Contents

List of Figures ................................................................. vii
List of Tables ................................................................. ix
List of Algorithms ............................................................ x
Certificate ................................................................. xi
Acknowledgements ........................................................... xii
Abstract ................................................................. xiv

I Introduction 1

1.1 Background ............................................................. 2
  1.1.1 VANET Architecture .............................................. 3

1.2 Security of VANETs ..................................................... 5
  1.2.1 Challenges .......................................................... 7
  1.2.2 Adversaries and their Attacks ................................. 9
    Classes of Adversaries .............................................. 9
    Attacks in VANETs ................................................. 10
  1.2.3 VANET Security Requirements ............................... 14

1.3 VANET Security Mechanisms ......................................... 17
  1.3.1 Identity Based Cryptography .................................. 18
  1.3.2 Certificateless Cryptography .................................. 20
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Results Analysis</td>
<td>128</td>
</tr>
<tr>
<td>5.2 Conclusion</td>
<td>137</td>
</tr>
<tr>
<td>6 Effective Vehicular Communications</td>
<td>138</td>
</tr>
<tr>
<td>6.1 Fuzzy Based Trust Prediction Model</td>
<td>138</td>
</tr>
<tr>
<td>6.1.1 Proposed Fuzzy Based Trust Model</td>
<td>140</td>
</tr>
<tr>
<td>6.1.2 Final Trust Level</td>
<td>148</td>
</tr>
<tr>
<td>6.1.3 Simulation Results and Discussion</td>
<td>151</td>
</tr>
<tr>
<td>6.2 Misbehaviour Detection Module</td>
<td>154</td>
</tr>
<tr>
<td>6.3 V-Health Systems</td>
<td>156</td>
</tr>
<tr>
<td>6.3.1 Secure Communication Process</td>
<td>158</td>
</tr>
<tr>
<td>6.4 Conclusion</td>
<td>159</td>
</tr>
<tr>
<td>7 Conclusions and Future Scope</td>
<td>160</td>
</tr>
<tr>
<td>7.1 Conclusions</td>
<td>160</td>
</tr>
<tr>
<td>7.2 Future Scope</td>
<td>162</td>
</tr>
<tr>
<td>References</td>
<td>163</td>
</tr>
<tr>
<td>List of Publications</td>
<td>184</td>
</tr>
</tbody>
</table>
# List of Figures

1.1 The general communication scenario in VANETs ........................................ 3
1.2 VANET general architecture ........................................................................ 4
1.3 Jamming of signals ..................................................................................... 13
2.1 Overview of the literature for securing VANETs ........................................ 32
3.1 The various steps involved for registration and key generation of vehicle .... 80
4.1 Phases of vehicular communication ............................................................... 101
4.2 System model .............................................................................................. 103
4.3 Network design architecture ........................................................................ 104
4.4 Framework for message generation and verification process ...................... 116
4.5 Bloom filters $BF_1$ and $BF_2$ in vehicle .................................................. 118
4.6 Flowchart for message verification process ................................................ 122
5.1 Comparison of proposed protocol with related protocols ......................... 132
5.2 Packet delivery rate of proposed scheme with various error probabilities under urban scenario ................................................................. 133
5.3 Packet delivery rate of proposed scheme with various error probabilities under rural scenario ................................................................. 133
5.4 Network latency of proposed scheme with various error probabilities under urban scenario ........................................ 133

5.5 Network latency of proposed scheme with various error probabilities under rural scenario ........................................ 133

5.6 Computational delays of proposed scheme with various error probabilities under urban scenario ........................................ 134

5.7 Computational delays of proposed scheme with various error probabilities under rural scenario ........................................ 134

5.8 Average throughput of the simple aggregate scheme and proposed scheme ........................................ 134

5.9 Failure rate of the simple aggregate scheme and proposed scheme ........................................ 134

5.10 Network latency of the simple aggregate scheme and proposed scheme ........................................ 135

5.11 Computational delays of the simple aggregate scheme and proposed scheme ........................................ 135

5.12 Packet delivery rate of the simple aggregate scheme and proposed scheme ........................................ 136

5.13 Packet loss rate of the simple aggregate scheme and proposed scheme ........................................ 136

5.14 Normalized routing load of the simple aggregate scheme and proposed scheme ........................................ 136

5.15 Computational delays of RSU ........................................ 136

6.1 Network topology ........................................ 144

6.2 Fuzzy membership functions for the relaying trust value inputs and outputs ........................................ 145

6.3 Fuzzy membership functions for the final trust value inputs and outputs ........................................ 149

6.4 Trusted path distance vs. nodes ........................................ 152

6.5 Connectivity time vs. nodes ........................................ 153

6.6 Unreliable paths count vs. number of nodes ........................................ 153

6.7 Inconsistency vs. number of nodes ........................................ 153

6.8 Network efficiency vs. number of nodes ........................................ 153
## List of Tables

1.1 Comparison of security attacks in VANETs ............................................ 15
2.1 Comparison of public key infrastructures for VANETs ................................ 33
2.2 Comparison of the various symmetric key approaches ............................... 36
2.3 Comparison of proposed ID based frameworks ........................................ 43
2.4 Comparison of certificateless approaches in VANETs ................................ 45
2.5 Properties of existing trust models .......................................................... 53
2.6 Comparison of security approaches for VANETs based on distinctive characterisitics .......................................................... 54
2.6 Comparison of security approaches for VANETs based on distinctive characterisitics .......................................................... 55
2.6 Comparison of security approaches for VANETs based on distinctive characterisitics .......................................................... 56
2.6 Comparison of security approaches for VANETs based on distinctive characterisitics .......................................................... 57
2.6 Comparison of security approaches for VANETs based on distinctive characterisitics .......................................................... 58
2.6 Comparison of security approaches for VANETs based on distinctive characterisitics .......................................................... 59
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Properties of related security schemes</td>
<td>100</td>
</tr>
<tr>
<td>4.2</td>
<td>The various notations used in the proposed security scheme</td>
<td>105</td>
</tr>
<tr>
<td>4.3</td>
<td>Publicly known security parameters</td>
<td>106</td>
</tr>
<tr>
<td>4.4</td>
<td>Schematic of registration, key generation and pseudonym generation phases</td>
<td>111</td>
</tr>
<tr>
<td>5.1</td>
<td>Comparison of the proposed signature scheme with four other schemes</td>
<td>130</td>
</tr>
<tr>
<td>5.2</td>
<td>Error probability for three cases considered</td>
<td>130</td>
</tr>
<tr>
<td>5.3</td>
<td>$P_{ver}$ and $E_x$ for various cases and scenarios considered</td>
<td>130</td>
</tr>
<tr>
<td>5.4</td>
<td>Comparison of various security schemes</td>
<td>132</td>
</tr>
<tr>
<td>6.1</td>
<td>Comparison of existing trust based schemes with proposed scheme in VANETS</td>
<td>139</td>
</tr>
<tr>
<td>6.2</td>
<td>Rule base to calculate relaying trust value</td>
<td>146</td>
</tr>
<tr>
<td>6.3</td>
<td>Rule base to calculate final trust level</td>
<td>150</td>
</tr>
<tr>
<td>6.4</td>
<td>Simulation parameters for trust prediction model</td>
<td>151</td>
</tr>
</tbody>
</table>
# List of Algorithms

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Registration phase executed by vehicle</td>
<td>107</td>
</tr>
<tr>
<td>4.2</td>
<td>Registration of vehicle by RTA</td>
<td>107</td>
</tr>
<tr>
<td>4.3</td>
<td>Partial private key generation</td>
<td>108</td>
</tr>
<tr>
<td>4.4</td>
<td>To check suspicious vehicle</td>
<td>123</td>
</tr>
<tr>
<td>6.1</td>
<td>Algorithm for fuzzy based trust calculation</td>
<td>150</td>
</tr>
</tbody>
</table>
Certificate

I hereby certify that the work which is being presented in this thesis entitled "A Framework for Secure Vehicular Communication Systems", in partial fulfillment of the requirement for the award of degree of "Doctor of Philosophy" submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Shalini Batra and refers other research works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(Avleen Kaur Malhi)
Regn. No. 901203001

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Shalini Batra)
Assistant Professor
Computer Science & Engineering Department
Thapar University
Patiala, 147004
Punjab, INDIA.
Acknowledgements

I would like to express my sincere appreciation to my supervisor, Dr. Shalini Batra, for being a pillar of support and encouragement throughout my research work. Her experience, strength, tenderness and willfulness, has taught me valuable lessons of life, which are going to be of immense help to me in taking decisions in going forward.

My sincere thanks are due to Dr. Deepak Garg, Associate Professor and Head, Computer Science and Engineering Department (CSED), Thapar University, Patiala for providing me the necessary administrative assistance in completion of the work. I am thankful to my Ph.D. committee members, Dr. Neeraj Kumar, Associate Professor, Computer Science and Engineering Department, Dr. V P Singh, Assistant Professor, Computer Science and Engineering Department, and Dr. Mandeep Singh, Associate Professor, Electrical and Instrumentation Engineering, Thapar University, Patiala for their constructive comments and regularly ensuring the progress of my research work. I am thankful to all the faculty and staff members of CSED for their support.

I offer my deepest gratitude to my loving father, Dr. Sukhwinder Singh Malhi whose love and affectionate blessings have been a constant source of inspiration in making my vision a reality. I am also thankful to my mother Mrs. Berinder Kaur and my brother Dr. Anmol Malhi for their love, encouragement, motivation and their confidence in me.

I also acknowledge the cooperation and encouragement extended to me by my friends at Thapar University, especially Mr. Vishal Sharma and Ms. Divya Pandove.

The chain of gratitude would be definitely incomplete without thanking the Almighty,
the prime mover, for inspiring and guiding me (a humble being) to complete this task successfully.

Patiala
April, 2016

(Avleen Kaur Malhi)
Abstract

Vehicular ad-hoc networks have attracted comprehensive consideration in last few years for their assurance in enhancing driving safety and revolutionizing the transportation systems. Fundamentally, VANET security design should assure the security primitives of authentication, privacy, non-repudiation, integrity, availability, and in some peculiar application scenarios, confidentiality, to defend the network against intruders. Authentication ensures that a message is trustable by correctly identifying the sender of the message. The trust between vehicles is vital to efficiently transmit the data amongst vehicles. The new and attractive paradigm which eliminates the use of certificates in public key cryptography and solves the key escrow problem in identity based cryptography is certificateless cryptography.

A new certificateless aggregate signature scheme is proposed for VANETs with constant pairing computations. Assuming the hardness of computational diffie-hellman problem, the scheme is proved to be existentially unforgeable in the random oracle model against adaptive chosen-message attacks. A secure privacy preserving authentication framework is proposed which employs certificateless cryptography for authentication, pseudonyms for anonymous communication and multiple authorities are involved in revealing the identity of the vehicle in case of revocation. The signature verification scheme is improved by the use of bloom filters and the results achieved by the proposed scheme have been implemented on a simulated environment.

A fuzzy based trust prediction model is proposed to effectively compute the trust of other vehicles for the secure path formation in Vehicular Ad Hoc Networks (VANETs). The results and analysis of the proposed model over the standard protocols is presented using simulations.

A new misbehaviour detection scheme is proposed for the dissemination of correct information. The proposed countermeasures are proven to be efficient in detecting and blocking
the internal attackers from sharing the false warning messages. A new ubiquitous patient monitoring service called V-Health System is proposed to ensure the reliability of end to end communication between patients and healthcare services irrespective of time and location dependencies.