An Effectual Instance to Mitigate Threat in Dense Mobile Ad-Hoc Network

Daljit Kaur, Jasdeep Singh

Department of Computer Science and Engineering, RIMT University, Mandi Gobindgarh, India

daljitkaur1144502@gmail.com, jasdeep42498@gmail.com

Abstract: A MANET is a self-organizing network in which all the sensor nodes of the system are self-governing without any central system to achieve routing. Nodes energetically establish paths to one more to communicate among the nodes, trusting on the neighbor nodes to keep system connected. In this paper the attention is on security matters associated to ad-hoc systems which are mainly required to deliver secure communications and possible security measures to avoid the attacks. Based on the environment of attack, the attacks are categorized into active and passive attacks. So in this paper, the important measure is taken using swarm intelligence approach which will increase the lifetime of the network and decreases the effect of attack in the networks.

Keywords: Ad-hoc networks, security threats, network lifetime.

I. INTRODUCTION

In the previous couple of decades the world has turn into a worldwide town by prudence IT sector. Information Technology (IT) is developing step by step. Organizations have a tendency to utilize more difficult system situations. Regardless of the endeavors of system heads and IT merchants to secure the computing situations, the dangers posed to individual protection, organization security and different resources by attacks upon systems and PCs. The MANETs are unquestionably a piece of this revolution. MANET is an accumulation of wireless devices or hubs that impart by dispatching packets to each other or for another device/hub, without having any framework controlling information for routing. MANET’s hubs have boundless network and versatility to different hubs. Having a secured transmission and correspondence in MANETS is a key issue because of the way that there are different sorts of attacks that the mobile system is interested in. To secure correspondence in such systems, understanding the at risk security attacks to MANETs tasks are extraordinary task and concern. MANET's example is having effects of a mixed bag of security attacks and dangers, for example,

1. Sybil attacks
2. Flooding attack
3. Wormhole attack
4. Black hole attack

II. APPLICATIONS OF MANETS

In this paper secure routing mechanism will be done to mitigate the effect of Sybil attack in which multiple copies are produced and affect the whole network in terms of signal losses, path losses, packets delivery and lifetime of the network.

Table 1: Applications of MANETS

<table>
<thead>
<tr>
<th>Areas</th>
<th>Possible scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military scenarios</td>
<td>Military communications and automated battle fields mainly based on MANETS network.</td>
</tr>
</tbody>
</table>

III. SYBIL ATTACKS

It is an unsafe advanced world out there. Security and antivirus programming is essential for any system. Restricted security can separate is in a Sybil attack. Sybil attack is a kind of security risk when a hub in a system guarantees various characters.

Most systems, similar to a shared system, depend on assumptions of personality, where every PC speaks to one character. A Sybil attack happens when an unreliable PC is captured to claim different characters. Issues emerge when a reputation system, (for example, a record sharing reputation on a system) is deceived into believing that an attacking PC has a disproportionally vast impact. Correspondingly, an attacker with numerous personalities can utilize them to act maliciously, by either taking data or disturbing correspondence.

IV. LITERATURE SURVEY

K.Sumathia et al. [5] presents the achievement of Adaptive HELLO messaging proposal to determine the local link connectivity information for monitor the link status between nodes along with the incorporation of Dynamic on Demand Routing Protocol to decrease the energy consumption of mobile nodes to certain extent. Ahmed, Mariwan et al. [6] they are suggesting modification in conventional AODV protocol to prevent Sybil attack. The essential idea to detect and isolate spurious nodes is which the use of false messages. Jhaveri, Rutvij et al. [7] proposed a scheme for Ad-hoc On-demand Distance Vector protocol, in which an middle node...
detects the spiteful node sending false routing in sequence; routing packets are used not only to pass routing in sequence, but also to pass information about spiteful nodes. V. Kamatchi et al. [8] deals with prevention of both types of sybil attacks and secure data communication using secret sharing and Random Multipath Routing Techniques.

V. RESULTS AND DISCUSSIONS

Figure 1: Sensor Network

The figure 1 shows the network creation using nodes deployment and shows the nodes are deployed in the random fashion. The normal nodes are magenta color and the nodes which are red in color are the malicious or Sybil nodes which are the duplicate copies of the original nodes.

Figure 2: Routing process

The figure 2 shows the routing between the nodes. The nodes are the neighbor nodes which are participating in the routing process in the presence of the attack. The network area is taken in 1000 meters in length and 1000 meters in width.

Figure 3: Average End Delay

The figure 3 shows the average end delay in the presence of sybil attack and shows that the system is having high end delay with increase of the sybil nodes which is of 28 ms.

Figure 4: Throughput (%) with Sybil attack

The figure 4 shows the throughput in terms of packet deliveries which shows that the 40 percent of packets are delivered with respect to the Sybil nodes which shows that the system is degraded in terms of packets deliveries.
VI. CONCLUSION AND FUTURE SCOPE

MANET is used in various types of real-time applications like military, pollution control, or any type of wireless detection arrangements. Therefore, the security, delay & protection become the main tasks in Ad-hoc networks. This paper deals with the mitigation and reduction of the effect in high dense MANET systems. So the swarm intelligence approach is able to achieve high reduction of effect and maintain routing of the nodes in optimized manner and increase the lifespan of the network. Security confrontations must be robust adequate to avoid contention to disturb the schemes. It is compulsory to handle the information with full confidentiality & with amazing level of security. The Future work can be the trust management schemes to provide more security and less error rate probabilities which more increase the lifespan of the network.

REFERENCES


