Software Requirements Specification

Version 1.0

October 20, 2010

SECURITY SERVICES IN MANET USING

CLUSTERING

# Team Members G .Sriram

M. Shahul Hameed

P. M. Sharan Babu

Project Guide

Dr. V .VetriSelvi

# **Table of Contents**

**Table of Contents** ii

**Table of Figures** ii

**1.0. Purpose** 1

1.1. Introduction 1

1.2. Scope 1

1.3. Acronyms 1

1.4. References 2

1.5. Document overview 2

**2.0. Overall description** 2

2.1. Product perspective 2

2.2. Product Functions 3

2.3. User Objectives 3

2.4. User Classes and Characteristics 3

2.5. Design and implementation constraints…………………………………………………………………… 3

2.6. Software Interface………………………………………………………………………………………… .4

2.7 Communication interface………………………………………………………………………………… .4

2.8 Use Case Model survey………………………………………………………………………………… 5

2.9 Architecture Diagram…………………………………………………………………………………….. .6

**3.0. Specific Requirements…….………………………………………………………………………….. .**6

3.1. Use Case Report 6

3.2. Description of the final Product 7

3.3. Performance Parameters 7

# **Table of Figures**

Figure 1 System Design 2

Figure 2 Use Case Diagram 4

Figure 3 Architecture Diagram 5

1. **Purpose**

**1.1) Introduction**

The purpose of this document is to present a detailed description of the security architecture that can be provided for Mobile Adhoc Networks that can be used for Secure Communication among Nodes . It will explain the purpose and features of the system, the interfaces of the system, what the system will do, the constraints under which it must operate and how the system will react to external stimuli. This document is intended for the developers of this architecture and will be proposed to the panel for its approval.

**1.2) Scope**

Wireless Adhoc Networks are subjected to various Kind of security threats . we propose a Security Architecture in which we provide Security services like Authentication and Confidentiality using Clustering and Key Management.

**1.3) Acronyms**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| MANET | Mobile Ad Hoc Network |
| CH | Cluster Head |
| WCA | Weighted Clustering Algorithm |
| CBC | Cipher Block Chaining |
| MAC | Message Authentication Code |
| DES | Data Encryption Standard |
| DHA | Diffie Hellman Algorithm |

**1.4) References**

[1] Hengjun Wang,Yadi Wang, Jihong Han. “A Security architecture for tactical Mobile Ad Hoc Networks",

Second International workshop on Knowledge Discovery and data Mining, 2009.

[2] S.Muthuramalingam,R.Rajaram. “A Transmission Range Based Clustering Algorithm for Topology Control Manet",

International journal on applications of graph theory in wireless ad hoc networks and sensor networks, 2010.

[3] M.Bechler,H.J.Hof,D.Kraft,F.Pahlke."A Cluster-Based Security Architecture for AdHoc networks",

IEEE Infocom 2004.

[4] Nishi Yadav,P.M.Khilar,"Hierarchically Adaptive Distributed Fault Diagnosis in Mobile Adhoc Networks"

,ICIIS 2010.

[5] mohamed Elhousine Elhdhili,Lamia Ben Azzouz,Farouk Kamoun,"A Totally Distributed Cluster Based Key

Management Model for Ad hoc Networks",MEDHOC'04.

**1.5) Document Overview**

The remainder of this document is two chapters, the first providing a full description of the project.The entire functionality of the project is described here . The later chapter explains about functions of each module in detail.

**2. Overall Description**

**2.1) Product Perspective**

# 

**2.2) Product Functions**

* The proposed architecture provides security services like authentication and confidentiality in MANET.
* It forms clusters of nodes with a cluster head for each cluster of nodes.
* Each cluster head will then generates and manages the secret keys.
* These keys are generated on demand from the cluster nodes for communication.
* Using these keys , nodes are authenticated during communication.
* If the message being transmitted is a classified information then that message is encrypted using encryption algorithms and thus confidentiality is ensured.

**2.3) User Objectives**

The mobile nodes in the network environment can communicate between them securely using this architecture irrespective of their mobility.This architecture also enable the nodes to avoid collision of messages in the network.Messages being sent are encrypted using secret keys so that mallicious behavior of nodes are identified .

**2.4) User Classes and Characteristics**

The main user of the system is the node participating in the network scenario.

**User:** Cluster Node.

**User Characteristics:**

* Nodes are mobile in the network.
* Nodes are of limited transmission power and computing capabilities.
* Nodes may be malicious- poses security threats to the network.

**2.5) Design and Implementation Constraints**

* The network scenario is simulated assuming that all the cluster heads chosen are non-malicious nodes.
* Different metrics are assumed for Weighted clustering algorithm which are optimal values for MANET.
* Routing protocol implemented is DSR.

**2.6) Software Interface**

OMNET –II is used to simulate the network scenario.

**2.7) Communication Interface**

* The communication between the mobile nodes takes place through DSR routing protocol.
* The communication layer is also responsible for sending and receiving the messages.
* Routing involves network and transport layer of the mobile nodes.

**2.8) Use Case Model Survey**

**2.9) Architecture Diagram**



**3) Specific Requirements**

**3.1) Use Case Reports**

* **Clustering:** The cluster head is elected based on WCA.All the nodes at one-hop distance from the cluster head are formed as a cluster.
* **Key Generation:** The secret Keys are generated by the elected cluster head and given to the nodes ,encrypted using master key, on demand.These keys are used for further communication within the cluster.For communication between the cluster symmetric key cryptographic technique- diffie hellman algorithm is used.
* **Key DB Management :** The cluster head saves the key information.
* **Authentication:** The sender generates a MAC and append it with the message and sent over to the destination.At the destination ,MAC is again generated and checked with the received MAC for authentication.

**3.2) Description of the Final Product**

We will demonstrate the simulation of the proposed architecture of MANET in OMNET II.The scenario will be chosen in such a way that security threats are posed by some nodes in the network.In spite of those threats ,we will simulate how secured communication is established between the nodes.Thus authentication and confidentiality are ensured among the nodes.

A comparative performance of our proposed architecture with Other security protocols will be demonstrated using performance graphs.

**3.3) Performance Parameters**

The parameters used to measure the performance are

* The delivery of secret Keys to those nodes on demand successfully.
* Successful communication(delivery of messages) betweeen the source and destination.
* The power spent by the cluster heads in managing the communication compared to other Non – clustering techniques .