

ABSTRACT

A vehicular ad hoc Network (VANET) comprises the self managing ad hoc mobile vehicles. VANET is inherited from Mobile Ad hoc Network (MANET) for improving Intelligent Transport System (ITS) where vehicles act as mobile nodes. VANET framework is designed using three essential communicating units- Road Side Unit present at road segments, On Board Unit present in vehicle, and backend infrastructure for interconnectivity among vehicles and internet. Communication can be established in vehicle-to-road units, inter vehicle units, and road-to-road side units. The major concern while communication is related to security, considering confidentiality, integrity, authentication as the prime services to be offered to the vehicles. Therefore, each connecting vehicle in VANET has to prove its liability through authentication and can take the benefit of other security services afterwards.

In this era of expanding transport facilities for users, intelligent pathway coordination and communication is required among the vehicles. Therefore, the current research in VANET is focused on reducing traffic congestion in rush hours of a day, and accidents on the road. In case of occurrence of traffic congestion or road accident, vehicles on the move get stuck that calls for an effective way of choosing an alternate path and hence clear up the jammed traffic. Alternative path map consists of segments that are less occupied and can be followed in unusual situations.

Therefore, the prime objective foundation on which this research work revolves around is to (1) propose a new scheme for data collection which will tend to improve throughput, packet delivery ratio, and reduce latency, (2) extract the possible paths from the data collected using association rule base mining on distributed RSUs, and (3) predict the common and most frequent paths on the basis of position, direction, time of day, and during any accident or jam.

In order to generate efficient path maps in unusual situations like congestion or road accidents, the first step is to collect data from each vehicle about the path that it traverses to reach from one source to destination. Data collection is dependent on numerous factors such as position, direction, and time of the day. RSUs present on the

other side, hold the data collected from different moving vehicles from different source to destination respectively. Vehicles while moving send the data about the path segments that they are going to traverse to their nearest RSU. For each vehicle separate path information is maintained from a specific source to destination.

Different data collection scheme (DCS) are investigated by researcher that can be either RSU initiated or vehicle initiated. In RSU initiated scheme, a beacon message is initiated by the RSU after a fixed interval of time say N seconds to the vehicles present in its vicinity. In response, every vehicle sends a packet to the RSU with information related to the partial path. Road side unit (RSU) use road side probing in which they initiate the procedure of probing in order to enquire every vehicle in its vicinity about the information related to traffic, environmental, or accidents information. On the other side, in vehicle initiated scheme, vehicle starts transmission of path information to the RSU. Vehicle Initiated can be further classified as Vehicle Initiated-RSU find mode (VIR) and Vehicle Initiated-Broadcast mode (VIB).

In VIR, before the vehicle initiates the transmission of packet, it first generates a RSU find message and broadcast it. RSUs which are currently in the vicinity of the vehicle will receive this message but the one who is close to the vehicle replies through a message detailing its address information. VIR is again categorized into two schemes. One is VIR-Complete Path (VIR-CP), here vehicle first collects the information for complete path and then transmit the packet to the RSU. Second is, VIR- New Segment (VIR-NS), here whenever a vehicle receives information related to new path, it transmits the packet to a specific RSU.

In VIB, the transmission of packets is initiated in the broadcast mode through vehicle to all the RSUs that are in its vicinity. VIB scheme is again categorized in two schemes. One is, VIB-Complete Path (VIB-CP), here vehicle first collects the information for complete path, that is, it covers all the path segments first and after reaching the destination it transmits the packet to the RSU. Second is, VIB- New Segment (VIB-NS), here whenever a vehicle receives information related to new path, it transmits the packet.

From the aforementioned existing DCSs, VIB-CP (Vehicle Initiated Broadcast Complete Path) is the best one whose performance index is high in provisions of

communication overhead, average delay, and packet delivery ratio. But VIB-CP is still vulnerable to attacks, as an unauthenticated user can send the wrong data information to RSU. An attacker can also block the resources of RSU by sending unlimited messages. Various types of attacks are possible on VIB-CP that result in low evaluation of the VIB-CP based on communication overhead, packet delivery ratio and average delay. Therefore, improvement is required in VIB-CP as it didn't provide any security features.

With an aspiration to integrate security in existing DCS in VANET, an intelligent Authentication based Vehicle Initiated Broadcast Dynamic Path (IAVIB-DP) is proposed. In IAVIB-DP, Vehicle authentication is performed first on the RSU i.e. the authenticity of the vehicle is first proved at the RSU. A reciprocal security mechanism is required by the RSU to prove its authenticity to the vehicle in a view to support advance authentication mechanism. Once mutual authentication among RSU and vehicle is completed, vehicle may initiate communication with that RSU.

This work aims to implement and compare VIB-CP and proposed IAVIB-DP in OMNet++ to fetch the results in controlled environment set by user. OMNeT++ is an modular discrete event object-oriented network simulation framework that provides graphical user interface (GUI) for the simulation making it interactive system to work with. Moreover, it also provides mobility support in VANET. Communication overhead, Packet Delivery Ratio, and Latency is improved by using IAVIB-DP scheme while achieving authenticity of the vehicles.

Once the data is collected securely from proposed IAVIB-DP data DCS from different vehicles, data is stored at RSUs. Further, data mining is applied to extract all the possible paths considering one source and one destination. Association rule based mining is used to mine huge database to find common and frequent paths followed by different vehicles from one source to destination at distributed RSUs. Multiple paths may exist from a source to destination and this process is repeated for multiple source and destinations.

Minimum support and confidence are applied by setting threshold values that decide whether to accept or reject the pattern generated. This is required to accept the

arrangements for further decision making. A prediction model is designed that is able to decide the next path to choose in unusual situations like accident, jams, or a particular time of day. Therefore, this study comes out with a smart way of getting the best path map at particular time of day to avoid delay. For society, it reduces delay during unusual situations such as in event of accident, theft, morning rush hours, ambulance.

ACKNOWLEDGEMENT

I would like to present my deepest gratitude to **Dr. Babita Pandey nee Shukla** for her guidance, advice, understanding and supervision throughout the development of this thesis and study. I would like to thank to the **research project committee members** for their valuable comments and discussions. I would like to thank to **Lovely Professional University** for their support on academic studies and letting me involve in research study.

ARUN MALIK

TABLE OF CONTENTS

Chapter	Contents	Page No.
	<i>Declaration</i>	i
	<i>Certificate</i>	ii
	<i>Abstract</i>	iii-vi
	<i>Acknowledgement</i>	vii
	<i>Table of Contents</i>	viii-xii
	<i>List of Tables</i>	xiii-xiv
	<i>List of Figures</i>	xv-xvii
	<i>List of Abbreviations</i>	xviii-xix
CHAPTER 1	INTRODUCTION	1-39
	1.1 INTRODUCTION	1
	1.2 LITERATURE SURVEY	2
	1.2.1 SECURITY CONSIDERATIONS IN VANET	3
	1.2.2 AUTHENTICATION SCHEMES IN VANET	15
	1.2.3 DATA COLLECTION SCHEMES IN VANET	18
	1.2.4 DATA MINING TECHNIQUES IN VANET	22
	1.2.4.1 FORMING CLUSTERS	22
	1.2.4.2 ASSOCIATION BASED RULES	23
	1.2.4.3 CLASSIFICATION	24
	1.2.4.4 SEQUENTIAL MINING	25
	1.2.5 SALIENT FEATURES OF DATA MINING TECHNIQUES IN VANET	25
	1.2.6 LOGICAL BEHAVIORAL ARRANGEMENTS	26
	1.2.7 PATH MAP GENERATION IN VEHICULAR AD HOC NETWORK	30
	1.3 PROBLEM STATEMENT	31
	1.4 MOTIVATION	32
	1.5 RESEARCH OBJECTIVES	33
	1.6 RESEARCH METHODOLOGY	35
	1.7 RESEARCH ASSUMPTIONS	36
	1.8 MAJOR CONTRIBUTION OF THE THESIS	38
	1.8.1 CONCEPTUAL FOUNDATION	38
	1.8.2 EXPERIMENTAL ANALYSIS	38
	1.9 ORGANIZATION OF THE THESIS	38
CHAPTER 2	BASIC CONCEPTS	40-60
	2.1 INTRODUCTION	40
	2.2 APPLICATIONS OF VANET	42
	2.3 VANET ARCHITECTURE	45

2.4	VANET COMMUNICATION TYPES	49
2.5	CHARACTERISTICS OF VANET	50
2.6	REQUIREMENTS AND ATTACKS RELATED TO SECURITY AND PRIVACY FACED BY VANET	51
2.6.1	SECURITY REQUIREMENTS	51
2.6.2	ATTACKERS IN VANET	53
2.6.3	ATTACKS IN VANET	54
2.6.3.1	ATTACKS ON AVAILABILITY	55
2.6.3.2	ATTACKS ON AUTHENTICATION AND SECRECY	57
2.6.3.3	ATTACKS ON PRIVACY AND CONFIDENTIALITY	58
2.6.3.4	ATTACKS ON INTEGRITY AND RELIABLE DATA	59
2.6.3.5	ATTACKS ON LIABILITY AND NON-REPUDIATION	60
2.7	SUMMARY	60
CHAPTER 3	A NOVEL IDENTITY BASED TWO WAY AUTHENTICATION SCHEME IN VANET	61-75
3.1	INTRODUCTION	61
3.2	AUTHENTICATION PROCESS IN VANET	61
3.2.1	DIGITAL CERTIFICATES AUTHENTICATION	62
3.2.2	PAIRING	63
3.2.3	INTERMEDIARY RE-ENCRYPTION	64
3.3	COMPARISON OF EXISTING AUTHENTICATION PROCESSES	66
3.4	PROPOSED SCHEME FOR AUTHENTICATION	67
3.4.1	METHODOLOGY	67
3.4.2	ALGORITHMS FOR V2I AND INTER RSU AUTHENTICATION	69
3.5	PERFORMANCE EVALUATION OF PROPOSED SCHEME	70
3.5.1	COMPUTATIONAL OVERHEAD	71
3.5.2	LATENCY	72
3.5.3	PACKET DELIVERY RATIO	73
3.6	SUMMARY	75

CHAPTER 4	SECURITY ANALYSIS OF DISCRETE EVENT BASED THREAT DRIVEN AUTHENTICATION APPROACH IN VANET	76-90
4.1	INTRODUCTION	76
4.2	PROPOSED AUTHENTICATION APPROACH: METHODOLOGY	76
4.3	ALGORITHMS FOR ESTABLISHING MUTUAL AUTHENTICATION	78
4.3.1	ALGORITHM 1: AUTHENTICATION BETWEEN VEHICLE AND RSU	78
4.3.2	ALGORITHM 2: AUTHENTICATION BETWEEN VEHICLE VI AND VEHICLE VJ	79
4.4	PETRI NET MODEL FOR PROPOSED AUTHENTICATION APPROACH	80
4.5	SYSTEM MODEL	84
4.6	RESULTS AND DISCUSSIONS	84
4.7	SUMMARY	89
CHAPTER 5	PROPOSED INTELLIGENT AUTHENTICATION BASED VEHICLE INITIATED BROADCAST-DYNAMIC PATH DATA COLLECTION SCHEME IN VANET	91-115
5.1	INTRODUCTION	91
5.2	EXISTING DATA COLLECTION SCHEMES	91
5.2.1	RSU INITIATED	92
5.2.2	VEHICLE INITIATED-BROADCAST MODE	92
5.2.2.1	VIB-NEW SEGMENT	92
5.2.2.2	VIB-COMPLETE PATH	92
5.2.3	VEHICLE INITIATED-RSU FIND MODE	92
5.2.3.1	VIR- NEW SEGMENT	93
5.2.3.2	VIR-COMPLETE PATH	93
5.3	NETWORK SIMULATOR	93
5.4	SIMULATION PARAMETERS	95
5.5	VEHICULAR MOBILITY FRAMEWORK	96
5.6	PERFORMANCE METRICS FOR DATA COLLECTION SCHEMES	96
5.6.1	COMMUNICATION OVERHEAD	97

5.6.3	PACKET DELIVERY RATIO	97
5.6.3	LATENCY	97
5.6.4	PERFORMANCE INDEX	97
5.7	COMPARATIVE ANALYSIS OF EXISTING DATA COLLECTION SCHEMES	98
5.8	VIB-CP DATA COLLECTION SCHEME IN VANET	104
5.9	PROPOSED IAVIB-DP COLLECTION SCHEME IN VANET	105
5.10	PACKET FORMAT FOR IAVIB-DP	109
5.11	COMPARISON OF RBRA, INSA, VIB-CP AND PROPOSED IAVIB-DP SCHEME	111
5.11.1	COMMUNICATION OVERHEAD	111
5.11.2	PACKET DELIVERY RATIO	112
5.11.3	THROUGHPUT	113
5.11.4	LATENCY	114
5.12	SUMMARY	115
CHAPTER 6	AN ESTIMATION MODEL TO GENERATE PATH MAP FOR VEHICLES IN UNUSUAL ROAD INCIDENTS USING ASSOCIATION RULE BASED MINING IN VANET	116-129
6.1	INTRODUCTION	116
6.2	LOGICAL BEHAVIORAL ARRANGEMENTS FORMAL DEFINITIONS	118
6.3	DETERMINING THE COMMON AND MOST FREQUENT PATHS BY USING FREQUENT RRANGEMENT MINING APPROACH	121
6.3.1	SUPPORT	121
6.3.2	CONFIDENCE	126
6.4	SUMMARY	129
CHAPTER 7	PERFORMANCE COMPARISON OF PROPOSED SCHEME WITH EXISTING SOLUTIONS DURING AUTHENTICATION, DATA COLLECTION AND PATH MAP GENERATION	130-144

7.1	INTRODUCTION	130
7.2	SIMULATION TOOL	130
7.3	PERFORMANCE EVALUATION PARAMETERS	131
7.4	SIMULATION PARAMETERS	132
7.5	COMPARATIVE ANALYSIS OF PROPOSED AUTHENTICATION APPROACH WITH EXISTING APPROACHES	134
7.6	COMPARATIVE ANALYSIS OF PROPOSED DATA COLLECTION SCHEME WITH EXISTING SCHEMES	139
7.7	EVALUATING MINIMUM SUPPORT AND CONFIDENCE OF GENERATED PATH MAPS	142
7.8	SUMMARY	144
CHAPTER 8	CONCLUSION AND FUTURE WORK	145-147
8.1	CONTRIBUTION	145
8.2	FUTURE SCOPE	147
	LIST OF PUBLICATIONS	148-149
	REFERENCES	150-163

LIST OF TABLES

TABLE NO	DESCRIPTION	PAGE NO.
1.1	Security Solutions for Providing Security and Privacy in VANET	9-14
1.2	Summary Table for Existing Authentication Schemes	17-18
1.3	Summary Table for Existing Data Collection Schemes	21
1.4	Salient Features of Data Mining Techniques	26
1.5	Salient Features of Existing Logical Behavioral Arrangements	29-30
1.6	Research Assumptions	37
3.1	Comparison of Various Authentication Processes in VANET	66
3.2	Notation referred in Algorithm 1 and 2	69
3.3	Traffic Simulation Parameters for Authentication	70
3.4	Network Simulation Parameters for Authentication	70
3.5	Performance Comparison of Existing Authentication Schemes and Proposed Scheme	74
4.1	Description of Places	83
4.2	Description of Transition	83
4.3	Traffic Simulation Parameters	84
4.4	Network Simulation Parameters	84
4.5	Comparison of Computational Overhead Parameters for Different Authentication Approaches	85
5.1	General Simulation Parameters	95-96
5.2	Comparison of Modern Data Collection Methods in VANET	102
5.3	Performance Range Values for communication overhead, packet delivery ratio, latency, and PI.	103
5.4	Notations for algorithm 3 and algorithm 4	106-107
5.5	Comparison between IAVIB-DP and VIB-CP based on key features	109
6.1	Motion Database-1	120
6.2	Motion Database-2	122
6.3	Generating Candidate 1 arrangement sets (CMP(1)) after	123

Scanning Motion Database

6.4	Generating MP(1) by Comparing Minimum Support Count with Candidate1 Arrangement Sets Support Count	123
6.5	Generating Candidate 2 Arrangement Sets CMP(2) by Combining MP1 with itself	123
6.6	Generating MP(2) by Comparing Minimum Support Count with Candidate2 Arrangement Sets Support Count	124
6.7	Generating Candidate 3 Arrangement Sets CMP(3) by Combining MP2 with itself	124
6.8	Generating MP(3) by Comparing Minimum Support Count with Candidate 3 Arrangement Sets Support Count	124
7.1	Final Traffic Simulation Parameters	132
7.2	Final Network Simulation Parameters	133
7.3	Simulation Parameters for Data Collection	133-134

LIST OF FIGURES

FIGURE NO	DESCRIPTION	PAGE NO
1.1	Percentage of Research Papers for Each Communication Type	15
1.2	Data Collection Schemes in VANET	18
1.3	Area consisting of 4 RSUs and Moving Vehicles	32
1.4	Flowchart for Research Work	35
1.5	Working Model	36
2.1	VANET Spectrum	42
2.2	Post Accident Warning	44
2.3	VANET Architecture	46
2.4	Communication Between OBUs and RSU	48
2.5	RSU as an Information Source	48
2.6	Internet Access to Vehicles Provided by RSU	49
2.7	Type of Attackers	53
2.8	Classifications of Attacks in VANET	54
3.1	Process of Authentication in VANET	62
3.2	DCA Process for Authentication	63
3.3	Pairing Process for Authentication	64
3.4	IRE Process for Authentication	65
3.5	Proposed Scheme for Authentication	68
3.6	Simulation Environment	71
3.7	Comparison of Existing Authentication Schemes with Proposed Scheme in terms of Computational Overhead	71
3.8	Comparison of Existing Authentication Schemes with Proposed Scheme in terms of Latency	72
3.9	Comparison of Existing Authentication Schemes with Proposed Scheme in terms of Packet Delivery Ratio	73
4.1	Petri Net Model for Proposed Authentication Approach	81
4.2	Reachability Graph for Proposed Authentication Approach	82

4.3	Comparison of Computational Overhead for Proposed and Existing Authentication Approaches	86
4.4	Comparison of Throughput for Proposed and Existing Authentication Approaches	87
4.5	Comparison of Packet Delivery Ratio for Proposed and Existing Authentication Approaches	88
4.6	Comparison of Average Delay for Proposed and Existing Authentication Approaches	89
5.1	Modern Data Collection Schemes in VANET	92
5.2	RSU Scenario in OMNeT++	93
5.3	Scheduled Event at RSU	94
5.4	Sumo Framework	94
5.5	Moving Vehicles and Hit Event in SUMO	95
5.6	Data Collection Scenario at Single RSU	98
5.7	Readings from OMNeT++ Environment	99
5.8	Communication overhead with for different DCSs with varying number of vehicles	100
5.9	Packet delivery ratio for different DCSs with varying number of vehicles	100
5.10	Latency for different DCSs with varying number of vehicles	101
5.11	Performance Index for different DCSs with varying number of vehicles	102
5.12	Packet Format for IAVIB-DP	109
5.13	Communication Overhead with Different Moving Vehicles	111
5.14	Packet Delivery Ratio with Different Moving Vehicles	112
5.15	Throughput with Different Moving Vehicles	113
5.16	Latency with Different Moving Vehicles	114
6.1	Path Segments and Intersections	119
6.2	Number of Frequent Motion Arrangements Vs Thershold With Minimum Support	125
6.3	Segment Intersection Scenario	127

6.4	Confidence of Generated Associated Rules	128
7.1	Veins Framework	131
7.2	Comparison on basis of Computational Overhead	135
7.3	Comparison on basis of Throughput	136
7.4	Comparison on basis of Packet Delivery Ratio	137
7.5	Comparison on basis of Average Delay	138
7.6	Comparison of Data Collection Schemes on basis of Throughput	139
7.7	Comparison of Data Collection Schemes on basis of Latency	140
7.8	Comparison of Data Collection Schemes on basis of Packet Delivery Ratio	141
7.9	Comparison of Data Collection Schemes on basis of Communication overhead	142
7.10	Comparison of number of frequent arrangements with Minimum Support for different data collection schemes	143
7.11	Comparing Confidence of Generated Associated Rules for different data collection schemes	144

LIST OF ABBREVIATIONS

Abbreviation	Description
AP	Access Point
APt	Active Path Table
AU	Application Unit
CDT	Cell Dwell Time
CH	Cluster Head
CMP	Candidate Motion Arrangement
DCA	Digital Certificates Authentication
DCS	Data Collection Scheme
DoS	Denial of Service
DSRC	Dedicated Short Range Communication Standard
GPS	Global Positioning System
GUI	Graphical User Interface
HMM	Hidden Markov Model
IAVIB-DP	Intelligent Authentication Based Vehicle Initiated Broadcast-Dynamic Path
INSA	Intermediate Node Selection Algorithm
IRE	Intermediary Re-Encryption
ISP	Internet Service Providers
ITA	Intelligent Transport Application
ITS	Intelligent Transport Systems
IVC	Inter Vehicle Communication
LT	Lane Table
MANET	Mobile Ad-Hoc Network
MDS	Minimum Dominating Sets
MP	Motion Arrangement
OBU	On Board Unit
PI	Performance Index
PL	Path Lane
PPC	Position Based Prioritized Clustering
PST	Probabilistic Suffix Trees
PUF	Physical Unclonable Functions
RBRA	Receiver Based Routing Algorithm
RCP	Resource Command Processor
RI	RSU Initiated
RS	Road Segment
RSU	Road Side Unit
SP	Service Provider
TOA	Time of Arrival
V2I	Vehicle To Infrastructure Communication
V2R	Vehicle-To-Road Side Unit
V2V	Vehicle To Vehicle Communication
VANET	Vehicular Ad-Hoc Network
VARM	VANET Association Rules Mining
VEINS	Vehicle In Network Simulation

VIB	Vehicle Initiated-Broadcast Mode
VIB-CP	Vehicle Initiated-Broadcast-Complete Path
VIB-NS	Vehicle Initiated-Broadcast-New Segment
VII	Vehicle Infrastructure Integration
VIR	Vehicle Initiated-RSU Find Mode
VIR-CP	Vehicle Initiated-RSU -Complete Path
VIR-NS	Vehicle Initiated-RSU - New Segment
WAVE	Wireless Access In Vehicle Environment