Wireless Spontaneous Network Creation with Energy Efficient Authentication

Prof. D.N. Rewadkar¹, Ms. Smita Karve²

¹ Professor in Computer Dept, RMD Sinhgad School of Engineering, Warje, Pune-58
² ME Research Student, Computer Dept, RMD Sinhgad School of Engineering, Warje, Pune-58

Abstract—Wireless Ad-Hoc networks are a form of peer-to-peer network where nodes can communicate with each other without any central infrastructure. In spontaneous network, devices are placed close to each other for accessing services and sharing resources among each other for short period of time and network is formed spontaneously without help of any external or central infrastructure. The proposed protocol creates and manage spontaneous network in order to save energy of network without dropping the packets. The proposed protocol also secure network by using symmetric and asymmetric cryptographic technologies. An authentication technique is used at the time of joining new user into the network.

Keywords—LID, Spontaneous Network, MANET, protocol.

I. INTRODUCTION

Spontaneous networks are created in a situation where devices are placed close to each other i.e. within a range of Wi-Fi. Consider an example, if you want to buy a gift for your friend and you go in a gift shop. You find shop is closed, in such situation; you will perform following steps:

1. Join Wi-Fi network of shop
2. Access services given by shop owner
3. Enter necessary information
4. Select gift and enter friends address and contacts
5. Send gift to friend
6. Leave network

To perform all these tasks you just connect to shop’s network without internet connection and access the services, is called spontaneous network. Just create network among wireless devices, placed close to each other for small period of time, join new user into the network, access services and resources and leave the network without any central infrastructure. First user creates the network and does all global settings like SSID, IP address space, session key generation etc. Just creating the network without security may be vulnerable to attacks so some security is required for managing network. In [2], authors have developed a secure protocol for wireless spontaneous network which provides various security measures for network. They have implemented authentication mechanism at the time of joining new user into the network. For authentication they used public key cryptography for transmitting packets. RSA algorithm is used for generating public and private key pair. After authentication for communication they used private key cryptography, session key is used as private key. Session key is generated using AES algorithm. This session key is revoked periodically after expiration. They have also used Central Authority (CA) for certificate generation and distribution. As, it is a peer-to-peer network, any user can acts as CA. Digital signature is created using SHA-1 algorithm which validated at the time of authentication. In [2] authors also used the trust mechanism. Trust is implemented on face-to-face basis. Consider there are three people A, B and C. if A knows B then A trusts on B. If B knows C then B trusts on C. And A also trusts on C. In proposed work, laptops are considered as wireless devices and Wi-Fi is used for communication among nodes of the network. The proposed system is implemeneter only for wireless communication using Laptops as wireless devices. Most of the system uses manual energy for simulation. In proposed work Battery capacity of Laptop is considered as energy of node. For experiments 15% of battery is considered as threshold value of laptop.
II. LITERATURE SURVEY

A lot of work has been done on spontaneous network. L.M. Feeney, B. Ahlgren, and A. Westerlund have proposed the concept of spontaneous networking in [1]. They have explained the need of spontaneous network and various features of spontaneous network in detail. IP addressing is one of the important part while grating a network. IP address is an address of node into the network. This IP address configuration in spontaneous network is explained by R. Lacuesta and L. Penaver in [4]. In [3], authors have given energy efficient protocol for spontaneous network which is based on manual energy not actual battery of laptop is one of the major issue which is overcome in proposed work where actual battery is considered for authentication. As I have mentioned that in spontaneous network we can share resources. On this basis authors R. Lacuesta, J. Lloret, M. Garcia, and L. Penalver have designed a spontaneous network to share WWW access in [5]. Just creating and accessing network without providing security is nothing but inviting attacks in to the network. To avoid attacks in [6] authors have explained security architecture for spontaneous network. Lacuesta, J. Lloret, M. Garcia, and L. Penalver have proposed two protocols for securing the network and also for saving energy of nodes for spontaneous mesh networks in [7]. In [8] and [9] authors have explain various security aspects and attacks on MANET. In [10] authors have given various works done on spontaneous network with their pros and cons. In [11] and [12] we have studied RSA and SHA algorithm. And in [13], author has provided cryptography and network security. After performing literature survey, some issues are figure out that are, all the works are done in simulation, also they have used Bluetooth for communication which is costly and also has very short range as compare to Wi-Fi. Node Energy is not considered because of that packets are dropped at the receiving node. In our proposed system we are implementing spontaneous network which will save nodes energy without packet drop by considering battery capacity of node.

III. NETWORK CREATION AND MANAGEMENT

There are various steps involve for network creation and management phase given in [3]. Every user has its own Logical ID i.e. LID which is unique into the network. User has to give LID, email ID at the beginning.

1. Create Network
2. Join Network
3. Trust Implementation
4. Discover Services
5. Leave Network

A. Create Network

In [3] authors have explain network creation for spontaneous network. First user is responsible for creating the network. She/he perform all global settings like SSID i.e. name of the network, setting transmission protocol, setting IP address space and generating session key. After creating network, she/he starts services given by her/him and waits for authentication requests.

B. Join Network

New user sends join requests to any existing user of the network as in [3]. She/he has to follow steps as shown in figure 1. In previous work, nodes energy is not considered, if energy of node is low it is unable to process the request and packets are dropped this problem is overcome in proposed system, where, if energy of authenticating node is low then she/he forward request to another trusted node. After that authentication and validation of new node is done.

![Figure 1: Join Network](image-url)
C. Discover Services

Users can access and discover the services of another node into the network.

D. Leave Network

Any user can leave the network at whatever time she/he wants.

IV. PROTOCOL OVERVIEW

Protocol uses various packet formats to send request and reply between nodes. It also contains various procedures for network operations as explained above. Protocol packets used in proposed work are similar to protocol packets in [3] only difference is energy in proposed work is based battery of laptop.

A. Protocol Packets

For performing all network tasks we have proposed 20 different packets types. These different packets are shown in Table I. Protocol packets 1 to 16 are used in previous system i.e. in [2]. In proposed system we have developed four more protocol packets. P_DEL (17) is used to forward request to another trusted node at the time of joining new user. Packet number (18) is used to send low energy error message to new joining node. Last packet (20) is used by nodes to send request for trust score.

Certification Procedure: Certificates are generated and distributed by CA. An authenticating user acts as CA and store certificate of new user into the database. Certificate consists of LID, public key, creation and expiration time of public key, certificate creation and expiration date/time and CA’s signature. If node A wants to communicate with node B then A request for certificate of B from CA.

Trust Implementation: Trust implementation is based on [3] where, Q is set of questions and A no. of correct answers then Trust T is calculated as,

\[ T = \frac{\text{no of A}}{\text{no. of Q}} \]

If T is greater than threshold then nodes are trusted.

Authentication Procedure: At the time of joining network authentication procedure is carried out by authenticating node. This authenticating procedure is as shown in Figure 2. In this figure, A and B are existing users and C is new user, who sends join request to node A having low energy. LID of A, B, C are A, B, C respectively. Pk_A and Pk_B are public key of A and B respectively. When node A has low energy, it cannot process C’s request. Then node A delegate request to trusted node B. Then node B process C’s join request.

"TABLE I"

<table>
<thead>
<tr>
<th>ID</th>
<th>Packet Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>P_DISCOVERY</td>
<td>Discovery Request</td>
</tr>
<tr>
<td>2</td>
<td>R_DISCOVERY</td>
<td>Discovery Reply</td>
</tr>
<tr>
<td>3</td>
<td>P_AUTHENT</td>
<td>Authentication Request</td>
</tr>
<tr>
<td>4</td>
<td>R_AUTHENT</td>
<td>Authentication Reply</td>
</tr>
<tr>
<td>5</td>
<td>P_IP</td>
<td>IP and email checking</td>
</tr>
<tr>
<td>6</td>
<td>R_IP</td>
<td>IP and email checking reply</td>
</tr>
<tr>
<td>7</td>
<td>P_ACTUALIZE</td>
<td>Update request to one node</td>
</tr>
<tr>
<td>8</td>
<td>R_ACTUALIZE</td>
<td>Update reply from one node</td>
</tr>
<tr>
<td>9</td>
<td>P_BROADCAST</td>
<td>Update request to all nodes</td>
</tr>
<tr>
<td>10</td>
<td>R_BROADCAST</td>
<td>Update reply from all nodes</td>
</tr>
<tr>
<td>11</td>
<td>P_NODO_CONF</td>
<td>Certificate request to trusted node</td>
</tr>
<tr>
<td>12</td>
<td>P_NODO</td>
<td>Certificate reply</td>
</tr>
<tr>
<td>13</td>
<td>P_DATES</td>
<td>Packet for sending data</td>
</tr>
<tr>
<td>14</td>
<td>P_ERROR</td>
<td>Error</td>
</tr>
<tr>
<td>15</td>
<td>P_PK</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>16</td>
<td>P_DEL</td>
<td>Delegation request to trusted node</td>
</tr>
<tr>
<td>17</td>
<td>P_REFRESH_NETWORK</td>
<td>Refresh the Network</td>
</tr>
<tr>
<td>18</td>
<td>P_ERROR_ENERGY</td>
<td>Low energy reply</td>
</tr>
<tr>
<td>19</td>
<td>P_TRUSTSCORE</td>
<td>Trust calculation request</td>
</tr>
</tbody>
</table>

Figure 2: Authentication Procedure
V. RESULTS

The proposed work has been implemented on Windows 7 or 8 in JAVA technology. Laptops are used for wireless communication. The following results are drawn from system.

A. Packet Latency:

Packet Latency is a time required to receive a reply after sending packet it means it is a time interval between packets send and reply of packet. There are two results we have taken for authentication and for discovery packets. It takes more time in existing system as compare to proposed system for authentication and for discovery packets as shown in figure 3 and 4.

B. Energy Loss

We have taken three Laptops for execution of proposed system as shown Figure 5. In this figure X axis is showing name of Laptops used and Y axis is showing energy loss in joule. In existing system packets are dropped so that energy loss is more as compare to proposed system where packets are delegated to another trusted node instead of dropping the packet. Therefore, energy loss is less in proposed system.

C. PDR

PDR i.e. Packet Drop Ratio is number of packets dropped per second. As in Figure 6 packets dropped in existing system are more than in proposed system.

References


