nodes and may use those nodes to create attacks in Mobile Wireless Sensor Networks. An adversary can launch Denial of Service (DOS) attacks by jamming the path from benign nodes [2]. To maximize the effectiveness of an adversary in the network, an adversary can also launch a node attack called a replication attack in which the replica nodes can be launched by accessing the node’s legitimate security credentials by compromising the nodes immediately at every sensor deployment. It is to be noted that an adversary can use these replica nodes in different patterns in an attempt to frustrate the Single Hop Detection (SHD). The replica nodes may collude with each other that lead to corruption of the detection protocol at zero delay. While running node replication attack detection protocol, an adversary can cause the routing protocol to selectively jam the path or damage few nodes in the network.
Due to this threat in mobile wireless sensor network model, the proposed method Enhanced SHD using Clonal Selection algorithm of AIS (CSSHD) is developed.

4. Proposed Methodology

The proposed work is based on the mobility assisted distributed detection of replica node in mobile WSN. The replica detection method is done by enhancing SHD using Clonal Selection algorithm. The selection of witness nodes is based on the Clonal selection algorithm. The existing SHD method is explained below.

4.1. SHD. The SHD method is a mobility assisted detection method. The SHD method [14] is based on the fact that at any occasion the node ID and private key of a node must not occur at other neighborhood communities. If it occurs, then there must be replicas in the network. The nodes that are present in the neighborhood community are defined by the list of one-hop neighbor nodes. Sensor nodes know their neighbors for communication.

The SHD method is composed of two main phases:

(i) Fingerprint claim.

(ii) Fingerprint verification.

4.1.1. Fingerprint Claim. Every node in the network signs its list of neighbor nodes. The signed neighbor node list is used as a fingerprint of its current neighborhood community. This is called fingerprint claim. The fingerprint claim is sent to all its one-hop neighborhood. After receiving the fingerprint claim from a neighboring claim node, the receiving node will make the decision to become a witness node of the claim made or not. When the node decides to become a witness node, it verifies the fingerprint claim.

4.1.2. Fingerprint Verification. The fingerprint verification consists of two steps, namely, the local verification process and the global verification process. The local verification process is performed when the receiving node accepts the fingerprint claim and decides to be the witness node. In the local verification process, the public key of the neighbor node is derived from the ID of the neighbor and the master public key is verified. The fingerprint claims are stored when the public key of the witnessed node and its fingerprint are the same. In the global verification phase, the nodes exchange the witness node when the relationship between the neighbors is built. When the private key of the node's ID shows two different locations, then they are detected as replica.

SHD has low detection rate when the witness node becomes a replica. Hence, an attempt is made to enhance the SHD method in terms of detection accuracy and control overheads; thereby the replicas are not selected as witness nodes. The enhancement of SHD using Clonal Selection Algorithm of Artificial Immune System is the proposed work.

The proposed method provides a solution to the problem related to the selection of witness node in replica detection.

The flow diagram of the proposed methodology is given in Figure 1.

4.2. Clonal Selection Algorithm. The Clonal Selection algorithm is one of the Artificial Immune System algorithms. The main consideration to propose the Clonal Selection algorithm for immunity includes safeguarding the specific memory set, selection and reproducing the most stimulated antibodies, affinity maturation, and reselection of the reproduce.

The Clonal Selection algorithm [19, 20] is explained as follows.

When the antigens affect an animal, the antibodies are produced by B-lymphocytes. Each cell produces an antibody related to the specific variety of antigen. The antigens stimulate the B-cells to divide and mature into plasma cells (terminal antibody secreting cells). As a result of the cell division process, clones are generated. The lymphocytes in addition to cell division also discriminate into long lived B-memory cells. These memory cells are circulated throughout the body. When the cells are stimulated by an antigen, large lymphocytes are produced. The large lymphocyte which generates high affinity antibodies is selected for particular antigen that triggers the primary response.

4.3. Enhanced Single Hop Detection Using Clonal Selection Algorithm (CSSHD). The proposed enhanced SHD method makes use of the Clonal selection algorithm for the enhancement. The enhanced SHD is similar to SHD except that the selection of witness nodes is done by the Clonal Selection algorithm.
Randomly select an antigen $A_n$ and assign it to all antibodies in the $A_b$.
Determine the vector $y_j$, which contain affinity of antibodies $N$.
Select the $n$ highest affinity antibodies from $A_b$.
Clone the selected antibodies $\sum_{j=1}^{n} s_n$.
Produce the number of clones $C_j$ for each of the $s_n$ selected antibodies.
Assign $C_j$ to an affinity maturation process.
Produce a population $c'^*$ of matured clones.
Determine the affinity $v_{j'}$ of the matured clones $c'^*$.
Among mature clones, elect witness node by choosing best highest affinity one ($A_b'^*$) from the mature clones in the group.
Replace the $d$ lowest affinity antibodies from $A_b[r]$, with relation to $A_g[r]$, by new individuals.

**Algorithm 1:** Selection of witness node.

The proposed CSSHD similar to SHD consists of fingerprint claim and fingerprint verification phases. In the fingerprint claim phase, the fingerprint of the node’s neighbors is exchanged between the one-hop neighborhoods. The *meeting time* $M_t$ of the two nodes "x" and "y" is computed [17] as follows:

$$M_t(x, y) = \min \left\{ t : |k_x(t) - k_y(t)| \leq R \right\}$$  \tag{1}$$

where $R$ is transmission range of sensor nodes. The mathematical formula of expectation $M_t$ is computed as $EM_t$. $EM_t$ is the time taken to deliver message from node $x$ to another node $y$.

Upon receiving the fingerprint claim, the receiving node will decide to become a witness node based on the Clonal selection algorithm.

4.3.1. Selection of Witness Node Using Clonal Selection Algorithm. The selection of witness node is based on the selection of large lymphocytes in the Clonal Selection algorithm. The node that has the maximum capability to forward data is selected as witness node. The maximum capability of the witness node is determined by its forwarding capability. The forwarding capability is determined by the trust value of the node. The trust value [18] is calculated based on the data packet forwarding ratio (DFR) and the control packet forwarding ratio (PFR). At time "$t"$, the trust value $T(t)$ of the node "y" is measured by using node "x" as follows:

$$T(t) = \delta_1 \ast CPR_x(t) + \delta_2 \ast PFR_y(t)$$  \tag{2}$$

where $\delta_1$ and $\delta_2$ are respective weights and the sum of the weights is equal to 1.

When the trust value $T(t)$ is maximum for the node "y" then the node "y" is chosen as the witness node. The replica cannot claim them as witness node because the trust value is calculated by the node "x" and not by the node "y".

The proposed Clonal Selection for witnessed node is given in Algorithm 1.

The enhanced SHD with Clonal Selection algorithm is specified by allowing antigens once from $A_n$ that performs Algorithm 1. The $n$ highest affinity antibodies were arranged in ascending order after selecting them from $A_b$, so that the number of clones for all these $n$ selected antibodies is calculated [19] as

$$N_d = \sum_{k=1}^{n} \text{round} \left( \beta \cdot \frac{N}{k} \right),$$  \tag{3}$$

where $N_d$ is the sum of number of clones produced for each of the antigens, $\beta$ is a multiple constant, $N$ is the sum of number of antibodies, and round$(\cdot)$ is operator used to round its values. Each term of this sum corresponds to the clone size of each selected antibody.

When a node becomes a witness node, it verifies the fingerprint claim. After successful verification process, fingerprint claims of the witnessed nodes are registered locally using Algorithm 2.

Upon successful verification and registration locally, the witness nodes undergo global verification process.

4.3.2. Global Fingerprint Verification. In the global fingerprint verification process, when two nodes "x" and "y" meet each other, they communicate and exchange their witnessed node lists by piggybacking the Hello message. This is the first beacon message exchanged at the time of establishment of neighbor relationship. Soon after the establishment of neighbors, these nodes exchange the fingerprint claims of nodes with each other. Further, these nodes are verified for feasible fingerprint claim conflict with received claims. The *group meeting time* $G_t$ [17] of the two node groups is defined as

$$G_t(G_A, G_B) = \min \left\{ t : |k_x(t) - k_y(t)| \leq R, \ x \in G_A, \ y \in G_B \right\},$$  \tag{4}$$

where $G_A$ and $G_B$ are the two groups of nodes. The mathematical formula of expectation $G_t$ is calculated as $EG_t$.

In a fingerprint claim conflict process, if two fingerprint claims have same ID but private key claims have different neighborhood communities, then the replicas are detected using Algorithm 3.

The flow diagram of the proposed methodology is given in Figure 2.

The pseudocode of the proposed algorithm is given in Algorithm 4.
If (local verification)
{
If (check (public key of neighbor node, fingerprint claim of neighbor node) ≠ 1)
Set signature = false
Else

claimed neighbors = extract neighbor list from fingerprint claim of a neighbor node
If (Node id not in claimed neighbors)
Set signature = false
Else
Set signature = true
}

Algorithm 2: Local verification.

If (global verification)
{
Replica list = 0
For each ID in the list of witnessed nodes of this node \( L_1 \) list of witnessed nodes of the meeting node \( L_2 \)
{
Local claim = fetch local claim of id from local stored claims
Compare claim = fetch claim of id from meeting node
If (neighbor list of local claim ≠ neighbor list in compare claim)
{
Set replica = true
Add id to replica list
}
}
}

Algorithm 3: Global verification.

The proposed CSSHD method helps in selecting the appropriate witness node. Hence, the detection accuracy can be improved by detecting the replicas with minimum control overheads. The above section clearly explained the proposed method. The next section explains the experimental setup and results.

5. Experimental Setup and Results

During experimentation, the characteristics of each node in the network and its performance are analyzed using the proposed CSSHD method. The proposed methodology is tested using NS-2 simulator, which is common and well known network simulator tool. The version of NS-2 is ns-2.34. This tool is mainly used in the simulation area of MANET, wireless sensor network, VANET, and so forth. Figure 3 shows the simulation methodology.

The simulation parameters are initialized while developing this concept and are shown in Table 2. These parameters are used for the construction of the network.

The simulation time varies from 500 seconds to 1000 seconds. During the simulation time, the statistics are collected. The statistics includes data packets received, control packets generated, sent packets, sum of all packets delay, total number of received packets, total number of replica nodes correctly found, total bytes received per second, and total number of kilobytes. Using the above statistics, the following metrics are defined:

(i) Packet delivery ratio.
(ii) Control overhead.
(iii) Average delay.
(iv) Message drop.
(v) Throughput.
(vi) Detection ratio.
(vii) False alarm rate.

The performance of the proposed method is evaluated in terms of the above parameters.

Packet Delivery Ratio (PDR). PDR is defined as percentage of packets successfully received at the destinations and the total number of packets sent by the sources defined as follows:

\[
PDR = \frac{\text{Received Packets}}{\text{Sent Packets}} \times 100. \tag{5}\]
Each packet $P$ transfer  

For each node $G^j$  

Select randomly and assign all antibodies in $Ab$  

$Ab_{Ab}^j \cup Ab_{(m)}$  

Determine vector $\nu_j$ and select $N$ highest affinity  

Assign affinity for clones and produce population for clones  

Produce clones for selected antibodies  

$N_d = \sum_{k=1}^{n} \text{round} \left( \beta \cdot \frac{N}{k} \right)$  

Set flag as 0  

Witness node  

No  

Add node to witness list $L_1$ and claim to local stored fingerprint claims  

Local verification  

No  

End  

Yes  

Global verification  

$L_1 \cap L_2$  

End  

Verify the public key and the fingerprint claim of the neighbor node  

Yes  

Fetch the local claim ID and compare it with the meeting node  

Check whether the neighbor node is in the neighbour list  

No  

Set replica as true and add ID to the replica list  

Set node as a benign node  

End  

Not equal to 1  

Extract the neighbor list from the fingerprint claim of the neighbour node  

Check whether the node id is present in the claimed neighbors  

Yes  

Set signature as true  

End  

No  

Set signature as 0  

Set signature as false  

Set signature as 0  

Set signature as true  

Set signature as false  

End  

$D = \sum_{i=1}^{n} \delta$, where $\delta = \begin{cases} 
1 & \text{if } Ab_i \neq Ag_i \\
0 & \text{otherwise} 
\end{cases}$  

$\beta \cdot N_k$  

$r$  

$\{m\}$  

$\{n\}$  

$\sum_{i=1}^{n} \text{round} \left( \beta \cdot \frac{N}{k} \right)$  

Figure 2: Flow diagram of the proposed CSSHD method.

**Overhead.** It is defined as the percentage of total numbers of control packets generated to the total number of data packets received during the simulation time given as follows:

$$\text{Overhead} = \frac{\text{Control Packet generated}}{\text{Data Packets Received}}.$$  \hfill (6)

**Average Delay.** The average delay is computed by sum of every data packet delay to the total number of received packets as defined below in (7). The parameter is measured only when the data transmission has been successful:

$$\text{Average Delay} = \frac{\text{Sum of All Packets Delay}}{\text{Total Number of Received Packets}}.$$  \hfill (7)
Set \( \{P_1, \ldots, P_n\} \) are neighbours of \( q \)

For each node \( P_i \)

- Send sign and add to neighbour list \( \{P_1, \ldots, P_n\} \)
- Beacon = \( q_{\text{id}} \)  // neighbour list
- Claim = beacon  // sign(beacon)
- Choose an antigen \( A_{n_j} \) (\( A_{n_j} \in A_{n} \))
- Add \( A_{n_j} \) to \( Ab = Ab_1 \cup Ab_m \) where \( r + m = N \)
- Vector \( V_j \) affinity and \( N \) antibodies in \( Ab \)
- Choose \( N \) highest affinity antibodies from \( Ab \)
- \( Ab = Ab_{(N)} \) where \( Ab_{(N)} \) subset of \( Ag_j \)
- Chosen \( N \) antibodies will be clones
- \( N_c = \sum_{i=1}^{N_N} \text{round}(\beta \cdot N) \)  // where \( N_c \) is the number of clones, \( N \) is the number of antibodies
- \( C = \{C_1, \ldots, C_j\} \) where \( C \) represents set of clones and \( 1 \leq j \leq n \)
- Assign clones \( C_j \) to affinity maturation process
- \( C_j = C^*_j \) of matured clones
- Calculate \( V_j^* \) of the matured clone \( C_j^* \)
- For \( j = 1 \) to \( n \)
  - Select within node \( C_j^* = \text{highest affinity (} AB_j^* \))

Next

If (node is witness node)

- Set flag = 1
- \( W = C_j^* + \{W\} \) where \( W \) is the witness node list
- Add claim of \( C_j^* \) to local stored fingerprint claim

Else
- Set flag = 0

End if

If (local verification)

- Neighbour\_claim = fingerprint of \( \{P_1, \ldots, P_n\} \)
- Neighbour\_PK = neighbour public key from \( (M_{PK} \text{ (neighbour Id)}) \)
- Check public key of neighbour node
- If (neighbour\_claim \( \neq \) true)
  - Set signature = 0
Else
  - Signature = 1
End if

Claimed neighbours = extract neighbour list from \( \{\text{neighbour claim list}\} \)

If (id \( \neq \) claimed neighbour)

- Set signature = 0
Else
- Set signature = 1

End if

End if

If (global verification)

- \( B^{\text{global}} = 0 \)
- \( L_1 = \{W_1, \ldots, W_n\} \)
- \( L_2 = \{M_1, \ldots, M_n\} \)
- For each ID in \( L_1 \cap L_2 \)
  - Claim = ID of location from \( \{\text{local stored claims}\} \)
  - Compare = ID from \( \{M_1, \ldots, M_n\} \)
  - If (neighbour list (Claim) \( \neq \) neighbour list (compare))
    - Add ID to \( B^{\text{global}} \)

Next

End if

End if

Next

Inject replicated nodes
Collect the details of the later communication between nodes
Apply SHD and enhanced SHD using Clonal Selection algorithms (CSSHD)
Evaluate the performance using the collected details
Tabulate and represent graphically the results and compare the performance

Parameters such as
(i) Channel type
(ii) Radio propagation model
(iii) Network interface type
(iv) MAC type
(v) Traffic
(vi) Mobility
(vii) Routing protocol
(viii) Simulation time
(ix) Number of nodes and mobile nodes
(x) Link layer and interface queue type
(xi) Antenna model
(xii) Maximum packet

Simulate the mobile WSN of 1000 * 1000 for different parameters

Table 2: Simulation parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel type</td>
<td>WirelessChannel</td>
</tr>
<tr>
<td>radio-Propagation model</td>
<td>TwoRayGround</td>
</tr>
<tr>
<td>network interface type</td>
<td>WirelessPhy</td>
</tr>
<tr>
<td>MAC type</td>
<td>802.11</td>
</tr>
<tr>
<td>interface queue type</td>
<td>DropTail/PriQueue</td>
</tr>
<tr>
<td>time of simulation end</td>
<td>200 s</td>
</tr>
<tr>
<td>link layer type</td>
<td>LL</td>
</tr>
<tr>
<td>antenna model</td>
<td>OmniAntenna</td>
</tr>
<tr>
<td>max packet</td>
<td>50 (Minimum: 512 bytes, Maximum: 10,000 bytes)</td>
</tr>
<tr>
<td>number of mobile nodes</td>
<td>50 (Minimum: 200 s, Maximum: 10000 s)</td>
</tr>
<tr>
<td>Simulation time</td>
<td>200 s</td>
</tr>
<tr>
<td>routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>X dimension of topography</td>
<td>1000</td>
</tr>
<tr>
<td>Y dimension of topography</td>
<td>1000</td>
</tr>
<tr>
<td>Traffic</td>
<td>tclfiles/cbr</td>
</tr>
<tr>
<td>Mobility</td>
<td>/tclfiles/speed5</td>
</tr>
<tr>
<td>number of replica node</td>
<td>5 (Minimum: 5, Maximum: 25)</td>
</tr>
<tr>
<td>Truelink</td>
<td>1</td>
</tr>
</tbody>
</table>

Message Drop. Message drop is defined as rate of number of message received in a packet at the destination by total number of message sent from source. It is represented by percentage (%):

\[
\text{Message Drop} = \frac{\text{Number of message received in a packet}}{\text{Total Number of Message Sent}} \times 100. \tag{8}
\]

Throughput. Throughput is defined as total file size transmitted in a given range. It is represented by kbps:

\[
\text{Throughput} = \frac{\text{File size}}{\text{Transmission range}}, \tag{9}
\]

where

\[
\text{Transmission time} = \frac{\text{File Size}}{\text{Bandwidth}} \tag{10}
\]

Detection Ratio. Detection ratio is defined as percentage of replica node correctly found by total number of replica node. It is represented by percentage (%):

\[
\text{Detection Rate} = \frac{\text{Number of Replica Node correctly found}}{\text{Total Number of Replica node}} \times 100. \tag{11}
\]

False Alarm Rate. False alarm rate is defined as number of replica nodes correctly found by total number of replica node. It is represented by percentage (%):
Table 3: Performance of proposed method and the existing method based on the number of nodes.

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>Control overhead (kbps)</th>
<th>Message drops (%)</th>
<th>Packet delivery ratio (%)</th>
<th>Average delay (s) * 10^{-3}</th>
<th>Throughput (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SHD</td>
<td>CSSHD</td>
<td>SHD</td>
<td>CSSHD</td>
<td>SHD</td>
</tr>
<tr>
<td>50</td>
<td>4.7500</td>
<td>2.5000</td>
<td>9.0000</td>
<td>5.7500</td>
<td>92.0000</td>
</tr>
<tr>
<td>100</td>
<td>9.5000</td>
<td>8.5000</td>
<td>13.5000</td>
<td>11.0000</td>
<td>86.2500</td>
</tr>
<tr>
<td>200</td>
<td>17.5000</td>
<td>14.2500</td>
<td>23.7500</td>
<td>21.5000</td>
<td>76.2500</td>
</tr>
<tr>
<td>Average</td>
<td><strong>11.5625</strong></td>
<td><strong>9.4375</strong></td>
<td><strong>16.4400</strong></td>
<td><strong>13.6900</strong></td>
<td><strong>83.6900</strong></td>
</tr>
</tbody>
</table>

Table 4: Performance of proposed and the existing based on the number of replicas.

<table>
<thead>
<tr>
<th>Number of replica nodes</th>
<th>Detection ratio (%)</th>
<th>False alarm rate (%) * 10^{-3}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SHD</td>
<td>CSSHD</td>
</tr>
<tr>
<td>5</td>
<td>96.5000</td>
<td>98.0000</td>
</tr>
<tr>
<td>10</td>
<td>94.7500</td>
<td>96.1500</td>
</tr>
<tr>
<td>15</td>
<td>91.5000</td>
<td>93.5000</td>
</tr>
<tr>
<td>20</td>
<td>88.5000</td>
<td>91.7500</td>
</tr>
<tr>
<td>25</td>
<td>86.5000</td>
<td>90.0000</td>
</tr>
<tr>
<td>Average</td>
<td><strong>91.5500</strong></td>
<td><strong>93.8800</strong></td>
</tr>
</tbody>
</table>

False Alarm Rate = \(\frac{\text{Total Number of Replica Node} - \text{Number of replica node correctly found}}{\text{Total Number of Replica Node}} \times 100\). \hspace{1cm} (12)

Figure 4 shows the graph for packet delivery ratio, in which the proposed method has higher packet delivery ratio compared to the existing method. The packet delivery ratio is represented by percentage (%).

Figure 5 shows the graph for control overhead where the proposed method has lower routing overhead compared to the existing method.

Figure 6 shows the graph for average packet delay wherein the proposed method has low packet delay compared to the existing method. The average delay is represented by milliseconds (s).

Figure 7 shows the graph for detection ratio where the proposed method has higher detection rate compared to the existing method. It is represented by percentage (%).

Figure 8 shows the graph for false detection ratio, in which the proposed method has low false detection ratio compared to the existing method. It is represented by percentage (%).

Figure 9 shows the graph for message drops, wherein the proposed method has lower message drop rate than the existing method. It is represented by percentage (%).

Figure 10 shows the graph for throughput where the proposed method has higher throughput when compared to the existing method. It is represented by kbps.

The overall comparison results of proposed work are shown in Tables 3 and 4. In both Tables 3 and 4, proposed method is specified as CSSHD in short.

From Table 3, it is observed that the proposed method shows a better result when compared to the existing method in terms of control overhead, message drops, PDR, average delay, and throughput.

The performance of the proposed method with that of the existing method by varying the number of replica nodes is given in Table 4.

From Table 4, it is observed that the detection ratio of the proposed method is improved whereas the false alarm rate has reduced to a greater extent when compared to the existing method.

The overall comparison results of proposed work are shown in Table 5.

Table 5 clearly shows the percentage of improvement achieved for various performance metrics of the proposed method. The proposed work improves its performance in all the metrics; particularly, the detection ratio is improved much better than the existing method.

6. Conclusion

In mobile WSN, node replication attack is a crucial one. The various replica detection methods are information exchanged based detection, node meeting based detection, and the mobility based detection. Out of these three replica detection methods, the proposed work concentrates on the mobility assisted based detection method. The proposed work
enhances the SHD method using Clonal Selection algorithm of AIS to improve the detection ratio by selecting the best witness node. The proposed CSSHD method is used in a fully distributed environment where communication occurs among single hop neighbors, highly strong against node collusion and efficient in protecting against multiple replica nodes. The experiment is conducted using the ns-2 simulator. The proposed method has high throughput, less overhead, and low false alarm rate. The results of the proposed approach are compared with existing method which shows that the average delay, control overhead, and message drops are minimized with higher packet delivery ratio value and higher detection ratio. This proves that the...
proposed method is efficient towards detecting clones that are not resilient against collusive replicas with minimum control overheads.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References


Submit your manuscripts at http://www.hindawi.com