CHAPTER 8

SECURE LOCALIZED NODE POSITIONING IN MANET USING PSO

The routing protocols of mobile ad-hoc networks use the concept of Euclidean space. Such approaches of this system will avail the mobile nodes’ position from previously used distance which measures static and dynamic mobile node positioning. The number of security issues increase when node position is known in advance. To put forth this, our strategy is to defect such security breaches using PSO and make an effective IDS. The simulated result portrays DREAM protocol to shoot out Sybil attack that replicates mobile ID within the boundary. Our assumption is that the mobile boundary has the account of mobile node and its neighbor with their distance measurement taken from routing protocol. The usage of PSO provides fitness value that tends to identify the mobile node neighbor within the boundary and thus enhances secure zone for data transmission.

8.1. SECURE LOCALIZED NODE POSITION

Including the inoperative mobile nodes in Mobile Adhoc network degrades the performance. Henceforth, an algorithm of scalability and deployability ensure maintenance of active and inactive mobile nodes that reflects in the routing table, for routing and forwarding data packets. The routine table indicates active and inactive mobile node transaction resulting in high scalable network with enormous power. Parallel storage of routing and forwarding data packets ensures balanced transaction and network setup.

The main objective is provision of secured routing protocol using Distance routing effect algorithm for mobility (DREAM) (Stefano Basagni et al, 1998) hence every node disseminates the data between the intermediate nodes using Link state algorithm.
Nodal location is the basis for focused secured nodal that is static or dynamic. The routing information (Chris Karlof et al, 2003) is updated by GPS (S. Capkun et. al, 2001) for a proactive node in the routing table in turn updates the topology. The change in one nodal update impacts all the corresponding nodes. The other scenarios are illustrated in this study.

The comparison of routing protocols was shown in the Table 1. This table shows the worst case scenario by using various routing protocol (Chris Karlof et. al, 2003).

### Table 8.1: Basic characteristic of proactive protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Relevant Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tiny OS beaconing</td>
<td>Bogus routing, Selective Forwarding, Sink Holes, Sybil, wormholes, HELLO Floods</td>
</tr>
<tr>
<td>Direct diffusion</td>
<td>Bogus routing, Selective Forwarding, Sink Holes, Sybil, wormholes, HELLO Floods</td>
</tr>
<tr>
<td>Geographical routing</td>
<td>Bogus routing, Selective Forwarding, Sink Holes, Sybil</td>
</tr>
<tr>
<td>Minimum cost forwarding</td>
<td>Bogus routing, Selective Forwarding, Sink Holes, Sybil, wormholes, HELLO Floods</td>
</tr>
<tr>
<td>Cluster based protocol</td>
<td>Selective forwarding, HELLO Floods</td>
</tr>
<tr>
<td>Rumor routing</td>
<td>Bogus routing, Selective Forwarding, Sink Holes, Sybil, wormholes</td>
</tr>
<tr>
<td>Energy conserving topology</td>
<td>Bogus routing, Sybil, HELLO Floods</td>
</tr>
</tbody>
</table>

### 8.2 OUR CONTRIBUTION

Sharing of information happens in SSH and SSL of higher layers where security issues are addressed in Link layer. The usage of protocol ensures nodal connections but not on security issues. Emerge of Sybil attack happens in Adhoc, GPS and to inculcate security using PSO and DREAM. The organization of our work focuses on the following

1. Sybil Attack
2. DREAM protocol
3. PSO for fixing fitness value to avoid attacks
Security problems that prevail in ad-hoc networks (S. Basagni et al, 2001) are enumerated within the literature (L. Zhou et. al, 1999) (F. Stefano et.al, 1999) and it does not address defense mechanisms for device networks.

8.3 Sybil attack and DREAM

Focus of our work addresses the Sybil attack and its countermeasure using PSO (James Kennedy et al, 1995) and DREAM for identifying secure neighbor node with delay measure since such delay paves way for Sybil attack.

The work of Won-Ik Kim et al highlights Stable zone and caution zone of mobile nodes as shown in Figure 8.1

![Figure 8.1: Stable and Caution zone within Transmission Range](image)

The AODV updates routing table based on time and avoids permanent route. The concepts of flooding for packet control were addressed with RREQ and RREP for deploying node transmission whereas Sybil attack creates virtual node to coordinate the delay. Maximum delay makes maximum security breach. Figure 8.2 shows DREAM implementation for proactive and reactive mechanism. It works with distance effect and mobility rate; finally results in flooding to deal with message overhead. Periodic routing table updates are avoided using
DREAM since it addresses the issue with Trajectory Based Forwarding review (TBF) (D. Niculescu et al, 2002)

8.3.1. SECURITY MEASURES

AODV requests its route based on time call which avoids mobile node to store its route permanently. In-built concept of RREQ and RREP were initiated for deploying node transmission and thus initiates flooding concept till the control packets reach the destination. The security breaches are more in AODV since it does reactive based transmission and the maximum delay paves way for more security threats. Meanwhile the Sybil attack creates virtual node position coordinates within the boundary.

Figure 8.2 depicts node distance using DREAM protocol and our assumption is that such strategy would work in proactive and reactive mechanism. DREAM protocol works based on distance effect [greater the distance slower the transmission] and mobility rate [using Local positioning system (LPS)]. The periodic updates of routing table can be boycotted in the case of adapting DREAM protocol.

Transmission between nodes using DREAM focuses on Trajectory Based Forwarding review (TBF) for maintaining decision factor before making transmission.

8.3.1. SECURITY BREACHES

Sybil attack makes multiple coordinates for an instant mobile node. This is due to the delay that occurs when mobile node makes transmission to the farthest mobile node. Figure 8.3 shows the scenario of our approach.
Figure 8.2: Distance Measure between Node A and B

Figure 8.3: Sybil Attack in Mobile Environment

Figure 8.2 shows the mobile transmission of two mobile nodes A and B. \( d \) is the distance, \( r \) is the range and \( \alpha \) is the mobile inter range boundary. Figure 8.3, depicts Sybil attack where malicious node boundary is duplicated with its coordinates. The influence of LPS comes into play to fix mobile coordinates and it reacts for both reactive and proactive nodes.
8.3.2. SYBIL COUNTERMEASURES

PSO optimizes mobile nodes based on its location along with LPS. This ensures the exact position of mobile node coordinates. The impact of Sybil attack tends to make duplicate coordinates of mobile nodes based on the mobile delay. Maximum delay leads to duplicate mobile coordinates.

8.4. PSO IMPLEMENTATION

Registration of mobile nodes sets the boundary

\[ B_{i,n} = \sum_{i=0}^{n} x^i b^{xy} \]  

(1)

Where B is the boundary set and x is the node and \( b^{xy} \) is the mobile coordinates.

The trajectory formation \( T^{xy} \) shown by the equation

\[ T^{xy} = \sum_{i=0}^{n} x^i X(t) \]  

(2)

If a connection establish between two nodes A and B then the Trajectory set for these nodes represented by

\[ T^{AB} = \sum_{i=0}^{n} x^A X(t) \]  

(3)

Where \( x^A \) is the starting node.

The distance between two nodes were estimated using the distance formulae (Subburaj.V et al, 2012)

\[ V_{ld} = w \cdot V_{ld} + C_1 \cdot r_1(P_{ld\text{-id}}) + C_1 + a/r_2(pgd-X_{id}) \]  

(4)

\[ V_{ld} = \begin{cases} V_{max}, & \text{if } V_{ld} \geq V_{max} \\ -V_{max}, & \text{if } V_{ld} \leq -V_{max} \end{cases} \]  

(5)

\[ X_{ld} = X_{ld} + V_{ld} \]  

(6)

The equation (3) to (5) are used for measuring particle movement.
The delay between nodes was identified using the RREQ and RREP within the said mobile boundary.

The transmission and delay was measured using

\[ B_{i,n} = B_{i,n-1} B_{i-1,n} \]  
\[ B_{i,n} = \prod_i^n B_{i-1,n} D_{i-1,n} \]  (7)  

The variable B is the boundary and D is the delay distortion.

![Figure 8.4: Distance measure based on LPS](image)

To optimize the mobile nodes based on its position and coordinates done with PSO shown in the equation (9).

\[ Fitness \left( B_{i,n} \right) = \frac{a}{A} - \frac{b}{B} \]  (9)  

Fitness of Sybil attack to avoid replicate coordinates

\[ Fitness \left( B_{i,n} \right) = \frac{a}{A} \]  (10)  

According the above equation for every node fitness value is set along with its coordinates. Once a node is been under Sybil attack it will never permit to access more coordinates.

For every node the following parameters are considered
1. Transmitted node (Its source and destination) also includes intermediate nodes
2. Its boundary
3. Its coordinates
4. Fitness value

All these values have to be considered in the single stretch for mobile node authentication and ensuring IDS in every transmission.

8.5 RESULTS AND OBSERVATIONS

Number of nodes used - 500
Transmission range - 250
Interference range - 550

Figure 8.5: Simulated node scenario using NS2 mobility simulator (with 25 nodes)
Figure 8.6: Node Interference on various locations

Figure 8.7: Node Interference within the boundaries of node 9, 4, 1

Figure 8.8: Node Interference between 5 and 6 and Boundary Set
8.6. RESEARCH FINDINGS

The PSO based optimized solution was proposed in this work which fight against attack. The proposed fitness value of PSO demolishes the impact of Sybil attack by removing multiple co-ordinates generation. Further the fitness function also adapts to various kind of environment to eradicate attacks in MANET environment. The experimental result with 500 mobile nodes optimizes the attack ratio of around 10 to 25 nodes. The extensions of this work will emphasis on increasing mobile node size and various types the attacks that favors the MANET environment.
Figure 8.10: Tracing Attacks in Secure and Caution Zone

Figure 8.10 shows the attack variations in secure and caution zone. The secure zone or the cluster is prevailed using PSO value and due to this the chance of attacks is very low as shown in the figure. The caution zone shows the attack impact and it can be either protected or traced for the attack and it happens in the absence of PSO optimization value.