Chapter 6

Conclusion

In this thesis author proposes self organization algorithm(s) for ad hoc networks. While discussing proposed algorithms author considers ad hoc network of sensor nodes or WSN as the application and security as the most challenging need to fulfill. Security is a relatively new area of research for WSN and public key infrastructure based security architecture is gaining momentum with some twist; such as certificate less PKI. This is not trivial.

In Chapter 1 author defines the term ad hoc networks and mention that a WSN is an ad hoc network of sensor nodes. Author also mentions that the term ad hoc network and WSN are used interchangeably in this thesis. Afterwards, motivations are discussed and identified requirements of self organization in ad hoc networks as: optimal network topology, security and performance. While outlining objectives of the thesis, the job of self organization in ad hoc networks are divided into three phases: node discovery, node joining and data communication. Author further mentions that security is a very important requirement during self organization in ad hoc networks and depending upon the type of applications users need to have option to choose low, medium and high degree of security. Structure of the thesis is discussed in overview section. Finally, in Chapter 1 contributions of the thesis are outlined in contributions section.

Chapter 2 discusses background for WSN and various assumptions and dependencies for the rest of the chapters in this thesis. In the following discussion in each section of this chapter are summarized:
- **Architecture.** Characteristics of WSN, architecture of a wireless sensor node and of a WSN.

- **Threat Analysis.** Outline threat model and trust model. Identify WSN security requirements and classify major attacks in a WSN.

- **Routing.** Discuss various routing models of a WSN and identify attacks on WSN routing protocols.

- **Key Management.** Discuss various key types in use in a WSN and provide a taxonomy on existing key management techniques for WSN.

- **Performance Metrics.** Discuss various performance metrics of a WSN.

- **Applications.** An architecture of an ad hoc sensor network for emergency medical care is discussed in this section.

Chapter 3 is a compilation of the literature survey done for this thesis work. For discussion it is grouped as follows:

- **Self Organization.** Literatures on self organization algorithms

- **Security.** Literatures on security aspects of self organization
  - Analysis: Threat analysis of a WSN.
  - Cryptographic Security: Cryptographic Algorithms which have relevance to this thesis work.
  - Security Protocols: Security Schemes that are related to this thesis.
  - Key Management: A survey is done here to understand key management in a WSN.
  - Policy & Planning: Security planning in areas such as enterprise system to understand the process and implementing the variant in a WSN.

- **Performance.** Literatures on performance of a WSN.

In Chapter 4 author proposes self organization algorithm for an ad hoc network of sensor nodes (WSN) with need based security. In the following discussion in this chapter are summarized:
• **Overview.** In this section author gives an overview of the proposed self organization approach. Horizontally, proposed approach is divided into three phases: node discovery, node joining, and data communication. Vertically, the process is divided into three categories: low, medium and high security. Key management and security planning are also considered for medium and high security. Figure 4.1 explains the whole process.

• **Node Discovery.** In this section author proposes node discovery algorithm based on unique triangulation method. Here author also demonstrates working of the algorithm by implementing it in Java and running on a synthetic data sets.

• **Node Joining.** This is the next and important phase of self organization in an ad hoc network where a new node formally joins the network. When security is not required, then any new node with its valid device id can join the network. This is termed as node joining in low security mode. However, if security is a necessity, then appropriate mutual device authentication in cipher text is required. Difference is the type of keys in use. In medium security mode author proposes to use symmetric keys. And in high security mode author discusses use of certificate less asymmetric keys. Use of symmetric keys in WSN is more common. However, if the key is compromised then the whole network is compromised. This disadvantage is eliminated by using certificate less asymmetric keys.

• **Data Communication.** The ultimate or the final phase of self organization is enabling data communication between sensor nodes and the base station. For this author proposes an end to end security scheme for encrypting and authenticating the data layer wise.

• **Key Management.** In this section author discusses key management for the keys in use for high security mode. Note that in medium security mode symmetric keys are used whose key distribution are discussed in the original SNEP algorithm proposed by Perrig et al. [2001].

• **Security Planning.** In order to provide fool proof security, an appropriate security planning is necessary. This is outlined in this section.
Table 6.1: Proposed Self Organization Algorithm

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm 1</td>
<td>Node Discovery</td>
</tr>
<tr>
<td>Algorithm 2</td>
<td>Node Joining: low security mode</td>
</tr>
<tr>
<td>Algorithm 3, 4, 5</td>
<td>Node Joining: Modified SNEP</td>
</tr>
<tr>
<td>Algorithm 6, 7, 8</td>
<td>Node Joining: HySecNJoining</td>
</tr>
<tr>
<td>Algorithm 9, 10, 11</td>
<td>Data Communication: E2ES</td>
</tr>
<tr>
<td>Algorithm 12, 13, 14, 15, 16, 17</td>
<td>Key Management</td>
</tr>
</tbody>
</table>

All the algorithms proposed in this thesis are enlisted in Table 6.1.

In Chapter 5 author discusses simulation results and analyzes the proposed algorithms. In the following discussion in this chapter are summarized:

- **Simulator Design.** For simulation author modifies and enhances the simulator designed by Stein and Esq. [2005]. In this section author gives detail view of the approach, design and test bed.

- **Cost Estimation.** As stated earlier, node joining with security is an extra overhead. In an environment where node joining happens in plain text, author assumes the overhead is null. Assuming this estimated the average cost that Modified SNEP and HySecNJoining incur for provisioning node joining in cipher text. Author also estimates the cost of provisioning end to end security of data with the help of E2ES Scheme in this section. Note that this cost estimation is fed to the simulator for simulation of the algorithms and understand its behaviors.

- **Simulation.** In this section five different simulation studies are made.
  
  - Study 1: In this study author simulates four algorithms: AllPath, Node Discovery, Modified SNEP and HySecNJoining and compare the residual energy of a WSN.
  
  - Study 2: In this study author simulates four algorithms: AllPath, Node Discovery, Modified SNEP and HySecNJoining and compare the number of alive nodes of a WSN.
– Study 3: In this study author compares residual energy and number of alive nodes of a WSN when data communication is done in plain text and when data communication is done with end to end security proposed by E2ES algorithm.

– Study 4: In this study using the WSN simulator following comparisons are made: (i) total residual energy of a WSN with and without key distribution, (ii) number of alive nodes with and without key distribution as proposed in the Chapter 4.

– Study 5: Finally, in this study scalability of the Node Discovery algorithm are tested.

• Discussion. In this section author analyzes and compares proposed algorithms with some well known algorithms and schemes.

Future Work: Due to unavailability of resources author could not test proposed algorithms in real environments involving physical motes and gateway. Author rather simulated proposed algorithms in a WSN Simulator. Testing proposed algorithms in real motes is left as future work. While designing self organization algorithms for ad hoc networks author considers WSN as its application network. Whereas author believes that the proposed algorithm will work in other class of ad hoc networks such as MANET and WMN, author has not made any study regarding this. This is left as a future work of this thesis.