Design New Secure Hybrid Hierarchical Link State Routing Protocol (Shhls) For Manet

*1K.Thamizhmaran
Department of Electronics & Communication Engineering
Annamalai University
tamil10_happy@rediff.com

Abstract: Current research developing year’s lot of young research’s interested in Mobile Ad-hoc Networks (MANET’s) a collection of independent mobile nodes dynamically form a network connection temporarily without any base station of static infrastructure. The self-configuring ability of nodes in MANETs made it popular among critical applications like military use or natural emergency recovery. Most of the proposed protocols assume that all nodes in the network are cooperative, and do not address any security issue. To adjust to such trend, it is vital to address its potential security issues. The main objective of this paper is design new secure routing protocol namely, Secure Hybrid Hierarchical Link State (SHHLS) routing protocol to define the path for security and to further improve performance and at the same time to create energy enhanced way with excellent security. We are implementing secure dynamic on-demand routing protocol in order to achieve security goals for following parameters packet delivery ratio, routing overhead, average energy and throughput. The proposed model test SHHLS with existing Zone Hierarchical Link State (ZHLS) hybrid routing protocol and analysis stimulated through Network Simulated (NS2).

Keywords: MANET, Security issues, Routing Protocol, ZHLS, SHHLS, NS2.

I. Introduction

A mobile ad-hoc network is a collection of all independent mobile nodes that can communicate with each other through radio waves. The mobile nodes that are in the radio range of each other can directly communicate, whereas others need the aid of intermediate linked nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully dynamically distributed, and can work at any place without the help of any fixed infrastructure as base stations. MANET’s provides high mobility and device portability’s that enable to node connect network and communication to each other. It allows the devices to maintain connection to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time. Mobile ad-hoc network consist large number of node, it form temporary network with dynamic topology. In this network each node communicates with each other through radio channel without any central authority. In MANET’s each node operates in a distributed peer-to-peer modes, serves as an independent router to forward message sent by other nodes. MANET suffers from a great efficiency loss due to the misbehaving nodes which may be constrained by the resources as battery power and bandwidth of topology. Different approaches have already been proposed to detect and prevent the misbehaviour in MANET. In ad-hoc network nodes are try to disrupt the proper functioning network, Modifying packets, injecting packets or creating routing loops. In this case Security is an important task. There are large numbers of secure routing protocols proposed by many researchers they fulfill different security requirements and prevent specific attacks show in figure 1 MANET.

Figure 1 mobile ad-hoc networks
1.1 Routing Protocols

They are divided into three categories routing protocol such as: reactive routing protocol, proactive routing protocol and hybrid routing protocol.

**Table Driven / Proactive:** Proactive routing protocols acquire routing information periodically and store them in one or more routing tables. The differences among the protocols in this class are routing structure, number of tables, frequency of updates, use of hello messages and the existence of a central node. Therefore, each protocol reacts differently to topology changes. Flooding of routing information is the mechanism that is often used to discover and update routes.

**On-Demand / Reactive:** Reactive routing protocols discover or maintain a route as needed. This reduces overhead that is created by proactive protocols. Flooding strategy is used to discover a route. Reactive routing protocols can be classified into two groups: source routing and hop by hop routing. In source routing, data packet headers carry the path to destination. Hence, intermediate nodes do not care about maintaining the routing information. On the other hand, this kind of protocols may experience high level of overhead as the number of intermediate nodes increases. Also they have a higher chance of a route failure.

**Hybrid:** This protocols exhibit both reactive and proactive features. Proactive strategy is used to discover and maintain routes to nearby nodes, while routes to far away nodes are discovered reactively. Consequently, overheads and delay that are introduced by proactive protocols and reactive protocols, respectively, are minimized. Hybrid protocols have been known to be more scalable than others fewer nodes take part in routing and topology discovery. Showin figure 2 categories of MANET routing protocols.

![Figure 2 Categories of MANET routing protocols](image)

II. Literature Survey

characteristics of wireless networks. The proposed approach scheme SHHLS is also based on this assumption to provide secure transmission with minimum delay.

III. Problem Identification

Network wide routing in MANETs is a vital task of transferring data from a source to destination. The dynamic nature of MANETs requires the routing protocols to refresh the routing tables frequently that suffer from transmission contention and congestion that are the results of the broadcasting nature of radio transmission. Since a node in MANET cannot directly communicate with the nodes outside its communication range, a packet may have to be routed through intermediate nodes to reach the destination. So it also becomes essential to monitor the constraints in intermediate nodes. Consequently, an efficient routing approach may generate route failures. The simplest scheme is routing in MANET is the one to find a route without malicious nodes. This paper aims to provide an unbreakable route for secured transmission. We design new routing protocol named SHHLS. This SHHLS provides better performance compared to the existing reactive routing protocols and also reduces routing overhead without any misbehaviour at intermediate nodes.

IV. Proposed System

Secure Hybrid Hierarchical Link State (SHHLS) routing protocol like hybrid routing protocol with more secure, is that topology information is transmitted by nodes both table-driven and on-demand.

RREQ - As an optimization, SHHLS uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded.

RREP - RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address.

RERR - When a link breakage in an active and secure route is detected, a RERR message is used to notify other nodes of the loss of the link.

Node 1 after receiving the further detection message broadcast a RREQ message by setting destination address to the malicious node, and at the same time it sends an Acknowledgment Packet (AP) to Source Node (SN) through some other route.

### Design of Shhls:

1. Source node broadcast RREQ with secure packet (SRREQ) along with the destination ID.
2. For every intermediate receives the SRREQ check.
3. For every node IN receives RREP with secure Check (SRREP).
4. After receiving the reply, source node broadcast a FD message to all mobile nodes.
5. For every mobile node receive further detection message.
6. Source node waits for “wt” time
7. If all the flags are “N”
8. End.

#### 1.1 Simulation Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examined protocol</td>
<td>SHHLS, ZHLS</td>
</tr>
<tr>
<td>Application traffic</td>
<td>CBR</td>
</tr>
<tr>
<td>Transmission range</td>
<td>800m</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Maximum speed</td>
<td>25m/s</td>
</tr>
<tr>
<td>Simulation time</td>
<td>700s</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>20, 40, 60, 80, 100</td>
</tr>
<tr>
<td>Area</td>
<td>800x800m</td>
</tr>
</tbody>
</table>

V. Results & Discussion

In this paper discuss SHHLS and ZHLS with follow above simulation parameters.

<table>
<thead>
<tr>
<th>Packet delivery ratio</th>
<th>20</th>
<th>40</th>
<th>60</th>
<th>80</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHHLS</td>
<td>0.84</td>
<td>0.78</td>
<td>0.72</td>
<td>0.66</td>
<td>0.60</td>
</tr>
<tr>
<td>ZHLS</td>
<td>0.90</td>
<td>0.84</td>
<td>0.78</td>
<td>0.72</td>
<td>0.66</td>
</tr>
</tbody>
</table>
From Figure 3 and Table 2, it is clear that secure proposed scheme SHHLS surpasses ZHLS performance by above 70% when there are 30 and 150 nodes in the network.

Table 3 routing over head

<table>
<thead>
<tr>
<th>RP / NN</th>
<th>20</th>
<th>40</th>
<th>60</th>
<th>80</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZHLS</td>
<td>0.17</td>
<td>0.23</td>
<td>0.29</td>
<td>0.35</td>
<td>0.41</td>
</tr>
<tr>
<td>SHHLS</td>
<td>0.14</td>
<td>0.20</td>
<td>0.26</td>
<td>0.32</td>
<td>0.38</td>
</tr>
</tbody>
</table>

Simulation results of routing overhead shown in Figure 4 and Table 3. It is clear that SHHLS has the lowest overhead of about 30 to 150 number of nodes.

Table 4 throughput:

<table>
<thead>
<tr>
<th>RP / NN</th>
<th>20</th>
<th>40</th>
<th>60</th>
<th>80</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZHLS</td>
<td>0.13</td>
<td>0.25</td>
<td>0.38</td>
<td>0.51</td>
<td>0.55</td>
</tr>
<tr>
<td>SHHLS</td>
<td>0.22</td>
<td>0.34</td>
<td>0.47</td>
<td>0.60</td>
<td>0.64</td>
</tr>
</tbody>
</table>

Figure 5 and Table 4 proves that the proposed SHHLS provides better performance of the throughput when there are 30 to 150 of nodes compared to ZHLS routing protocol.
VI. Conclusion And Future Work

Link breakage, misbehaviour attack and packet dropping have always been a major threat to the security in MANETs. In this research paper, a novel approach named SHHLS protocol newly implemented specially designed for MANETs is proposed in comparison with other popular protocol named ZHLS through simulations. The results demonstrated positive performance of the remaining energy in SHHLS than ZHLS. Although it generates more end-to-end delay in some cases, as demonstrated in this research, it can vastly improve the network’s PDR to more than 6% compared to the existing ZHLS routing protocol and improve remaining energy by 3% compared to the existing ZHLS routing protocol when the misbehavior attackers. Eventually, it is arrived to the conclusion that the SHHLS scheme is more suitable to be implemented in MANETs also plan to investigate the following issues in our future research.

1. The same concept can be applied in satellite to reduce more congestion in the route and also to save more energy.
2. The performance of SDORP can be tested in real time network environment instead of software simulation.

Reference

Design New Secure Hybrid Hierarchical Link State Routing Protocol (Shhls) For Manet


Prof. K. Thamizhmaran has received his M.E degree from Annamalai University, Chidambaram and Tamilnadu, India in the year of 2010 and 2012 respectively. He is currently working as an Assistant Professor in ECE / Department of Electronics and communication Engg, FEAT, Annamalai University, Annamalainagar, Chidambaram, Tamilnadu, India. His research interested includes area includes Networks security, Ad-hoc Networks, Mobile Communications, Digital Signal Processing. He has published more than 74 technical papers at various National / International Conference and Journals. He is reviewer of 03 international journals and technical committee reviewer of 08 international conferences.He is a member of IAENG, IACSIT, ADSL.