

جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences



A SECURE AGENT BASED VEHICULAR COMMUNICATION SYSTEMS

A thesis submitted in partial fulfilment of the requirements for the degree of
Master of Science in (Information/Network) Security

By:

Sara Saleh Al-amri

Bachelor degree, Princess Nourah bint Abdulrahman University, 2016

Under Supervision of:

Dr. Meryem Ammi

Submitted to:

Department of Information Security, Computer and Information Security College
Naif Arab University for Security Sciences

May 2019

Table of Contents

| | |
|---|------|
| Abstract | ii |
| Acknowledgements | iii |
| Statement of Original Authorship | iv |
| Table of Contents | v |
| List of Figures..... | viii |
| List of Tables..... | ix |
| List of Abbreviations..... | x |
| Chapter 1: Introduction | 1 |
| 1.1 IMPORTANCE OF VCS | 1 |
| 1.2 IMPORTANCE OF AGENT SOFTWARE TECHNOLOGY..... | 2 |
| 1.3 OBJECTIVES..... | 3 |
| 1.4 PROBLEM STATEMENT | 3 |
| 1.5 CONTRIBUTIONS | 5 |
| 1.6 THESIS ORGANIZATION..... | 5 |
| Chapter 2: Theoretical Background and Literature Review | 7 |
| 2.1 THEORITICAL BACKGROUND..... | 7 |
| 2.1.1 Vehicular Communication Systems | 8 |
| 2.1.2 Mobile Agents in a Mobile Environment..... | 9 |
| 2.2 RELATED WORKS | 10 |
| 2.2.1 Classification of Security Approaches for Agents..... | 10 |
| 2.2.1.1 First group: Protecting the Agent Platform | 11 |
| 2.2.1.2 Second Group: Protecting the Mobile Agent | 12 |
| 2.2.2 VCS systems' Protocols | 14 |
| 2.3 SUMMARY | 16 |
| Chapter 3: Methodology | 18 |
| 3.1 INTRODUCTION..... | 18 |
| 3.2 THREAT MODEL AGAINST THE VEHICULAR COMMUNICATION SYSTEM BASED AGENTS | 18 |

| | | |
|------------|---|----|
| 3.3 | PROPOSED PROTOCOL ARCHITECTURE | 19 |
| 3.4 | ROLES OF USED AGENTS | 22 |
| 3.5 | SECURITY REQUIREMENTS DISCUSSIONS | 27 |
| 3.6 | SECURITY OF AGENTS..... | 28 |
| 3.6.1 | Defense Against Eavesdropping Attack | 29 |
| 3.6.2 | Defense Against Man in the Middle Attack | 29 |
| 3.6.3 | Multiple Colluded Attack | 29 |
| 3.6.3.1 | Defense Against Multiple Colluded Attack..... | 30 |
| 3.6.4 | DoS attack | 33 |
| 3.6.4.1 | Defense Against DoS Attack..... | 34 |
| 3.7 | ARCHITECTURE DETAILS OF THE PROPOSED PROTOCOL..... | 38 |
| 3.8 | SECURITY ANALYSIS..... | 40 |
| 3.8.1 | Conditions-of-Success of Eavesdropping Attack | 40 |
| 3.8.2 | Conditions-of-Success of Man in the Middle Attack | 40 |
| 3.8.3 | Conditions-of-Success of Multiple Colluded Attack..... | 41 |
| 3.8.4 | Conditions-of-Success of DoS Attack..... | 41 |
| Chapter 4: | Results and Discussions | 42 |
| 4.1 | USED METRICS | 42 |
| 4.1.1 | Performance Metrics | 42 |
| 4.1.2 | Level of Protection Metrics | 43 |
| 4.2 | EXPERIMENTAL RESULTS AND EVALUATIONS | 44 |
| 4.2.1 | Simulation Setup and Settings..... | 44 |
| 4.2.2 | Results and Discussions | 45 |
| 4.2.2.1 | Complexity Metric based Evaluation | 45 |
| 4.2.2.2 | Time gap metric based evaluation | 47 |
| 4.2.2.3 | Maturity metric based evaluation | 50 |
| 4.2.2.4 | Number of killed agents based evaluation..... | 53 |
| Chapter 5: | Conclusion and Future Work..... | 57 |
| 5.1 | CONCLUSION | 57 |
| 5.2 | LIMITATIONS OF THE CURRENT WORK..... | 58 |
| 5.3 | FUTURE WORK | 58 |
| References | | 59 |

| | |
|------------------------|----|
| Arabic Summary | 66 |
| Arabic Title Page..... | 67 |

List of Figures

| | |
|---|----|
| Figure 1.1 General Structure of Using VCSs | 2 |
| Figure 2.1 Interactions between VCS and other research field..... | 8 |
| Figure 2.2 Classification of security approaches for mobile agents | 11 |
| Figure 3.1 VCS general architecture..... | 20 |
| Figure 3.2 Multi-hop agent based protocol..... | 21 |
| Figure 3.3 the proposed agent-based protocol architecture..... | 23 |
| Figure 3.4 Granting certificates by traffic manager center | 24 |
| Figure 3.5 Scenario of executing a mission by an agent. | 25 |
| Figure 3.6 Multiple Colluded Attacks..... | 29 |
| Figure 3.7 attaching the public key of the HM with the mobile agent..... | 30 |
| Figure 3.8 Copying the OMA before executing the mission | 31 |
| Figure 3.9 encrypting the generated results by the public key of the HM | 32 |
| Figure 3.10 Denial of Service Attack..... | 33 |
| Figure 3.11 Defense against DoS attack..... | 34 |
| Figure 3.12 correct scenario against DoS attack..... | 35 |
| Figure 3.13 Defenses against DoS attack | 36 |
| Figure 3.14 Attacks and corresponding defenses summarization | 38 |
| Figure 3.15 Collaboration among the agent against DoS attack | 39 |
| Figure 3.16 collaboration among the agent against multiple colluded attack..... | 39 |
| Figure 4.1 Classification of used metrics | 42 |
| Figure 4.2 Number of total operations v.s. N value | 46 |
| Figure 4.3 TG v.s. number of detected DMs..... | 47 |
| Figure 4.4 Maturity metric based evaluation comparison | 50 |
| Figure 4.5 Other maturity metric based evaluations..... | 52 |
| Figure 4.6 Resistance against multiple colluded attack..... | 54 |
| Figure 4.7 Resistance against DoS attack. | 54 |

List of Tables

| | |
|---|----|
| Table 1.1 Security requirements terms. | 3 |
| Table 2.1 Drawbacks of the reviewed protocols..... | 16 |
| Table 3.1 Capabilities of attacker. | 18 |
| Table 3.2 Agents. | 22 |
| Table 4.1 Works for comparison. | 44 |
| Table 4.2 Simulation setting up. | 45 |
| Table 4.3 Time Gap values for MHABP protocol..... | 49 |
| Table 4.4 Scyther tool parameter settings..... | 50 |
| Table 4.5 Achieved security requirements based on scyther tool..... | 51 |
| Table 4.6 Achieved security requirements based on scyther tool (other protocols)...18 | |

List of Abbreviations

| Abbreviations | Explanations |
|---------------|---------------------------------|
| VCS | Vehicular Communication System. |
| MHABP | Multi Hop Based Protocol. |
| NoI | Number of Instructions. |
| IT | Information Technology. |
| IoT | Internet of Things. |
| RSUs | Roadside Units. |
| TMC | Traffic Manager Center. |
| HM | Home Machine. |
| DM | Destination Machine. |
| DoS | Denial of Services. |
| MHABP | Multi-Hop Agent Based Protocol. |
| PKI | Public Key Infrastructure. |
| VANET | vehicular ad-hoc network |
| P2P | (Peer-to-Peer) |