ENHANCED SECURITY FRAMEWORK FOR GRAY-HOLE ATTACK PREVENTION IN VEHICULAR NETWORKS

A PROJECT REPORT

Submitted by

KARVENDAN P	**(927621BEC077)**
KAVINESH A S	**(927621BEC081)**
KISHORE K	**(927621BEC094)**
MIDHUN R	**(927621BEC120)**

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

M.KUMARASAMY COLLEGE OF ENGINEERING, KARUR

ANNA UNIVERSITY: CHENNAI 600 025

APRIL 2025

M.KUMARASAMY COLLEGE OF ENGINEERING, KARUR

BONAFIDE CERTIFICATE

Certified that this project report **" ENHANCED SECURITY FRAMEWORK FOR GRAY-HOLE ATTACK PREVENTION IN VEHICULAR NETWORKS"** is the Bonafide work of "**KARVENDAN P (927621BEC077), KAVINESH A S(927621BEC081), KISHORE K (927621BEC094), MIDHUN R (927621BEC120)**" who carried out the project work under my supervision in the academic year 2024-2025.

SIGNATURE
Dr. A. KAVITHA, M.E., Ph.D.,
HEAD OF THE DEPARTMENT
Professor,
Department of Electronics and Communication Engineering,
M.Kumarasamy College of Engineering,
Thalavapalayam, Karur-639113

SIGNATURE
Dr. S. VIMALNATH, M.E., Ph.D.,
SUPERVISOR
Associate Professor**,**
Department of Electronics and Communication Engineering,
M.Kumarasamy College of Engineering,
Thalavapalayam, Karur-639113

This project report has been submitted for the **18ECP107L - Project Work** Viva Voce Examination held at M. Kumarasamy College of Engineering, Karur on _____.

INTERNAL EXAMINER **EXTERNAL EXAMINER**

INSTITUTION VISION AND MISSION

Vision

To emerge as a leader among the top institutions in the field of technical education.

Mission

M1: Produce smart technocrats with empirical knowledge who can surmount the global challenges.

M2: Create a diverse, fully -engaged, learner -centric campus environment to provide quality education to the students.

M3: Maintain mutually beneficial partnerships with our alumni, industry and professional associations

DEPARTMENT VISION, MISSION

Vision

To empower the Electronics and Communication Engineering students with emerging technologies, professionalism, innovative research and social responsibility.

Mission

M1: Attain the academic excellence through innovative teaching learning process, research areas & laboratories and Consultancy projects.

M2: Inculcate the students in problem solving and lifelong learning ability.

M3: Provide entrepreneurial skills and leadership qualities.

M4: Render the technical knowledge and skills of faculty members.

DEPARTMENT PEO, PO AND PSO

Program Educational Objectives

PEO1: Core Competence: Graduates will have a successful career in academia or industry associated with Electronics and Communication Engineering

PEO2: Professionalism: Graduates will provide feasible solutions for the challenging problems through comprehensive research and innovation in the allied areas of Electronics and Communication Engineering.

PEO3: Lifelong Learning: Graduates will contribute to the social needs through lifelong learning, practicing professional ethics and leadership quality.

Program Outcomes

PO 1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO 2: Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO 3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO 4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO 5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO 6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO 7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO 8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO 9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO 10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO 11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO 12: Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Specific Outcomes

PSO1: Applying knowledge in various areas, like Electronics, Communications, Signal processing, VLSI, Embedded systems etc., in the design and implementation of Engineering application.

PSO2: Able to solve complex problems in Electronics and Communication Engineering with analytical and managerial skills either independently or in team using latest hardware and software tools to fulfil the industrial expectations.

Abstract	Matching with POs, PSOs
VANET, AODV, Routing Protocol, DPGHA	PO1, PO2, PO6, PO7, PO9, PO12, PSO1, PSO2

S.No.	Project Domain	Mapping with POs/PSOs
1.	Cloud Computing	PO1, PO2, PO3, PO4,PO5, PO6,PO8,PO9,PO10,PO11, PO12, PSO1, PSO2
2.	Wireless Communication and Networks	PO1, PO2, PO3,PO4,PO5,PO8, PO9, PO10,PO11, PO12, PSO1, PSO2

ACKNOWLEDGEMENT

We gratefully remember our beloved **Founder Chairman, (Late) Thiru M. Kumarasamy**, whose vision and legacy laid the foundation for our education and inspired us to successfully complete this project.

We extend our sincere thanks to **Dr. K. Ramakrishnan, Chairman**, and **Mr. K. R. Charun Kumar, Joint Secretary**, for providing excellent infrastructure and continuous support throughout our academic journey.

We are privileged to extend our heartfelt thanks to our respected Principal, **Dr. B. S. Murugan, B.Tech., M.Tech., Ph.D.,** for providing us with a conducive environment and constant encouragement to pursue this project work.

We sincerely thank **Dr. A. Kavitha, B.E., M.E., Ph.D.,** Professor and **Head, Department of Electronics and Communication Engineering**, for her continuous support, valuable guidance, and motivation throughout the course of this project.

Our special thanks and deep sense of appreciation go to our **Project Supervisor, Dr. S. Vimalnath, B.E., M.E., Ph.D.,** Associate Professor, **Department of Electronics and Communication Engineering,** for his exceptional guidance, continuous supervision, constructive suggestions, and unwavering support, all of which have been instrumental in the successful execution of this project.

We would also like to acknowledge **Dr. S. Vimalnath, B.E., M.E., Ph.D., Associate Professor, our Class Advisor,** and **Dr. S. Vimalnath, B.E., M.E., Ph.D.**, the **Project Coordinator**, for their constant encouragement and coordination that contributed to the smooth progress and completion of our project work.

We gratefully thank all the **faculty members of the Department of Electronics and Communication Engineering** for their timely assistance, valuable insights, and constant support during various phases of the project.

Finally, we extend our profound gratitude to our **parents and friends** for their encouragement, moral support, and motivation, without which the successful completion of this project would not have been possible.

ABSTRACT

This research proposes an innovative and efficient approach for the detection and prevention of Gray-Hole attacks in Vehicular Ad Hoc Networks (VANETs). Gray-Hole attacks pose a significant threat to the reliability and security of VANETs by selectively dropping or modifying network packets. Our approach employs a combination of anomaly detection techniques and dynamic trust management to identify suspicious nodes exhibiting abnormal behavior indicative of Gray-Hole attacks. Upon detection, a proactive prevention mechanism is triggered to isolate and mitigate the impact of compromised nodes. The proposed solution is implemented in Network Simulator 2 (NS-2) using Tcl programming language, demonstrating its feasibility and effectiveness in enhancing the resilience of VANETs against Gray-Hole attacks. The results showcase improved network performance and security, making our approach a valuable contribution to the field of VANET security.

Keywords: VANET, AODV, Routing Protocol, DPGHA.

TABLE OF CONTENTS

CHAPTER No.	CONTENTS		PAGE No.
	INSTITUTION VISION AND MISSION		**iii**
	DEPARTMENT VISION AND MISSION		**iii**
	DEPARTMENT PEOS, POS AND PSOS		**iv**
	ABSTRACT		**ix**
	LIST OF TABLES		**xiv**
	LIST OF FIGURES		**xv**
	LIST OF ABBREVIATIONS		**xvii**
1	**INTRODUCTION**		**1**
	1.1	Overview Of Cut Detection in Wireless Sensor Networks	1
	1.2	Introduction To Wireless Sensor Networks	2
2	**LITERATURE SURVEY**		**10**
	2.1	Scalable And Distributed Detection Analysis on Wormhole Links	10
	2.2	Wireless body area networks MAC protocol for energy efficiency	10
	2.3	An energy efficient routing protocol using Omnet CC for Wireless Sensor Network.	10
	2.4	Improved LEACH protocol with cache nodes to increase lifetime of wireless sensor network.	11
	2.5	Extensive usage of wireless sensor network (WSN) is the reason of development of many routing protocols.	11
	2.6	Evolving a Hybrid K-Means Clustering Algorithm for Wireless Sensor Network Using PSO and Gas	12
	2.7	Minimization of Average Energy Consumption to Prolong Lifetime of	12

Wireless Sensor Network

3	**EXISTING SYSTEM`**	**14**
	3.1 Existing Technique	14
	3.2 Objective	14
4	**PROPOSED SYSTEM**	**16**
	4.1 Proposed Technique	18
	4.2 Application	18
	4.3 Dynamic Trust and Reputation System	19
	4.4 Ids With Anomaly Detection	19
	4.5 Advanced Secure Routing Protocol (Aodv / Dsr)	20
	4.6 Collaborative Detection Mechanism	21
	4.7 Adaptive Detection with Machine Learning	22
	4.8 Low Overhead Multi-Path Routing	22
5	**METHODOLOGY**	**23**
	5.1 Module Explanations	23
	5.2 Flow Chart	27
6	**SOFTWARE REQUIRMENTS**	**28**
	6.1 Implementation Tools	28
	6.2 Discrete Event Simulator	29
	6.3 NS2 Features	30
	6.3.1 Platform To Run Ns2	31
	6.3.2 Ns Programming Structure	31
	6.3.3 Event Schedular	31

	6.4	Trace Analysis	31
		6.4.1 Create Network Topology	32
	6.5	Transport Connection	32
	6.6	Generate Traffic (Application Layer)	33
	6.7	Network Animator (Nam)	33
7	**SIMULATION&LANGUAGE SPECIFICATION**		**35**
	7.1	Introduction	35
	7.2	Motivation For Simulation	35
	7.3	Ns Features	36
		7.3.1 Ns Programming Structures	36
		7.3.2 Event Scheduler	36
	7.4	Packets	36
	7.5	Turn on Tracing	37
	7.6	Creating Network Topology (Physical Layer)	37
	7.7	Transport Connection (Transport Layer)	38
	7.8	Generate Traffic (Application Layer)	38
		7.8.1 Motivation For Simulations	39
	7.9	Model Output	39
		7.9.1 Network Animator	39
	7.10	NS Features	41
8	**SOFTWARE INSTALLATION**		**42**
	8.1	Installation Of Ns2	42

	8.2 System Modelling	45
	8.3 Analytical Approach	45
	8.4 Simulation Approach	46
9	**RESULTS AND DISCUSSION**	**48**
	9.1 Performance Evaluation	48
	9.2 Result	50
	9.2.1 Simulation Result	50
	9.2.2 Throughput	58
	9.2.3 Delay	59
	9.2.4 Pocket Delivery Factor	60
10	**CONCLUSION AND FUTURE WORK**	**61**
	10.1 Conclusion	61
	10.2 Future Enhancements	62
	APPENDICES	**65**
	REFERENCES	**77**

LIST OF TABLES

TABLE No.	TITLE	PAGE No.
1.1	Vanets Simulation Parameter	21

LIST OF FIGURES

FIGURE No.	TITLE	PAGE No.
1.1	Basic Building Blocks of Sensor Node	4
1.2	Functionality of a Sensor Node	5
1.3	Block Diagram for Proposed System	16
1.4	Process Diagram 1	17
1.5	Process Diagram 2	17
1.6	Topology Formation	25
1.7	Repair points	26
1.8	Flow Chart for Proposed System	27
1.9	Basic NS2 architecture	35
1.10	Stack Register of Packet	37
1.11	Trace of a packet	37
1.12	Simulated output of NAM	40
1.13	Tracing	40
1.14	Xgraph for simulated output	41
1.15	Packet Arrival event	46
1.16	Successful Packet Transmission	47

1.17	Comparison of throughput	49
1.18	End To End Delay	50
1.19	Simulation Result On Ns2 Tool 1	50
1.20	Simulation Result On Ns2 Tool 2	51
1.21	Simulation Result On Ns2 Tool 3	52
1.22	Node Creation	53
1.23	Gray Hole Attackers Present	54
1.24	Detection Gray Hole Attacker	55
1.25	Proper Gray Whole Detection and Avoidance	56
1.26	Data Communication	57
1.27	Throughput	58
1.28	Delay	59
1.29	Pocket Delivery Factor	60

LIST OF ABBREVIATIONS

ACRONYM		ABBREVIATION
WSN	-	Wireless Sensor Networks
DSSD	-	Distributed Source Separation Detection
BS	-	Base Station
WSAN	-	Wireless Sensor and Actuator Networks
ADC	-	Analog To Digital Converter
MAC	-	Medium Access Control
LEACH	-	Low-Energy Adaptive Clustering Hierarchy
VANET	-	Vehicular Ad Hoc Networks
MCRP	-	Magnetic Resonance Cholangiopancreatography
IDS	-	Intrusion Detection System
AODV	-	Ad-Hoc On-Demand Distance Vector
DSR	-	Dynamic Source Routing
ML	-	Machine Learning
CSMA	-	Carrier Sense Multiple Access
TCH	-	Target Cluster Head
TDMA	-	Time Division Multiple Access
RSS	-	Received Signal Strengths
RP	-	Repair Points
OTCL	-	Object-Oriented Tcl
UDP	-	User Datagram Suite
NAM	-	Network Animator
GHA	-	Gray-Hole Attack

PDR	-	Packet Delivery Ratio
ITS	-	Intelligent Transportation Systems
CNN	-	Convolutional Neural Networks
LSTM	-	Long Short-Term Memory
SDN	-	Software-Defined Networking
IOV	-	Internet Of Vehicles

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF CUT DETECTION IN WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSN), composed of numerous sensor nodes with small, low-power, inexpensive radios, have attracted a large amount of research that has led to interesting and innovative applications. However, challenging problems still exist. One of the most challenging problems in WSN is maintaining network connectivity to reliably deliver data to a specified point, or sink, in an energy-efficient manner. Disrupted connectivity, known as a “cut”, can lead to skewed data, ill-informed decisions and even entire network outages. It can also lead to memory and power exhaustion in disconnected nodes and network congestion in disconnected segments.

Such data loss and wasted resources can be avoided if a node can independently determine if a cut exists in the network. Cut detection algorithms attempt to recognize and locate cuts. Using a state-based convergence mechanism, the current state-of-the-art cut detection algorithm, Distributed Source Separation Detection (DSSD), reliably detects arbitrarily-shaped cuts and allows individual nodes to perform cut detection autonomously. However, the algorithm suffers from a number of problems. First, DSSD fails to address security, a critical component of sensor deployments in unattended environments. Second, the algorithm requires a lengthy, iterative convergence process. Finally, all nodes participate in the frequent broadcasts required to achieve convergence.

This is cost-prohibitive with regards to power, especially in denser networks. In light of these problems, we propose an algorithm with two principal components. Outlier detection, a statistical data analysis technique, resolves the security threat where a malicious node injects erroneous data into the cut

detection process. Using data analysis, outlier detection identifies malicious source data and provides a light-weight, energy-efficient mechanism to validate neighbor data. Additionally, we propose an improved cut detection algorithm called robust cluster-based cut detection. This algorithm divides the network into a set of location-based clusters. Cluster leaders form a virtual grid network and the cut detection algorithm runs on this high-level network. As the algorithm executes, leaders converge to some state. A leader finding inconsistency in its expected state informs its neighbors and the sink that a cut has happened.

1.2 INTRODUCTION TO WIRELESS SENSOR NETWORKS

Wireless Sensor Networks consists of a large number of low costs, low-power, low maintenance sensor nodes. Sensor nodes usually consist of sensing, communicating, computing, storing and power components. The sensor nodes are capable of storing data sensed from the environment according to their specific application, collaborating and computing the data to perform some specific tasks and communicating those data to the higher level or the base station (BS) for decision making. BSs have enhanced capabilities over simple sensor nodes and can-do complex data processing. Sensor nodes are often randomly deployed in huge numbers over a large area to monitor physical conditions like temperature, humidity, intensity, vibration, pressure, motion, pollutants etc.

They are also deployed in military battlefield to track enemy movements. Based on the characteristics,

Wireless Sensor Networks has following main features:

a) Because of the limited energy supply for the wireless nodes, the wireless links between nodes in the Sensor Network are quite inconsistent for the communication participants.

b) Due to high memory and energy constraint, sensor nodes have restricted computational capacity and communication bandwidth.

c) They may remain unattended in hostile environment. Due to this, the major feature concerning WSN is energy efficient routing.

To offer energy efficient routing, one of the challenges is to ensure that the network is connected. The connectivity of the network can easily be disrupted due to unpredictable wireless channels, early depletion of node's energy, and physical tampering by hostile users. Network disconnection, typically referred as a network cut, may cause a number of problems. For example, ill-informed decisions to route data to a node located in a disconnected segment of the network might lead to data loss, wasted power consumption, and congestion around the network cut.

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The

topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Wireless sensor nodes are equipped with sensing unit, a processing unit, communication unit and power unit. Each and every node is capable to perform data gathering, sensing, processing and communicating with other nodes. The sensing unit senses the environment, the processing unit computes the confined permutations of the sensed data, and the communication unit performs exchange of processed information among neighboring sensor nodes.

The basic building block of a sensor node is shown

Fig 1.1 Basic Building Blocks of Sensor Node

The sensing unit of sensor nodes integrates different types of sensors like thermal sensors, magnetic sensors, vibration sensors, chemical sensors, bio sensors, and light sensors. The measured parameters from the external environment by sensing unit of sensor node are fed into the processing unit. The analog signal generated by the sensors are digitized by using Analog to Digital converter (ADC) and sent to controller for further processing. The processing unit is the important core unit of the sensor node. The processor executes different tasks and controls the functionality of other components.

The required services for the processing unit are pre-programmed and loaded into the processor of sensor nodes. The energy utilization rate of the processor varies depending upon the functionality of the nodes. The variation in the performance of the processor is identified by the evaluating factors like processing speed, data rate, memory and peripherals supported by the processors. Mostly ATMEGA 16, ATMEGA 128L, MSP 430 controllers are used in commercial motes. The computations are performed in the processing unit and the acquired result is transmitted to the base station through the communication unit. In communication unit, a common transceiver act as a communication unit and it is mainly used to transmit and receive the information among the nodes and base station and vice versa. There are four states in the communication unit: transmit, receive, idle and sleep.

Fig 1.2 Functionality of a Sensor Node

The major characteristics of the sensor node used to evaluate the performance of WSN.

1. Fault tolerance

Each node in the network is prone to unanticipated failure. Fault tolerance is the capability to maintain sensor network functionalities without any break due to sensor node failures.

2. Mobility of nodes

In order to increase the communication efficiency, the nodes can move anywhere within the sensor field based on the type of applications.

3. Dynamic network topology

Connection between sensor nodes follows some standard topology. The WSN should have the capability to work in the dynamic topology.

4. Communication failures

If any node in the WSN fails to exchange data with other nodes, it should be informed without delay to the base station or gateway node.

5. Heterogeneity of nodes

The sensor nodes deployed in the WSN may be of various types and need to work in a cooperative fashion.

6. Scalability

The number of sensor nodes in a sensor network can be in the order of hundreds or even thousands. Hence, WSN designed for sensor networks is supposed to be highly scalable.

7. Independency

The WSN should have the capability to work without any central control point.

8. Programmability

The option for reprogramming or reconfiguring should be available for the WSN to become adaptive for any dynamic changes in the network.

9. Utilization of sensors

The sensors should be utilized in a way that produces the maximum performance with less energy.

10. Impracticality of public key cryptosystems

The limited computation and power resources of sensor nodes often make it undesirable to use public key algorithms.

11. Lack of a prior knowledge of post-deployment configuration

If a sensor network is deployed via random distribution, the protocols will not be aware of the communication status between each node after deployment.

The following metrics are used to evaluate the performance of a WSN:

- Network coverage,
- Node coverage,
- Efficiency in terms of system lifetime,
- Effortless deployment,
- Data accuracy,
- System response time,
- Fault tolerance,
- Scalability,
- Network throughput,
- Sample rate,
- Security,
- The cost of the network and
- Network architecture used.

The individual sensor node in the WSN is evaluated using flexibility, robustness, computation, communication, security, synchronization, node size and cost.

The components of WSN system are sensor node, rely node, actor node, cluster head, gateway and base station which are explained below.

Sensor node

Capable of executing data processing, data gathering and communicating with additional associated nodes in the network. A distinctive sensor node

capability is about 4-8 MHz, having 4 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency.

Relay node

It is a midway node used to communicate with the adjacent node. It is used to enhance the network reliability. A rely node is a special type of field device that does not have process sensor or control equipment and as such does not interface with the 7 process itself. A distinctive rely node processor speed is about 8 MHz, having 8 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency. Actor node: It is a high-end node used to perform and construct a decision depending upon the application requirements. Typically, these nodes are resource rich devices which are outfitted with high quality processing capabilities, greater transmission powers and greater battery life.

A distinctive actor node processor capability is about 8 MHz, having 16 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency. Cluster head: It is a high bandwidth sensing node used to perform data fusion and data aggregation functions in WSN. Based on the system requirements and applications, there will be more than one cluster head inside the cluster. A distinctive cluster head processor is about 4-8 MHz, having 512 KB of RAM, 4 MB flash and preferably 2.4 GHz of radio frequency. This node assumed to be highly reliable, secure and is trusted by all the nodes in the sensor network.

Gateway

Gateway is an interface between sensor networks and outside networks. Compared with the sensor node and cluster head the gateway node is most powerful in terms of program and data memory, the processor used, transceiver range and the possibility of expansion through external memory. A distinctive gateway processor speed is about 16 MHz, having 512 KB of RAM, 32 MB flash and preferably 2.4 GHz of radio frequency.

Base station

It is an extraordinary type of nodes having high computational energy and processing capability. 8 Attractive functionality of sensor nodes in a WSN includes effortlessness installation, fault indication, energy level diagnosis, highly reliability, easy coordination with other nodes in the network, control protocols and simple network interfaces with other smart devices. In WSN, based on the sensing range and environment, the sensor nodes are classified into four groups, namely specialized sensing node, generic sensing node, high bandwidth sensing node and gateway node. The radio bandwidth for the sensor nodes is <50 Kbps, <100 Kbps, ≈500 Kbps and >500 Kbps respectively.

On board processing, computational rate and communication ranges differ from node to node in WSN. Particularly for some dedicated application sensor nodes with different capabilities are used. For example, smart specialized sensing nodes are preferred for special purpose devices, intelligent generic sensing node preferred for generic functions. For interconnectivity functions high end smart bandwidth sensing node and gateway nodes are preferred.

CHAPTER 2

LITERATURE REVIEW

2.1 Scalable and distributed detection analysis on wormhole

Padmanabhan and V. Manickavasagam. In this paper, a scalable and distributed scheme which uses sequential probability ratio test is proposed, to avoid single point failures and to handle high mobility, with no additional resource requirements. It is observed that wormholes are detected using few packets and detection is faster with increasing mobility. The system is highly customizable as system parameters can be chosen to balance the speed and accuracy of detection. System overheads in terms of communication, computation, and storage aspects are analyzed and presented.

2.2 Wireless body area networks MAC protocol for energy efficiency

We design a novel medium access control (MAC) layer protocol to enhance the energy efficiency and extend the lifetime of body sensor nodes in WBANs. The proposed protocol utilizes a hybrid scheme by taking advantage of carrier-sense multiple accesses with the collision avoidance and time division multiple access schemes. In addition, we allocate the main transmission overhead at the personal station side and design a novel awaiting order state for sensor nodes to improve energy efficiency.

2.3 An energy efficient routing protocol using Omnet CC for Wireless Sensor Network.

We propose a novel modified routing protocol in this paper. The newly proposed improved energy-efficient LEACH (IEE-LEACH) protocol considers the residual node energy and the average energy of the networks. To achieve satisfactory performance in terms of reducing the sensor energy consumption, the proposed IEE-LEACH accounts for the numbers of the optimal CHs and prohibits the nodes that are closer to the base station (BS) to join in the cluster formation.

Furthermore, the proposed IEE-LEACH uses a new threshold for electing CHs among the sensor nodes, and employs single hop, multi-hop, and hybrid communications to further improve the energy efficiency of the networks.

2.4 Improved LEACH protocol with cache nodes to increase lifetime of wireless sensor network.

In this research paper, the Improved LEACH protocol is further improved by deploying cache nodes in the network. In the Improved LEACH protocol with cache nodes, the cluster head are selected on the basis of distance and energy. The cluster heads transmit data to cache node which is nearest and has minimum access time. The simulation of proposed modal is done in MATLAB. To validate the results of Improved LEACH protocol is compared with Improved LEACH protocol with cache node.

2.5 Extensive usage of wireless sensor network (WSN) is the reason of development of many routing protocols.

Recent advances in WSN now witness the increased interest in the potential use in applications like Military, Environmental, Health (Scanning), Space Exploration, Vehicular Movement, Mechanical stress levels on attached objects, disaster management, combat field reconnaissance etc. Sensors are expected to be remotely deployed in unattended environments. Routing as one key technologies of wireless sensor network has now become hot research because the applications of WSN is everywhere, it is impossible that there is a routing protocol suitable for all applications. In this paper, the various routing protocol are classified and described. The growing interest in WSN and the continual emergence of new architectural techniques inspired surveying the characteristics, applications and communication protocols for such a technical area.

2.6 Evolving a Hybrid K-Means Clustering Algorithm for Wireless Sensor Network Using PSO and Gas.

Wireless Sensor Networks (WSN) became an essential component in many real-life applications such as military, smart energy, commercial, health and many others. However, WSN still suffer many problems related to energy consumption. Clustering found to be an effective technique to solve the energy consumption problem for WSN by avoiding long distance communication. In this paper, we explore our initial idea on developing a hybrid clustering algorithm which has two folds 1) Use the K-Means unsupervised learning algorithms to select the sensors belonging to each cluster using an arbitrary number of clusters 2) Use Particle Swarm Optimization (PSO) and Genetic Algorithms (GAs) separately to select the best CHs. We name these two algorithms as KPSO and KGAs. The developed hybrid algorithms are tested over number of experiments with various layouts. KPSO provided better results compared to the KGAs.

2.7 Minimization of Average Energy Consumption to Prolong Lifetime of Wireless Sensor Network.

Wireless Sensor Network (WSN) is a network of sensor nodes that can sense the environment and send the information through wireless links to a sink. Wireless sensor nodes possess limited processing capability, storage and energy resources. The existence of sensor network depends on the life of sensor nodes i.e. ultimately on the energy consumption during its operation. Thus, in WSN, the efficient use of energy resources is very much necessary. Clustering is one of the approaches for energy saving in WSN. A cluster is a group of sensor nodes with one central entity named Cluster Head (CH). In this article, a new way of clustering for CH selection and cluster formation in WSNs is proposed; in which sensor network is divided into zones as per geographic locations of nodes. Clusters are formed within the zones by taking into account the residual energy of nodes and node distance. All cluster members send the sensed data to their respective CH. Hence, CH consumes more energy as it processes the collected

data before forwarding it to Base Station (BS). Dropping of cluster head's residual energy below threshold value initiates cluster reformation. Performance analysis and simulation results are given with variations in number of nodes and transmission range. The obtained results show good performance of our algorithm in terms of reduced energy consumption, increased network lifetime and scalability of the network.

CHAPTER 3

EXISTING SYSTEM

In the current landscape of Vehicular Ad Hoc Networks (VANETs), security remains a critical concern due to the susceptibility to various attacks, including the Gray-Hole threat. Existing systems often rely on conventional security mechanisms, such as encryption and authentication, to safeguard communication channels. These methods may fall short in detecting and preventing sophisticated attacks like Gray-Hole, which involve nodes selectively manipulating or dropping packets without overtly violating encryption or authentication protocols. Traditional approaches may lack the adaptability required to address the dynamic nature of VANETs, where nodes frequently join or leave the network. There is a pressing need for an advanced system that goes beyond conventional security measures and provides a comprehensive solution to identify and mitigate Gray-Hole attacks effectively in VANETs.

3.1 EXISTING TECHNIQUE:

- Low-Energy Adaptive Clustering Hierarchy (LEACH)

Disadvantage:

- Less Security
- Low Throughput
- More Losses

3.2 OBJECTIVE:

The primary objective of this research is to develop a robust solution for the detection and prevention of Gray-Hole attacks in Vehicular Ad Hoc Networks (VANETs). Gray-Hole attacks pose a severe threat to the integrity of communication in VANETs by selectively manipulating or dropping data packets. This research aims to enhance the security and reliability of VANETs by employing innovative anomaly detection techniques and dynamic trust

management mechanisms. The ultimate goal is to provide an efficient and effective means of identifying and mitigating Gray-Hole attacks in real-time, thereby safeguarding the communication infrastructure of vehicular networks.

CHAPTER 4

PROPOSED SYSTEM

Our proposed algorithm uses an end-to-end time delay between sensor nodes and the BS to pin point links that are potentially under wormhole attacks and in turn be avoided in the shortest path. We will specify some assumptions in our sensor network. Then, we propose the concept of Time Ratio Threshold to detect wormhole links in the network. The foundation of MCRP is based on a single BS, which is a high-energy node with an unlimited amount of energy supply. Thus, MCRP employs the BS to facilitate network management to improve the performance of establishing a routing path from the source nodes to the sink.

BLOCK DIAGRAM:

Fig 1.3 Block Diagram for Proposed System

PROCESS DIAGRAM 1:

Fig 1.4 Process Diagram 1

PROGRESS DIAGRAM 2:

Fig 1.5 Process Diagram 2

4.1 PROPOSED TECHNIQUE:

- Detection and Prevention of GHA'' (DPGHA)

PROPOSED SYSTEM ADVANTAGES:

Improves the network scalability in terms of

- Energy consumption
- End-to-end delay
- Throughput
- Frame Delivery Ratio

4.2 APLLICATIONS:

WSN has wide application possibilities, such as

- temperature, pressure, humidity, and habitat monitoring
- disaster management
- Military reconnaissance
- forest re-tracking
- Building automation
- Security surveillance

An integrated system combining multiple technologies and strategies is proposed for enhancing the safety of VANETs against Gray-Hole attacks. We will combine IDS, Reputation Management, Secure Routing Protocols, and mechanisms for Collaborative detection into one unique framework, making it more resilient to attacks while optimizing the use of network resources. The proposed system is designed to identify Gray-Hole attackers-sending nodes that selectively drop packets-by real-time monitoring, trust-based evaluations, and enhancements for secure routing. The system also allows mechanisms to work properly in the dynamic and mobile environment of VANETs without encountering significant overhead or performance degradation. Key Features of the Proposed System Dynamic Trust and Reputation System Intrusion Detection System (IDS) with Anomaly Detection Enhanced Secure Routing Protocol

(AODV/DSR) Collaborative Detection Mechanism Adaptive Detection with Machine Learning Low-Overhead Multi-Path Routing.

4.3 DYNAMIC TRUST AND REPUTATION SYSTEM

Trust and reputation models are at the heart of identifying malicious nodes, especially Gray-Hole attackers, in a VANET. This proposed system employs a dynamic trust assessment mechanism based on packet forwarding node behaviors.

Trust Metrics: Each node will compute a trust score for its neighbors based on their past behavior, focusing on packet forwarding success rates and responsiveness to routing requests. Nodes that consistently drop packets (selectively drop certain packets while forwarding others) will have a lower trust score.

Adaptive Thresholds: These trust thresholds will be adaptive-they will change upon changing network conditions like mobility and density. False positives will be avoided as network conditions may sometimes cause loss of packets.

Reputation Sharing: Trust scores will be shared by neighboring nodes. Nodes can update and propagate trust values within their communication range, enabling them to detect Gray-Hole attacks based on collective data.

Sybil Attack Mitigation The system employs public-key cryptography (PKI) to authenticate nodes and their reputation data. Each node's identity will be validated by certificates issued by a trusted authority, and the update to their reputation will be signed digitally.

4.4 IDS WITH ANOMALY DETECTION

An IDS will complement this reputation system by monitoring network traffic and detecting anomaly indicators of a Gray-Hole attack.

Packet forwarding monitoring: IDS will monitor packet forwarding behavior on each node and track dropped packets if these are being dropped at

higher rates than normal. This will include the comparison of observed packet dropping behavior to baseline metrics for the detection of nodes that behave with selective packet dropping.

Anomaly Detection: The IDS will utilize machine learning to apply algorithms for example Support Vector Machines SVM or K-means clustering that detects abnormal packets that do not forward according to normal patterns. These models will be trained to recognize attack signatures and automatically classify behavior as normal or anomalous.

Collaborative IDS: The nodes will collaborate with each other by exchanging detection alerts to verify and improve the accuracy of the detection of attacks. Nodes with higher trust scores
relied upon to a greater extent in the detection process.

4.5 ADVANCED SECURE ROUTING PROTOCOL (AODV / DSR)

The routing schemes, AODV and DSR, are thus prone to the Gray-Hole attack, which, in turn, involves the selective discard of packets by the malicious nodes in the route discovery and maintenance phases. The proposed system develops the protocols with enhanced security measures-Packet Forwarding Verification.

A node will not pass on a packet toward a neighbor if it refused to forward it-up and thus, will be suspected and rejected from further consideration as a route. Route Integrity Validation: It will also check for integrity according to this protocol, where all nodes in the path can have trust values sufficiently above a pre-defined threshold, any node with a low trust value will be suspected of being a Gray-Hole attack node and thus filtered from the routing table. Security-Enhanced AODV/DSR: The protocols of the secure versions of AODV and DSR will encompass digital signatures for route authentication; all nodes participating in the route are authenticated by means of digital signatures. In such a case, only

those nodes having authentic signatures will be utilized in route formation and maintenance.

Parameter	**Values**
Area size	1000*1000
Nodes	100
Communication range	250 m
Mobility Model	Srinagar Highway
Simulation Time	900 seconds
Packet Transmission Parameters	512 bytes
Type of Traffic	CBR

TABLE: 1.1 Vanets Simulation Parameter

4.6 COLLABORATIVE DETECTION MECHANISM

The proposed system has a collaborative detection mechanism to enhance the accuracy and robustness of detection against Gray-Hole attacks, where nodes cooperate with each other.

Feedback Exchange: Nodes exchange feedback about their experience with interactions from their neighboring nodes. A node that discovers it is being targeted by a neighbor node which persistently drops packets will disseminate a warning regarding the malicious node.

Voting Mechanism: A voting mechanism would be used to confirm the suspicious nodes. If independent nodes flag a node as malicious multiple times, it will be marked as a Gray-Hole attacker. This minimizes the chances of false alarms and ensures cooperation in the detection of malicious behaviors by the network.

Collaborative IDS: The collaborative detection system will also be integrated with the IDS. Nodes will cross-check the anomalies detected with neighboring nodes, thus increasing the overall accuracy of attack detection.

4.7 ADAPTIVE DETECTION WITH MACHINE LEARNING

The proposed system uses machine learning (ML) to adaptively detect and respond to changing network conditions and attack patterns Adaptive Detection Thresholds: It learns adaptively through reinforcement learning, adjusting the detection thresholds according to changes in the network conditions, such as mobility of nodes and network density. Under these varying conditions, this approach ensures that the system does not give too many false positives or negatives. Behavioral Prediction Machine learning models, especially in particular, supervised learning, predict future node behavior based on historical packet forwarding data. These would be trained to detect emergent Gray-Hole attack patterns for updating detection algorithms at run time.

4.8 LOW OVERHEAD MULTI-PATH ROUTING

To nullify the effects of Gray-Hole attacks, which rely on selective packet dropping, the proposed system incorporates multi-path routing to increase resilience. Multiple Routes: Unlike a single path, the system will send packets along multiple paths concurrently. If a Gray-Hole attacker disrupts one path by dropping packets, the other paths will ensure successful delivery. Route Selection: Multi-path routing algorithms will use trust-based metrics to select the most reliable paths for data transmission, minimizing the risk of relying on paths involving malicious nodes. Load Balancing: Multi-path routing also provides opportunities for load balancing across the network, reducing congestion and improving overall network performance.

CHAPTER 5

METHODOLOGY

5.1 MODULES EXPLANATIONS:

Cluster Formation:

Cluster formation is the process of grouping the nodes in to a single is known as cluster formation. This cluster has n number of nodes those are having same characteristics and also, they are in the single area. This group of single nodes forms the network. There are lot of clusters comes under a base station.

Cluster Head Selection:

Initially, when clusters are being created, each node decides whether or not to become a cluster head for each round as specified by the original LEACH protocol. Each self-selected cluster head, broadcasts an advertisement (ADV) message using non-persistent carrier sense multiple access (CSMA) protocol. The message contains the header identifier (ID).

Cluster Setup:

Each non-cluster head node chooses one of the strongest received signal strengths (RSS) of the advertisement as its cluster head, and transmits a join-request (Join-REQ) message back to the chosen cluster head. The information about the node's capability of being a cooperative node, that is, its current energy status is added into the message. If a cluster head receives the advertisement message from another cluster head y, and if the received RSS exceeds a threshold, it will mark cluster head y as the neighboring cluster head and it record ID. If the sink receives the advertisement message, it will find the cluster head with the maximum RSS, and sends the sink-position message to that cluster head marking it as the target cluster head (TCH).

Schedule Creation:

After all the cluster heads has received the join-REQ message, each cluster head creates a time division multiple access (TDMA) schedule and broadcasts the schedule to its cluster members as in original LEACH protocol. This prevents

collision among data messages and allows the radio of each non-cluster head node to be turned off until its allocated transmission time to save energy.

Route Discovery:

Route discovery is the process of selecting the route for the destination. It used RREQ and RREP for the route discovery process. In this process the RREQ is the broadcast message that is called as a route request. When the destination is identified, the destination sends the unicast RREP through the same path. This is used to find the best path between the source and destination.

Energy Drain:

After finding route, source can make communication with destination. For every data transmission and reception energy level will be decreased at initial energy level of node. Most Probably intermediate node energy can firstly dry due to trans-receiver characteristics. If its energy level is below 1 tends to node failure. It will not able to make communication with others.

1. Topology Formation:

Topology formation is an important issue in a wireless sensor network. Performance parameters such as energy consumption, network lifetime, data delivery delay, sensor field coverage depend on the network topology. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical. Wireless sensor network mainly used for monitoring the events such as disaster tactical in military surveillance. It can be placed in two different manners 1) Regular manner and 2) Irregular manner. Mostly in irregular manner we are deploying sensors in irregularly is the chance for create a fault in sensor networks. Battery depletion is the attack, it drained the energy of sensors. Fault are created by these kind of attack also. It is considered that the sensors are distributed randomly over a large target region A, and designed to detect specified events. Each every one

of sensors can sense specified events in its sensing range, and communicate with others in its transmission range.

Fig 1.6 Topology Formation

2. Isolated Node and Repairing Node

When a sensor does not have a path or communication to another sensor in any cluster, or may receive broken messages, the sensor is an isolated sensor. Some sensors often have irregular communication or unstable connectivity with others, due to reasons such as the location not being suitable for wireless sensor node communication, the environmental interference being very high, etc. Missing RREQ messages can be used to detect the failure of actors**.** After that it's just check whether failed node is critical node or not.

3. Worm whole detection

In this step we finding smallest or large disjoint block**.** Search and Place algorithm is distributed and light weight. The boundary nodes are detected by that are struck nodes, which will launch the Warm whole discovery and the healing process even if these nodes are actually not stuck nodes. In order to differentiate the network border and hole border we are comparing coordinate value of nodes. In real wireless sensor network the node deployment is not uniform. So these networks contain some regions that are not covered by any sensor nodes, called

holes. Topological hole and border detection methods are simple distributed approach to locate nodes near the boundary of the sensor field and the hole boundaries. This method purely relay on the topology of the communication graph. Here the only information available is, whether the nodes can communicate with each other or not. The topological methods never use the any location informations about the sensor nodes. The communication graph has node and edges if corresponding wireless station can communicate with each other. If two nodes can communicate with each other then they come under a common communication radius.

4. Backup Sensor Selection

A middle point between two sensors and of a cluster is a Repair points (RP) which is with the longest and irregular transmission distance and the link between r1 and r2 is vulnerable. Find

Fig 1.7 Repair points

Critical midpoint, search a place algorithm implement to place backup sensor in a network. The RP's identified are provided with the backup sensors of similar configuration as primary sensors. It improves the stability of the network by making system fault tolerant. The search for repair points runs continuously through all the clusters till all the RPs are provided backup sensors.

5.2 FLOW CHART

Fig 1.8 Flow Chart for Proposed System

CHAPTER 6

SOFTWARE REQUIREMENTS

6.1 IMPLEMENTATION TOOLS

NS-2 OVERVIEW

Operating system: windows 7

Simulator: ns2

Ns (from network simulator) is a name for series of discrete event network simulators, specifically ns-1, ns-2 and ns-3. All of them are discrete-event network simulator, primarily used in research and teaching. ns-3 is free software, publicly available under the GNU GPLv2 license for research, development, and use. The goal of the ns-3 project is to create an open simulation environment for networking research that will be preferred inside the research community It should be aligned with the simulation needs of modern networking research. It should encourage community contribution, peer review, and validation of the software. Since the process of creation of a network simulator that contains a sufficient number of high-quality validated, tested and actively maintained models requires a lot of work, ns-3 project spreads this workload over a large community of users and developers.

In 1996-97, ns version 2 (ns-2) was initiated based on a refactoring by Steve McCanne. Use of Tcl was replaced by MIT's Object Tcl (OTcl), an object-oriented dialect Tcl. The core of ns-2 is also written in C++, but the C++ simulation objects are linked to shadow objects in OTcl and variables can be linked between both language realms. Simulation scripts are written in the OTcl language, an extension of the Tcl scripting language. Presently, ns-2 consists of over 300,000 lines of source code, and there is probably a comparable amount of contributed code that is not integrated directly into the main distribution (many forks of ns-2 exist, both maintained and unmaintained). It runs on GNU/Linux,

FreeBSD, Solaris, Mac OS X and Windows versions that support Cygwin. It is licensed for use under version 2 of the GNU General Public License.

The general process of creating a simulation can be divided into several steps: Topology definition: to ease the creation of basic facilities and define their interrelationships, ns-3 has a system of containers and helpers that facilitates this process. Model development: models are added to simulation (for example, UDP, IPv4, point-to-point devices and links, applications); most of the time this is done using helpers.

Node and link configuration: models set their default values (for example, the size of packets sent by an application or MTU of a point-to-point link); most of the time this is done using the attribute system. Execution: simulation facilities generate events, data requested by the user is logged. Performance analysis: after the simulation is finished and data is available as a time-stamped event trace. This data can then be statistically analyzed with tools like R to draw conclusions. Graphical Visualization: raw or processed data collected in a simulation can be graphed using tools like Gnu plot, matplotlib or XGRAPH.

Ns-2 is often criticized because modelling is a very complex and time-consuming task, since it has no GUI and one needs to learn scripting language, queuing theory and modelling techniques. Also, of late, there have been complaints that results are not consistent (probably because of continuous changes in the code base) and that certain protocols have unacceptable bugs.

Ns-3 is often criticized [by whom?] for its lack of support for protocols (like WSN, MANET etc.) which were supported in ns-2, as well as for the lack of backward compatibility with ns-2. As with ns-2, ns-3 is also time consuming to learn and use compared to GUI-based simulators.

6.2 DISCRETE EVENT SIMULATOR

NS (version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and OTcl. NS is primarily useful for simulating local and wide area networks. Although NS is fairly easy to

use once you get to know the simulator, it is quite difficult for a first-time user, because there are few user-friendly manuals. Even though there is a lot of documentation written by the developers which has in depth explanation of the simulator, it is written with the depth of a skilled NS user. The purpose of this project is to give a new user some basic idea of how the simulator works, how to setup simulation networks, where to look for further information about network components in simulator codes, how to create new network components, etc., mainly by giving simple examples and brief explanations based on our experiences. Although all the usage of the simulator or possible network simulation setups may not be covered in this project, the project should help a new user to get started quickly.

Ns is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. Ns began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. In 1995 ns development was supported by DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. Currently ns development is support through DARPA with SAMAN and through NSF with CONSER, both in collaboration with other researchers including ACIRI. Ns has always included substantial contributions from other researchers, including wireless code from the UCB Daedalus and CMU Monarch projects and Sun Microsystems.

6.3 NS2 FEATURES

NS is an object-oriented discrete event simulator

- Single thread of control: no locking or race conditions
- Simulator maintains list of events and executes in sequence order i.e.) one event after another.
- Back end is C++ event scheduler

- Protocols mostly
- Fast to run, more control
- Front end is OTCL
- Creating scenarios, extensions to C++ protocols
- Fast to write and change

6.3.1 PLATFORM TO RUN NS2

- Unix and Unix like systems
- Linux (Use Fedora or Ubuntu versions)
- Free BSD
- SunOS/Solaris
- Windows 95/98/NT/2000/XP

6.3.2 NS PROGRAMMING STRUCTURE

- Create the event scheduler
- Turn on tracing
- Create network topology
- Create transport connections
- Generate traffic
- Insert errors

6.3.3 EVENT SCHEDULAR

In this Event scheduler while we processing many data at a time it will process one by one (i.e.) FIFO concept, so there is no congestion while transferring the packets.

6.4 TRACE ANALYSIS

Trace packets on individual link Trace file format. This section shows a trace analysis a trace analysis a tree analysis. Running the TCL script generates a NAM trace file that is going to be used as an input to NAM and a trace file called “ont.tr” that will be used for our simulation analysis.

Each trace line starts with an event (+, -, d, r) descriptor followed by the si6mulation time (in seconds) of that event, and from and to node, which identify the like on which the event occurred information in the line before flags is packet type and size (in byte).

The next field is flow id (fid) of IPv6 that a user can set for each flow at the input OTcl script. Each though fid field may not be used in a simulator, users can use this field for analysis purpose. The fid field is also used when specifying stream color for the NAM display. The next two fields are source and destination address in forms of “node. Port”.

The next field shows the network layer protocol’s packet sequence number. The last field shows the unique id of the packet.

6.4.1 CREATE NETWORK TOPOLOGY

Create network topology in Physical layer. The Physical Layer is the first and lowest layer in the seven-layer OSI model of computer networking. The implementation of this layer is often termed PHY. The Physical Layer which consists of the basic hardware and bit transmission over transmission medium in network. It is a fundamental layer underlying the logical data structures of the higher-level functions in a network.

The Physical Layer defines the means of transmitting stream of bits rather than logical data packets over a physical link connecting networking nodes. The bit stream may be grouped into code words or symbols and converted to a physical that is transmitted over hardware.

6.5 TRANSPORT CONNECTION

Transport connection which performs in Transport layer. Transport layers are contained in both the TCP/IP which is the foundation of the INTERNET and the OSI model of general networking. The definitions of the Transport Layer are slightly different in these two models.

This article primarily refers to the TCP/IP model, in which TCP is largely for a convenient application programming interface to internet hosts, as opposed to the OSI model of definition interface. The most well-known transport protocol is the (TCP). It lent its name to the title of the entire internet protocol suite TCP/IP.

It is used for connection-oriented transmissions, whereas the connectionless user datagram suite (UDP) is used for simpler messaging transmissions. TCP is the more complex protocol, due to its state full design incorporating reliable transmission and data stream services.

6.6 GENERATE TRAFFIC (APPLICATION LAYER)

In TCP/IP, the Application Layer contains all protocols and methods that fall into the realm of process-to-process communications via an Internet Protocol (IP) network using the Transport layer protocols to establish underlying host-to-host connections. In the OSI model, the definition of its Application Layer is narrower in scope, explicitly distinguishing additional functionality above the Transport Layer at two additional levels: session layer and presentation layer OSI specifies strict modular separation of functionality at these layers and provides protocol for each layer.

INSERT ERRORS: Start debugging of errors.

6.7 NETWORK ANIMATOR (NAM)

Network animator (NAM) is an animator tool for viewing network simulation and real-world packet teaches. It supports topology layout, packet level animation and various DATA inspection tool. Before to use NAM, trace file needs to be created. This trace file is usually generated by NS.

It contains topology information, e.g nodes and links, as well as packet traces. During a simulation, the user can produce topology configuration, layout

information and packet trace using tracing events in NS. Once the trace file is generated, NAM can be used to animate it.

ADVANTAGES OF NS2

- NS is an ongoing effort of research and development.
- It does not require costly equipment.
- Simulators help in easy verification of protocols in less time, money
- Complex scenarios can be easily tested.
- NS offers support for simulating a variety of protocol suites and scenarios.

CHAPTER 7

SIMULATION&LANGUAGE SPECIFICATION

7.1 INTRODUCTION:

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

Fig 1.9 Basic NS2 architecture

7.2 MOTIVATION FOR SIMULATION:

1. Cheap does not require costly equipment
2. Complex scenarios can be easily tested
3. Results can be quickly obtained – more ideas can be tested in a smaller timeframe
4. The real thing isn't yet available
5. Controlled experimental conditions – Repeatability helps aid debugging
6. Disadvantages: Real systems too complex to model.

7.3 NS FEATURES:

1. NS is an object-oriented discrete event simulator – Simulator maintains list of events and executes one event after another
2. Single thread of control: no locking or race conditions
3. Back end is C++ event scheduler
    a. Protocols mostly
    b. Fast to run, more control
4. Front end is OTCL
    a. Creating scenarios, extensions to C++ protocols
    b. Fast to write and change

7.3.1 NS PROGRAMMING STRUCTURES:

1. Create the event scheduler
2. Turn on tracing
3. Create network topology
4. Create transport connections
5. Generate traffic
6. Insert errors

7.3.2 EVENT SCHEDULER:

In this Event scheduler while we processing many data at a time it will process one by one FIFO concept, so there is no congestion while transferring the packets.

7.4 PACKETS

It is the collection of data, whether header is called or not, all header files where present in the stack registers.

Fig 1.10 Stack Register of Packet

7.5 TURN ON TRACING

Trace packets on individual link Trace file format

event	time	from node	to node	pkt type	pkt size	flags	fid	src addr	dst addr	seq num	pkt id

```
r : receive (at to_node)
+ : enqueue (at queue)              src_addr : node.port (3.0)
- : dequeue (at queue)              dst_addr : node.port (0.0)
d : drop    (at queue)
```

```
r 1.3556 3 2 ack 40 ------- 1 3.0 0.0 15 201
+ 1.3556 2 0 ack 40 ------- 1 3.0 0.0 15 201
- 1.3556 2 0 ack 40 ------- 1 3.0 0.0 15 201
r 1.35576 0 2 tcp 1000 ------- 1 0.0 3.0 29 199
+ 1.35576 2 3 tcp 1000 ------- 1 0.0 3.0 29 199
d 1.35576 2 3 tcp 1000 ------- 1 0.0 3.0 29 199
+ 1.356 1 2 cbr 1000 ------- 2 1.0 3.1 157 207
- 1.356 1 2 cbr 1000 ------- 2 1.0 3.1 157 207
```

Fig 1.11 Trace of a packet

7.6 CREATING NETWORK TOPOLOGY (PHYSICAL LAYER)

The Physical Layer is the first and lowest layer in the seven-layer OSI model of computer networking. The implementation of this layer is often termed PHY.

The Physical Layer consists of the basic hardware transmission technologies of a network. It is a fundamental layer underlying the logical data structures of the higher-level functions in a network.

Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture.

The Physical Layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting networking nodes.

The bit stream may be grouped into code words or symbols and converted to a physical that is transmitted over hardware.

7.7 TRANSPORT CONNECTION (TRANSPORT LAYER)

Transport layers are contained in both the TCP/IP which is the foundation of the INTERNET and the OSI model of general networking. The definitions of the Transport Layer are slightly different in these two models.

This article primarily refers to the TCP/IP model, in which TCP is largely for a convenient application-programming interface to Internet hosts, as opposed to the OIS model of definition interface.

The most well-known transport protocol is the (TCP). It lent its name to the title of the entire Internet protocol suite TCP/IP.

It is used for connection-oriented transmissions, whereas the connectionless user datagram suite (UDP) is used for simpler messaging transmissions. TCP is the more complex protocol, due to its design incorporating reliable transmission and data stream services.

7.8 GENERATE TRAFFIC (APPLICATION LAYER)

In TCP/IP, the Application Layer contains all protocols and methods that fall into the realm of process-to-process communications via an Internet Protocol (IP) network using the Transport layer protocols to establish underlying host-to-host connections.

In the OSI model, the definition of its Application Layer is narrower in scope, explicitly distinguishing additional functionality above the Transport Layer at two additional levels: session layer and presentation layer OSI specifies strict modular separation of functionality at these layers and provides protocol for each layer.

7.8.1 MOTIVATION FOR SIMULATIONS

1. Cheap does not require costly equipment
2. Complex scenarios can be easily tested
3. Results can be quickly obtained – more ideas can be tested in a smaller timeframe
4. The real thing isn't yet available
5. Controlled experimental conditions – Repeatability helps aid debugging
6. Disadvantages: Real systems too complex to model

7.9 MODEL OUTPUT

There are three types of outputs

- Nam window
- Tracing
- Xgraph

7.9.1 NETWORK ANIMATOR

Network Animator (NAM) provides the packet level simulation output in a graphical manner. Network Animator is an animation tool for viewing network simulation traces and real-world packet traces. It supports topology layout, packet level animation and various data inspection tools. Before starting to use NAM, a trace file needs to be created. This trace file is usually generated by NS. It contains topology information, e.g. nodes and links, as well as packet traces. During a simulation, the user can produce topology configurations, layout information and packet traces using tracing events in NS. Once the trace file is generated, NAM can be used to animate it as shown in figure 5.1. Upon startup,

NAM will read the trace file, create topology, pop up a window, do layout if necessary and then pause at time 0. Through its user interface, NAM provides control over many aspects of animation.

Fig 1.12 Simulated output of NAM

Tracing

Trace packets on individual link Trace file format

event	time	from node	to node	pkt type	pkt size	flags	fid	src addr	dst addr	seq num	pkt id

```
r : receive (at to_node)
+ : enqueue (at queue)          src_addr : node.port (3.0)
- : dequeue (at queue)          dst_addr : node.port (0.0)
d : drop    (at queue)

        r 1.3556 3 2 ack 40 ------- 1 3.0 0.0 15 201
        + 1.3556 2 0 ack 40 ------- 1 3.0 0.0 15 201
        - 1.3556 2 0 ack 40 ------- 1 3.0 0.0 15 201
        r 1.35576 0 2 tcp 1000 ------- 1 0.0 3.0 29 199
        + 1.35576 2 3 tcp 1000 ------- 1 0.0 3.0 29 199
        d 1.35576 2 3 tcp 1000 ------- 1 0.0 3.0 29 199
        + 1.356 1 2 cbr 1000 ------- 2 1.0 3.1 157 207
        - 1.356 1 2 cbr 1000 ------- 2 1.0 3.1 157 207
```

Fig 1.13 Tracing

Xgraph

Provides the throughput comparison based on a graph which will be generated automatically based on the TCL coding as shown in figure 5.2.

Fig 1.14 Xgraph for simulated output

7.10 NS FEATURES

NS is an object-oriented discrete event simulator

- Simulator maintains list of events and executes one event after another
- Single thread of control: no locking or race conditions

Back end is C++ event scheduler

- Protocols mostly
- Fast to run, more control

Front end is OTCL

- Creating scenarios, extensions to C++ protocols
- Fast to write and change

CHAPTER 8

SOFTWARE INSTALTION

8.1 INSTALLATIONN OF NS2

After completing the installation of ubuntu 10.04, update all the things in that. How to update means Goto the top menu**, system-Administration-update manager**

STEP 1

- Open the terminal. For this Goto **Application-Accessories-Terminal** (or press Ctrl+alt+T)
- Then paste the following command

  sudo apt-get install build-essential autoconf automake libxmu-dev gcc-4.3

STEP 2

Then u need to some files. So, for this, open the Ns-allinone2.34 folder on the desktop, in that open folder OTCL1.13. In that folder, you need to modify the following files.

- Modify **Makefile.in** file
  - In this file, u need to replace **CC= @CC@**
  - With CC**= gcc-4.3**
  - To replace this press **ctrl + H**
  - Then save the document.
- Modify **configure.in** and **configure** files

  In these two files u need to modify. Means u need to replace **ld -shared** with gcc – **shared.** For replacing **ctrl+H** then one dialog box will come. Then save the document.

STEP 3

- Open the **ns-allinone2.34** folder which is present on the desktop,

  Then press **ctrl+L.** Then copy the path on the address bar.

STEP 4

- Then open **Terminal** and do the following.
- Type $**cd "paste the path here" without quotes and press enter**.
- Then Type **$. /Install**
- Then wait for some time, finally if successfully installed, it will display a message as **"for Related Posts"**. Otherwise, some problems might have occurred.

STEP 5

- Then execute the following command in the **Terminal**

  $ gedit ~/.bashrc
- Then one document will be opened automatically.
- Then delete all the content in that document and paste the following code in it.

```
#LD_LIBRARY_PATH
OTCL_LIB=/home/programmer/ns-allinone-2.33/otcl-1.13
NS2_LIB=/home/programmer/ns-allinone-2.33/lib
X11_LIB=/usr/X11R6/lib
USR_LOCAL_LIB=/usr/local/lib
export
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$OTCL_LIB:$NS2_LI
B
:$X11_LIB:$USR_LOCAL_LIB
#TCL_LIBRARY
TCL_LIB=/home/programmer/ns-allinone-2.33/tcl8.4.18/library
USR_LIB=/usr/lib
exportTCL_LIBRARY=$TCL_LIB:$USR_LIB
#PATH
XGRAPH=/home/programmer/ns-allinone-
2.33/bin:/home/programmer/ns-allinone-
```

2.33/tcl8.4.18/unix:/home/programmer/ns-allinone-2.33/tk8.4.18/unix:/home/programmer/ns-allinone-2.33/xgraph-12.1/
NS=/home/programmer/ns-allinone-2.33/ns-2.33/
NAM=/home/programmer/ns-allinone-2.33/nam-1.13/
export PATH=$PATH:$XGRAPH:$NS:$NAM

Then after doing this, press Ctrl+H and replace the following.

/home/programmer/ns-allinone-2.33

Replace this with **/home/your system name/Desktop/ns-allinone-2.34**

- And in that document, at the 2nd line from the last, put **1.14** instead of **1.13**
- And at the 3rd line from the last, make the change as **ns-2.34** instead of **ns-2.33**
- **Then save the document and close it.**

STEP 6

- Then finally copy the following command into the **Terminal**

  "sudo ln -s /home/programmer/ns-allinone-2.33/ns-2.33/ns /usr/bin/ns"
- After pasting it into the **Terminal,** just make the following modifications and then press Enter.
- **Make 2.33 as 2.34**
- And in the place of **"programmer"** in that command, just type your system name. Then the command should be like this.

  "sudo ln -s /home/ur system name/Desktop/ns-allinone-2.34/ns-2.34/ns /usr/bin/ns"
- Then press Enter.
- It will ask for password, enter the password**.**

STEP 7

- Then finally type **"ns"** in the **Terminal** and press Enter**.**
- Then "%" symbol will be displayed.

- Then it was successfully installed. Otherwise, some problems might have occurred in the installation process**.**

STEP 8

- Then finally execute the following command in the Terminal
- Type **"sudo apt-get install xgraph"** and press enter.
- Finished installing Network Simulator.

8.2 SYSTEM MODELLING

System modeling refers to an act of representing an actual system in a simply way. System modeling is extremely important in system design and development, since it gives an idea of how the system would perform if actually implemented.

Traditionally, there are two modeling approaches: analytical approach and simulation approach.

8.3 ANALYTICAL APPROACH

The general concept of analytical modeling approach is to first come up with a way to describe a system mathematically with the help of applied mathematical tools such as queuing and probability theories, and then apply numerical methods to gain insight from the developed mathematical model. When the system is simple and relatively small, analytical modeling would be preferable (over simulation). In this case, the model tends to be mathematically tractable. The numerical solutions to this model in effect require lightweight computational efforts.

If properly employed, analytical modeling can be cost-effective and can provide an abstract view of the components interacting with one another in the system. However, if many simplifying assumptions on the system are made during the modeling process, analytical models may not give an accurate representation of the real system.

8.4 SIMULATION APPROACH

Simulation is a process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system.

Simulation is widely-used in system modeling for applications ranging from engineering research, business analysis, manufacturing planning, and biological science experimentation, just to name a few.

Compared to analytical modeling, simulation usually requires less abstraction in the model (i.e., fewer simplifying assumptions) since almost every possible detail of the specifications of the system can be put into the simulation model to best describe the actual system.

When the system is rather large and complex, a straightforward mathematical formulation may not be feasible. In this case, the simulation approach is usually preferred to the analytical approach.

In common with analytical modeling, simulation modeling may leave out some details, since too many details may result in an unmanageable simulation and substantial computation effort. It is important to carefully consider a measure under consideration and not to include irrelevant detail into the simulation.

Fig 1.15 Packet Arrival event

Fig 1.16 Successful Packet Transmission

CHAPTER 9

RESULTS AND DISCUSSION

A simulation process on how to prevent a gray-hole attack (GHA) in vehicular ad-hoc networks using MATLAB will involve a step-by-step design of the simulation environment, attack implementation, and application of the dynamic prevention of gray hole attack. Below is the broad outline of what one could do in MATLAB. Through MATLAB, one is further able to create and simulate VANETs and the possible network behaviors,

Let us discuss the simulation parameters for the approach of DPGHA against a gray-hole attack in VANETs with the help of MATLAB as well as network simulators like NS-2, SUMO, or custom MATLAB scripts. Such parameters will help you set up your simulation, evaluate performance, and compare the results against benchmark protocol.

9.1 PERFORMANCE EVALUATION

The performance of the proposed DPGHA approach is assessed by comparing it to existing benchmark methods. To ensure a fair evaluation, the following performance metrics were considered: Routing Overhead. By focusing on this key metric, the study aims to quantify how efficiently the proposed approach manages the overhead associated with routing in the system. The comparison highlights the effectiveness of DPGHA in optimizing routing processes while minimizing additional communication costs, offering valuable insights into its practical applicability and advantages over traditional approaches.

- Packet Delivery Ratio
- Throughput
- End-to-End Delay
- Packet Loss Ratio

- Detection Ratio

1) Routing Overhead

Routing overhead is defined as the number of Control packets (CPs) sent in comparison with the total number of Data packets (DPs) received at the destination end. The metric indicates the number of CPs required to send for a given the number of DPs. The major CPs of AODV routing protocol consist of RREQ, RREP, RERR (Route Error), and Hello messages.

$$ROH = \frac{\Sigma CP\ Transmitted}{\Sigma DP\ Transmitted} \quad \ldots (1)$$

Increased overhead is measured. More number of RREPs will be desired routes to accommodate the increased number of malicious nodes in the network when routing overhead becomes very huge. More packets, due to a large number of malicious nodes, hence leads to loss more in conventional AODV. Hence average routing overhead of traditional AODV is about 5508.33.

2) Packet Delivery Ratio (PDR)

The PDR is referred to the ratio of the total number of Number of data packets sent by the source node to the total number of data packets received by the destination node. Calculated by

$$PDR = \left(\frac{\Sigma DP\ Received}{\Sigma DP\ Sent}\right) * 100 \quad \ldots (2)$$

Fig 1.17: Comparison of throughput

Fig 1.18: End To End Delay

9.2 RESULTS:

9.2.1 Simulation Result:

Simulation Result On Ns2 Tool 1

The terminal window shows the user navigating to the project directory using the Ubuntu operating system. The command prompt repeatedly displays the current directory path indicating script testing or re-execution. The user prepares to execute the main simulation script using Network Simulator (NS-2).

Fig 1.19 Simulation Result On Ns2 Tool 1

The command ns main.tcl is used to initiate the simulation. The script prompts for the selection of the routing protocol—Leach (0), Lightweight (1), or comp (2). This interface allows the user to test different protocol configurations against grey-hole attacks.

It highlights the flexibility of running multiple scenarios in VANETs. Grey-hole attackers can be analysed by switching between routing mechanisms. The focus here is on simulating network behaviour before visualization. This stage is essential for initializing parameters for node communication in the simulation.

Simulation Result On Ns2 Tool 2

The terminal shows the loading of the Lightweight.tcl file within the main simulation. The error message indicates that the file is referenced at line 100 of main.tcl. This suggests modular scripting where different protocols or strategies are stored separately.

Fig 1.20 Simulation Result On Ns2 Tool 2

The user continues by executing ns main.tcl again, likely after editing or correcting the code. TCL scripting is essential in NS-2 for configuring VANETs and defining node behaviour. The process emphasizes testing protocol-specific strategies against grey-hole attacks.

This iterative execution helps refine detection algorithms and their responses. Each execution may simulate different attacker behaviour for comparison. The terminal logs act as feedback for script syntax and logic validation. This step is critical before generating trace and animation files for output.

Simulation Result On Ns2 Tool 3

This screenshot shows the Network Animator (NAM) window used to visualize node mobility. The simulation depicts the movement of 100 nodes in a VANET scenario.

Fig 1.21 Simulation Result On Ns2 Tool 3

Each green circle represents a vehicular node communicating with others. The animation bar at the bottom allows control over simulation time steps. The visual interface helps in tracking node interaction and behaviour patterns. It provides a platform to observe how grey-hole nodes drop packets selectively.

Analysts can identify abnormal routing or data loss through this visual inspection. NAM supports real-time or stepwise playback to capture attack patterns. It is an important tool to verify protocol performance visually. This visualization validates the effectiveness of grey-hole prevention techniques implemented.

Node Creation

This terminal screen displays the initialization output after running the simulation. It sets the total number of nodes to 100, as defined in the script. A warning regarding channel usage is displayed, suggesting NS-2 version compatibility tips.

Fig 1.22 Node Creation

The TCL script initializes a list for node-based routing or detection logic. Parameters such as highest AntennaZ and distCST are configured for transmission modelling. These parameters influence communication range and signal behavior in VANETs.

The simulation calculates distances and transmission strength dynamically. It highlights the underlying mathematical computation before node deployment. Sorting lists based on antenna power and coverage ensures realistic communication modelling. This setup stage is essential to accurately detect and analyse grey-hole attacker influence.

Gray Hole Attackers Present

This NAM simulation shows vehicular nodes (green circles) starting communication. A few nodes are transmitting data packets, visualized by black arrows.

Fig 1.23 Gray Hole Attackers Present

Nodes are arranged in random mobility, representing vehicle movement. Black circles represent possible malicious or inactive nodes (grey-hole suspects). The routing protocol begins identifying inconsistent behavior. Communication delay and missing acknowledgments are used for detection.

Some nodes act as monitors for packet flow observation. Initial data sharing is affected due to grey-hole attacks. The detection module flags abnormal drop behavior in specific nodes. This stage shows the early alert system for attacker detection in VANETs.

Detection Gray Hole Attacker

In this frame, communication continues while some nodes are bypassed. A suspicious node fails to forward packets, confirming grey-hole behavior The routing protocol reconfigures alternative paths to prevent packet loss.

Fig 1.24 Detection Gray Hole Attacker

Non-cooperative nodes are visually isolated or darkened. Multiple healthy nodes reroute data to maintain delivery. Cluster-based communication helps in attacker avoidance. Packets rerouted avoid the compromised node using updated tables.

This demonstrates real-time attacker response using lightweight routing. The protocol maintains seamless communication despite threats. The step marks successful detection and dynamic prevention of the attack.

Proper Gray Whole Detection and Avoidance

A data packet is being transmitted (Data ID: 116) to the destination node. A pop-up shows packet size, source, and send time. Packet monitoring reveals successful detection of previous packet drops.

Fig 1.25 Proper Gray Whole Detection and Avoidance

The simulation filters out suspicious nodes, preventing further misuse. The attacker node (red) is bypassed in current routing. Communication resumes with trusted nodes only.

This step reflects enhanced network integrity after prevention. Accurate detection leads to no further packet loss or rerouting. Node activity is monitored to confirm behavior over time. The filtering mechanism effectively removes grey-hole influence.

Data Communication

Post-detection, the network returns to stable communication. All nodes are synchronized and actively forwarding packets. Grey-hole nodes are no longer in the path of critical data flow.

Fig 1.26 Data Communication

Communication routes are cleaner with no visible drops. The animation shows real-time movement and link establishment. Finalized routing ensures minimal disruption and faster delivery.

The visual confirms improved packet delivery ratio. Nodes maintain energy and connectivity in safe regions. This step represents the success of the prevention strategy. VANET is now resilient to grey-hole threats using the proposed model.

9.2.2 THROUGHPUT

The image shows a NAM (Network Animator) simulation window. It represents the movement of 100 nodes in a VANET environment. Nodes are color-coded to show their roles and communication behavior.

Fig 1.27 Throughput

The black arrows between nodes indicate tbbbbhe transmission of data packets. Green nodes are normal, black nodes may indicate suspicious or grey-hole attackers. The step time is set to observe packet flow and detection in sequence. The simulation helps visualize attacker detection and response.

Grey-hole behavior (dropping selective packets) can be observed via missing links. Prevention methods are simulated by changing node status and packet redirection. This visualization aids in understanding the defense mechanism implementation.

9.2.3 DELAY

This graph compares the delay rates between two scenarios. The red bar shows higher delay due to grey-hole attacks. The green bar represents improved delay after prevention.

Fig 1.28 Delay

X-axis represents two techniques: delay_U and delay_V. Y-axis indicates delay values in seconds. The simulation confirms that grey-hole attacks increase delay. Implementing prevention mechanisms reduces end-to-end delay.

Less delay leads to better communication in real-time VANET. This performance metric supports adopting the proposed method. It highlights how security directly affects network latency.

9.2.4 POCKET DELIVERY FACTOR

The graph plots PDR over time for two scenarios. The green line represents performance after prevention. The red line shows PDR in the presence of grey-hole attackers. The X-axis represents time in seconds. The Y-axis shows the number of packets delivered (×10^5). Without prevention, PDR drops due to packet loss. With prevention, the PDR improves consistently. This proves the efficiency of the grey-hole detection system.

Fig 1.29 Pocket Delivery Factor

CHAPTER 10

CONCLUSION AND FUTURE WORK

10.1 CONCLUSION

This research has explored a critical vulnerability within Vehicular Ad Hoc Networks (VANETs)—the Gray-Hole attack—by presenting a hybrid, intelligent, and adaptive detection and prevention framework. Unlike traditional attacks, Gray-Hole attacks are particularly deceptive as they intermittently drop packets, making them harder to detect through conventional means. The proposed system, which integrates anomaly detection techniques, trust and reputation management, and dynamic behaviour monitoring, provides a robust and scalable solution to this challenge.

Through extensive simulation using NS-2 and MATLAB, the proposed approach demonstrates a significant enhancement in key performance metrics. These include higher Packet Delivery Ratio (PDR), reduced average end-to-end delay, minimized packet loss, and better network throughput—even in scenarios with a high density of malicious nodes. The success of this model confirms the hypothesis that combining statistical anomaly detection with behavioural trust models creates a more accurate and responsive system for identifying malicious behaviour in real time.

Moreover, this research bridges the gap between theoretical security models and practical implementation by offering a lightweight, modular design that can be deployed in resource-constrained environments such as on-board vehicle systems. It also emphasizes the importance of proactive threat detection over reactive defence, shifting the paradigm toward intelligent vehicular security systems.

The proposed framework not only mitigates current threats but sets a foundation for the future development of secure, autonomous vehicular communication systems. It contributes to the broader vision of Intelligent Transportation Systems (ITS), where secure, efficient, and resilient data exchange between vehicles can ultimately lead to safer roads, reduced congestion, and enhanced driver assistance technologies.

10.2 FUTURE ENHANCEMENTS

As technology continues to advance and VANETs become an integral part of smart cities and autonomous driving infrastructure, there are several potential directions for future research and development:

1. Adaptive Learning with Artificial Intelligence (AI): While the current system uses a basic machine learning approach for anomaly detection, future iterations can benefit from incorporating deep learning models such as Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNNs), or hybrid models for pattern recognition in traffic behaviour and attack vectors. These AI-driven approaches will enable continuous learning and adaptation to evolving threats.

2. Federated Learning for Privacy-Preserving Intelligence: Given the sensitivity of vehicular data, incorporating federated learning will allow multiple vehicles to collaboratively train models without sharing raw data, enhancing privacy and reducing communication overhead while maintaining high detection accuracy.

3. Integration with Software-Defined Networking (SDN): Employing SDN in VANETs enables centralized control and flexible reconfiguration of network traffic. Integrating the proposed security

framework with SDN controllers can improve real-time response and policy enforcement against malicious behaviour, especially in highly mobile and large-scale networks.

4. Quantum-Resistant-Cryptography:
   With the rapid advancement of quantum computing, future systems must consider implementing post-quantum cryptographic algorithms for authentication and data protection to ensure long-term security sustainability in VANETs.

5. Behavioural Biometrics for Vehicle Profiling:
   Leveraging behavioural biometrics such as driving style, acceleration patterns, and route preferences can further enhance trust models by building unique, tamper-resistant vehicle profiles, making impersonation attacks and Sybil attacks harder to execute.

6. Hybrid VANET-Internet of Vehicles (IoV) Compatibility:
   As VANETs evolve into the broader Internet of Vehicles (IoV), compatibility and integration with other IoT systems such as smart traffic signals, smart homes, and cloud platforms will be essential. Future enhancements should ensure that the security framework can adapt to multi-modal communication environments and heterogeneous devices.

7. Energy Efficiency and Green Computing:
   With the increasing focus on sustainability, optimizing the energy consumption of security protocols in electric and hybrid vehicles is becoming critical. Future research could explore energy-aware security solutions that balance protection and resource conservation.

8. User Interface for Driver Alerts and Manual Overrides:
   Including an intuitive interface for alerting drivers about potential threats,

suspicious nodes, or suggested route changes could bridge the gap between automated systems and human decision-making, increasing trust and usability.

9. Cross-Layer-Security-Integration:
   Future versions of the framework can adopt a cross-layer security strategy that integrates security protocols at the physical, data link, network, and application layers. This comprehensive approach will help detect and prevent multi-faceted attacks that exploit vulnerabilities across different communication layers.

10. Real-Time Analytics and Visualization Tools**:**
    Providing real-time dashboards and visualization tools for network administrators or vehicle manufacturers can help monitor security health, perform diagnostics, and assess attack patterns dynamically.

These enhancements, collectively, will transform the proposed model into a full-fledged, real-world deployable solution. They reflect a broader vision for secure, intelligent, and connected vehicular systems that are not only reactive to attacks but are predictive, adaptive, and resilient. As VANETs pave the way toward fully autonomous transportation and smart mobility ecosystems, continued innovation in security mechanisms like those proposed in this work will be vital in ensuring safe and trustworthy communication on the road.

APPENDICES

SIMULATION

```
puts "Enter option Leach (0) or Lightweight (1) or comp (2)"
set opt_ [gets stdin]
set bopt_ 1
if {$opt_==0} {
set bopt_ 0
}
if {$opt_==2} {
        exec xgraph en_grp_0 en_grp_1 -x "time" -y "energy" -lw 2 &
        exec xgraph PDF_0 PDF_1 -x "time s" -y "pkts" -lw 2 &
        #exec xgraph TPDF_0 TPDF_1 TPDF_2 -x "time s" -y "pkts" -nl -
bar -brw 0.5 &
        exec xgraph OH_0 OH_1 -x "time s" -y "pkts" -lw 2 &
      exec xgraph delay_0 delay_1 -x "tech" -y "Delay rate" -bg "black" -
fg "white" -bar -brw 1 -nl &
      exec xgraph th_0 th_1 -x "time" -y "Packet size" -t "Throughput" -
bg "black" -fg "white" -lw 3 &
exit
}
#
==================================================================
# Define options
#
==================================================================
set val(chan) Channel/Wireless Channel; # Channel Type
```

```
set val(prop) Propagation/TwoRayGround ;#Nakagami
#TwoRayGround; # radio-propagation model
set val(netif) Phy/WirelessPhy
set val(ant)Antenna/Omni Antenna; # antenna model
set val(mac) Mac/802_11
set val(ll) LL; # link layer type
set val(rp) DSDV; # AODV; # routing protocol
set val(ifq) Queue/DropTail/PriQueue; #; #; CMUPriQueue; # #
Queue/DropTail/PriQueue for AODV & DSDV CMUPriQueue for DSR
set val(ifqlen) 50; # max packet in ifq
set val(nn) 51; # number of mobilenodes
set val(x) 500;
set val(y) 500;
#Set val(nam) out.nam;
#Set val(traffic) ftp; # cbr/poisson/ftp
#
=====================================================
========================
set ns_                 [new Simulator]
set ns $ns_
set ran [new RNG]; #random number generator
set tracefd [open out.tr w]
set namtrace[open out.nam w]
set En_fl[open en_grp_$opt_ w]
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)
$ns_ trace-all $tracefd
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
set God[create-god100]
```

```
#
==========================================================
=========================
if {1} {
set txp 0.001
$ns_ node-config -energyModel EnergyModel \
-rxPower 0.0005 \
-txPower $txp \
-initialEnergy 100 \
-idlePower 0.5
}
#
==========================================================
====================
$ns_ node-config -adhocRouting $val(rp) \
                -llType $val(ll) \
                -macType $val(mac)\
                -ifqType $val(ifq) \
                -ifqLen $val(ifqlen) \
                -antType $val(ant) \
                -propType $val(prop) \
                -phyType $val(netif) \
        -channelType  $val(chan)\
                -topoInstance $topo \
                -agentTrace ON \
                -routerTrace ON \
                -macTrace ON \
                -movementTrace ON
```

```
#
==========================================
$ns_ color 1 red
$ns_ color 2 green
$ns_ color 3 purple
#
=========================================
source trace
source Lightweight.tcl
source Leach.tcl
set fg 300
set PS [new Pan_Sim]
for {set i 0} {$i<$val(nn)} {incr i} {
set node_($i) [$ns_ node]
        set nd_($i) [$PS Node]
        set CH_lst [list]
   $node_($i) color black
}
  $node_ (0) set X_ 83
  $node_ (0) set Y_ 168
  $node_ (1) set X_ 59
  $node_ (1) set Y_ 110
  $node_ (2) set X_ 100
  $node_ (2) set Y_ 13
  $node_ (3) set X_ 120
  $node_ (3) set Y_ 100
  $node_ (4) set X_ 140
  $node_ (4) set Y_ 160
  $node_ (5) set X_ 155
```

```
  $node_ (5) set Y_ 270
  $node_ (5) set X_ 1
  $node_ (5) set Y_ 270
set y 200
set z 100
set n 6
#$ns_ at 7.1 "$nd_(1) make-failure"
for {set i 200} {$i<280} {incr i +70} {
        for {set j 100} {$j<180} {incr j +70} {
                $node_($n) set X_ $i
                $node_($n) set Y_ $j
      incr n
      if {$n >=$val(nn)} {break}
  }
      if {$n >=$val(nn)} {break}
}
  $node_ (10) set X_ 237
  $node_ (10) set Y_ 134
  $node_ (11) set X_ 165
  $node_ (11) set Y_ 280
  $node_ (11) set X_ -25.4646
  $node_ (11) set Y_ 473.608
set in 12
for {set i 310} {$i<390} {incr i +70} {
        for {set j 250} {$j<330} {incr j +70} {
                $node_($n) set X_ $i
                $node_($n) set Y_ $j
      incr n
      if {$n >=$val(nn)} {break}
```

```
  }
      if {$n >=$val(nn)} {break}
}
  $node_ (16) set X_ 344
  $node_ (16) set Y_ 290
  $node_ (17) set X_ 100
  $node_ (17) set Y_ 399
  $node_ (18) set X_ 170
  $node_ (18) set Y_ 402
  $node_ (19) set X_ 100
  $node _ (19) set Y_ 481
  $node_ (20) set X_ 170
  $node_ (20) set Y_ 481
  $node_ (21) set X_ 135
  $node_ (21) set Y_ 446
 $node_ (22) set X_ -87.9252
 $node_ (22) set Y_ 425.696
 $node_ (23) set X_ -58.3266
 $node_ (23) set Y_ 444.847
 $node_ (24) set X_ -106.207
 $node_ (24) set Y_ 442.236
 $node_ (25) set X_ -55.715
 $node_ (25) set Y_ 420.472

 $node_ (26) set X_ 194.132
 $node_ (26) set Y_ 237.658
 $node_ (27) set X_ 242.883
 $node_ (27) set Y_ 245.493
 $node_ (28) set X_ 221.119
```

```
$node_ (28) set Y_ 268.128
$node_ (29) set X_ 279.446
$node_ (29) set Y_ 237.659
$node_ (30) set X_ 266.387
$node_ (30) set Y_ 270.74
$node_ (31) set X_ 227.213
$node_ (31) set Y_ 329.066
$node_ (32) set X_ 208.061
$node_ (32) set Y_ 310.784
$node_ (33) set X_ 181.944
$node_ (33) set Y_ 321.23
$node_ (34) set X_ 151.475
$node_ (34) set Y_ 346.476
$node_ (35) set X_ 152.455
$node_ (35) set Y_ 305.017
$node_ (36) set X_ -52.8857
$node_ (36) set Y_ 137.329
$node_ (37) set X_ -29.2721
$node_ (37) set Y_ 190.32
$node_ (38) set X_ -75.5199
$node_ (38) set Y_ 161.921
$node_ (39) set X_ -24.7018
$node_ (39) set Y_ 163.336
$node_ (40) set X_ -63.6587
$node_ (40) set Y_ 189.561
$node_ (41) set X_ -110.124
$node_ (41) set Y_ 248.432

$node_ (42) set X_ -161.813
```

```
$node_ (42) set Y_ 260.619
$node_ (43) set X_ -122.856
$node_ (43) set Y_ 200.225
$node_ (44) set X_ -178.244
$node_ (44) set Y_ 229.824
$node_ (45) set X_ -148.102
$node_ (45) set Y_ 228.736
$node_ (46) set X_ -102.289
$node_ (46) set Y_ 299.794
$node_ (47) set X_ -69.6437
$node_ (47) set Y_ 350.504
$node_ (48) set X_ -113.171
$node_ (48) set Y_ 356.924
$node_ (49) set X_ -160.724
$node_ (49) set Y_ 326.019
$node_ (50) set X_ -117.85
$node_ (50) set Y_ 324.082
$nd_ (0) set-en 70
$nd_ (7) set-en 70
$nd_ (0) set drt_ 0.015
$nd_ (1) set drt_ 0.018
$nd_ (1) set drt_ 0.021
$nd_ (6) set drt_ 0.014
$nd_ (7) set drt_ 0.018
$nd_ (8) set drt_ 0.022
set BS 5
#$ns_ at 1.0 "$nd_ (5) label BaseStation"
$ns_ at 0 "$node_ (5) label BS"
$ns_ at 0 "$node_ (5) color red"
```

```
#$ns_ initial_node_pos $node_ (5) 30
#Set Mc 11
$ns_ at 1.1 "$nd_ (0) send_Data $BS"
$ns_ at 1.11 "$nd_ (1) send_Data $BS"
$ns_ at 1.12 "$nd_ (2) send_Data $BS"
$ns_ at 1.13 "$nd_ (3) send_Data $BS"
$ns_ at 1.14 "$nd_ (4) send_Data $BS"
$ns_ at 1.1 "$nd_ (6) send_Data $BS"
$ns_ at 1.11 "$nd_ (7) send_Data $BS"
$ns_ at 1.12 "$nd_ (8) send_Data $BS"
$ns_ at 1.13 "$nd_ (9) send_Data $BS"
$ns_ at 1.14 "$nd_ (10) send_Data $BS"
$ns_ at 1.1 "$nd_ (16) send_Data $BS"
$ns_ at 1.11 "$nd_(12) send_Data $BS"
$ns_ at 1.12 "$nd_ (13) send_Data $BS"
$ns_ at 1.13 "$nd_(14) send_Data $BS"
$ns_ at 1.14 "$nd_(15) send_Data $BS"
$ns_ at 1.1 "$nd_(21) send_Data $BS"
$ns_ at 1.11 "$nd_(17) send_Data $BS"
$ns_ at 1.12 "$nd_(18) send_Data $BS"
$ns_ at 1.13 "$nd_(19) send_Data $BS"
$ns_ at 1.14 "$nd_(20) send_Data $BS"
$ns_ at 1.1 "$nd_(22) send_Data $BS"
$ns_ at 1.11 "$nd_(23) send_Data $BS"
$ns_ at 1.12 "$nd_(24) send_Data $BS"
$ns_ at 1.13 "$nd_(25) send_Data $BS"
$ns_ at 1.13 "$nd_(11) send_Data $BS"
$ns_ at 1.1 "$nd_(26) send_Data $BS"
$ns_ at 1.11 "$nd_(27) send_Data $BS"
```

```
$ns_ at 1.12 "$nd_(28) send_Data $BS"
$ns_ at 1.13 "$nd_(29) send_Data $BS"
$ns_ at 1.14 "$nd_(30) send_Data $BS"
$ns_ at 1.1 "$nd_(31) send_Data $BS"
$ns_ at 1.11 "$nd_(32) send_Data $BS"
$ns_ at 1.12 "$nd_(33) send_Data $BS"
$ns_ at 1.13 "$nd_(34) send_Data $BS"
$ns_ at 1.14 "$nd_(35) send_Data $BS"
$ns_ at 1.1 "$nd_(36) send_Data $BS"
$ns_ at 1.11 "$nd_(37) send_Data $BS"
$ns_ at 1.12 "$nd_(38) send_Data $BS"
$ns_ at 1.13 "$nd_(39) send_Data $BS"
$ns_ at 1.14 "$nd_(40) send_Data $BS"
$ns_ at 1.1 "$nd_(41) send_Data $BS"
$ns_ at 1.11 "$nd_(42) send_Data $BS"
$ns_ at 1.12 "$nd_(43) send_Data $BS"
$ns_ at 1.13 "$nd_(44) send_Data $BS"
$ns_ at 1.14 "$nd_(45) send_Data $BS"
$ns_ at 1.1 "$nd_(46) send_Data $BS"
$ns_ at 1.11 "$nd_(47) send_Data $BS"
$ns_ at 1.12 "$nd_(48) send_Data $BS"
$ns_ at 1.13 "$nd_(49) send_Data $BS"
$ns_ at 1.14 "$nd_(50) send_Data $BS"
if {$opt_>0} {
        $ns_ at 1.3 "$nd_(6) make-failure"
} else {
        $ns_ at 1.3 "$nd_(8) make-failure"
      $ns_ at 1.3 "$nd_(50) make-failure"
      $ns_ at 1.3 "$nd_(33) make-failure"
```

```
}
proc Grph {} {
        global En_fl nd_ ns_
        set en 100
set nd x
        foreach n [array names nd_] {
                set ene [$nd_($n) set energy]
                if {$en>$ene && ($n!=5 && $n!=11) && $ene>2} {
                        set en $ene
                        set nd $n
                }
        }
puts "$nd -- $en"
        puts $En_fl "[$ns_ now] $en"
        $ns_ at [expr [$ns_ now]+1] "Grph"
}
$ns_ at 0 "Grph"
for {set i 0} {$i<$val(nn)} {incr i} {
  $ns_ initial_node_pos $node_($i) 10
}
proc finish {} {
        global ns_ namtrace  nd_ opt_ En_fl
        $ns_ flush-trace
        close $namtrace
        close $En_fl
        exec awk -f pdf.awk out.tr >PDF_$opt_
        exec awk -f OH.awk out.tr >OH_$opt_
       exec awk -f th.awk out.tr >th_$opt_
        #exec awk -f LT.awk out.tr >LifeTime_$opt_
```

```
        #exec awk -f energy.awk out.tr >en_grp_$opt_
          exec nam out.nam &
          #exec xgraph en_grp_$opt_ -x "time" -y "energy" -lw 2 &
        exec xgraph th_$opt_ -x "time s" -y "pkts" &
          exec xgraph PDF_$opt_ -x "time s" -y "pkts" &
          exec xgraph OH_$opt_ -x "time s" -y "pkts" &
          #exec xgraph LifeTime_$opt_ -x "No of Rounds" -y "No of Active
Nodes" &
          exit
}
$ns_ at 40 "finish"
$ns_ run
```

REFERENCES

[1] V. Tabus, D. Moltchanov, Y. Koucheryavy, I. Tabus, and J. Astola, ``Energyefcient wireless sensor networks using linear-programming optimization of the communication schedule," J. Commun. Netw., vol. 17, no. 2, pp. 184197, Apr. 2015.

[2] M. Sefuba and T. Walingo, ``Energy-efcient medium access control androuting protocol for multihop wireless sensor networks," IET WirelessSensor Syst., vol. 8, no. 3, pp. 99108, Jun. 2018.

[3] S. K. Singh, P. Kumar, and J. P. Singh, ``A survey on successors of LEACHprotocol," IEEE Access, vol. 5, pp. 42984328, 2017.

[4] H. Kim and S.-W. Han, ``An efficient sensor deployment scheme for large-scale wireless sensor networks," IEEE Commun. Lett., vol. 19, no. 1, pp. 98101, Jan. 2015.

[5] K. Eritmen and M. Keskinoz, ``Improving the performance of wirelesssensor networks through optimized complex eld network coding," IEEESensors J., vol. 15, no. 5, pp. 29342946, May 2015.

[6] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, ``Topological detection onwormholes in wireless ad hoc and sensor networks," IEEE/ACM Trans.Netw., vol. 19, no. 6, pp. 17871796, Dec. 2011.

[7] J. Padmanabhan and V. Manickavasagam, ``Scalable and distributed detection analysis on wormhole links in wireless sensor networks for networkedsystems," IEEE Access, vol. 6, pp. 17531763, 2018.

[8] M. Ditzel and K. Langendoen, ``D3: Data-centric data dissemination inwireless sensor networks," in Proc. Eur. Conf. Wireless Technol., Paris,France, 2005, pp. 185188.

[9] P. R and M. Pushpalatha, ``SDN enabled SPIN routing protocol for wirelesssensor networks," in Proc. Int. Conf. Wireless Commun., Signal Process.Netw. (WiSPNET), Chennai, India, Mar. 2016, pp. 639643.

[10] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva,``Directed diffusion for wireless sensor networking," IEEE/ACM Trans.Netw., vol. 11, no. 1, pp. 216, Feb. 2003.

[11] P. Mishra and R. Tripathi, ``Optimum energy path (OEP) protocol forwireless sensor network," in Proc. Int. Conf. Circuits, Syst., Commun. Inf.Technol. Appl. (CSCITA), Mumbai, India, Apr. 2014, pp. 116120.

[12] S Vimalnath, G Ravi (2020) “Optimized Geographic Routing in Mobile Ad Hoc Network using Bees Swarm Optimization”, Journal of Scientific & Industrial Research, Publishe: NISCAIR-CSI,Vol. 79, pp. 727-729.

[13] X. Yang, L. Wang, and Z. Zhang, ``Wireless body area networks MACprotocol for energy efciency and extending lifetime," IEEE Sensors Lett.,vol. 2, no. 1, Mar. 2018, Art. no. 7500404.

[14] M. Elsersy, T. M. Elfouly, and M. H. Ahmed, ``Joint optimal placement,routing, and ow assignment in wireless sensor networks for structuralhealth monitoring," IEEE Sensors J., vol. 16, no. 12, pp. 50955106, Jun. 2016.

[15] S. Puvaneshwari and S. Vijayashaarathi, ``Efficient monitoring system forcardiac patients using wireless sensor networks (WSN)," in Proc. Int. Conf.Wireless Commun., Signal Process. Netw. (WiSPNET), Chennai, India,2016, pp. 15581561.

[16] Vimalnath. S, Ravi. G., (2020). “Optimized Geographic Routing in Mobile Ad Hoc Network Using Gray Wolf Optimization,” EAI (Research Article-EAI.EU). endorsed transaction.

[17] H. Lin, L. Wang, and R. Kong, ``Energy efcient clustering protocolfor large-scale sensor networks," IEEE Sensors J., vol. 15, no. 12, pp. 71507160, Dec. 2015.

[18] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan,``An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660670, Oct. 2002.

[19] D. M. Birajdar and S. S. Solapure, ``LEACH: An energy efcient routing protocol using Monets for Wireless Sensor Network," in Proc. Netconf. Inventive Commun. Compute. Technol. (ICICCT), Coimbatore, India,2017, pp. 465470.

[20] T. Giannetsos and T. Dimitriou, ``LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks," J. Comput. Syst. Sci., vol. 80, no. 3, pp. 618643, May 2014.

[21] Vimalnath, M. S., Priyanka, S., & Sandhiya, M. (2020). “Vehicle as vehicular networks for big data transfer between data centers in ICF”. (2020) International Research Journal of Engineering and Technology (IRJET), (e-ISSN: 2395-0056).

LIST OF PAPERS PUBLISHED

Dr. S. Vimalnath, Midhun R, Kavinesh A S, Karvendan P, Kishore K, “Enhanced Security Framework for Gray-hole Attack Prevention in Vehicular Networks” International Conference on Visual Analytics and Data Visualization ICVADV-2025 , 979-8-3315-2139-4/25/$31.00 ©2025 IEEE.

Proceedings of

International Conference on Visual Analytics and Data Visualization (ICVADV 2025)

Date: 4-6, March 2025

Organised by: Francis Xavier Engineering College, Tirunelveli, India

48	Enhancing E-commerce using Fashion Recommendation System Vinodh Kumar S, Kumar P, Saravanan S	300
49	Non- Intrusive Load Monitoring Techniques for Intelligent Energy Management: A Comparative Study of Fhmm and LSTM Approach N. Rajkumar, Anitha Govindaram, R. Geetha, Subhamathi A S F, Nithya S. , Jose Anand A. ,	306
50	A Comparative Analysis of IoT Platform Tools: Security and Scalability Preferences in Device Management using Ahp Maheswari S. , N. Rajkumar, R. Geetha, Kalakuntla Theja, M. Malleswari, Jose Anand A. ,	312
51	Continuous Sign Language Recognition and Translation using Deep Learning Approach Rakesh Kumar M, Kumar P, Vaseekaran R	318
52	AI based Efficient Analysis and Monitoring of Sugarcane Buds Detection and Leaf Disease Classification Ananthajothi K, Kumar P, Koteeswaran V	324
53	Integrated Deep Learning Framework for Automated Glaucoma Detection, Optic Disc/ Cup Segmentation, and Cdr Calculation Tina Brivitha K J, Sophia S,	330
54	Gesturelanguagerecognitionthroughdeep Learning D. Pradeep, Monisha S, Nandhini J, Poogesh R, Praneeshwar R	338
55	Drone Cyber Attack Detection through Machine Learning Sophia S, Getzi Jeba Leelipushpam paulraj, Devanshu Kumar	346
56	Lightweight Contextual Llms for IoT Data Interpretation in Smart Cities Tamilarasan Kannadasan	354
57	Svd Processor to Minimize the Number of Rotations in Jacobi Algorithm Sudhakar K, Balaji N, Tharunkumar R B,	360
58	Automating Brain Hemorrhage Detection through Deep Learning Approaches Shakina Princess S, Vignesh. R,	367
59	Contextual Aligned Tamil Sign Language Retrieval System with Semantic Masked Transformer S Thillai Sivakavi, R I Minu	374
60	Visionaid: Enhancing Accessibility for the Visually Impaired with YOLO and Gtts Bhagya Lakshmi Raghupathy, Nithyashri J	380
61	Electric Vechicle Battery Parameters Monitoring System using IoT Aruna S, Dharaneesh V M, Hariprasath E, Somasundaram PL	387
62	Development of Solar Powered 21-level Transformer-less Multilevel Inverter B. SharmilaDevi, M. P. Prasanna Venkatesh, S. Sulochini, T. Sudhakaran, R. Srinithi	393
63	Intelligent Battery Management Strategy Kamalraj VR, Dharshine B, Archana J, Dhanush V, Indhumathi R	397
64	Exploring Depression and Co-dependency Among Spouses of Individuals with Alcohol Use Disorder Padmapriya D. , Mahalakshmi M. , Manisha V. , Manju S. , Suganya M. , Ajith M. ,	404
65	Enhanced Security Framework for Gray-hole Attack Prevention in Vehicular Networks S. Vimalnath, Midhun R, Kavinesh A S, Karvendan P, Kishore K	410
66	Enhancing Master Data Management Within Enterprise Resource Planning Systems using Artificial Intelligence for Optimized Business	416

Proceedings of the International Conference on Visual Analytics and Data Visualization (ICVADV-2025)
DVD Part Number: CFP25VQ6-DVD; ISBN: 979-8-3315-2138-7

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

Dr. S. Vimalnath
Associate Professor
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
vimalnaths.ece@mkce.ac.in

Midhun R
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
rvmidhun5784@gmail.com

Kavinesh A S
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
Kavinesh565@gmail.com

Karvendan P
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
karvendanselva@gmail.com

Kishore K
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
kishoresuriya638@gmail.com

***Abstract* --The gray-hole attacks are certainly destructive to the integrity and reliability of vehicular ad-hoc networks where a malicious node will drop packets selectively while keeping the instance innocuous. Commercial and Safety Applications Vehicular Ad-Hoc Networks and IoT of Vehicles, ITS, and V2X VANETs nowadays are advancing fast in tune with the commercial and safety applications. Nonetheless, despite offering plenty of possible advantages, VANETs cowl an openly-distributed-dynamic nature that raises their exposure to different classes of attacks and threats, one of those being the gray-hole attack (GHA)_. The first version is known as Smart GHA that did not disclose its wrongdoing during routing discoveries, whereas in the second variant-a sequence-based GHA-it behaves wrongly at the route discovery stage but selectively drops packets-after the route was established-in this two-pronged form. The present work specifies the novel strategy in the field of security which is termed Detection and Prevention of GHA (DPGHA). In it, both forms of GHA have been detected and prevented in AODV-based VANETs. The dynamic threshold values defined in DPGHA are based on the anomalies in the packets that are received, forwarded, and generated with their sequence numbers. Dynamic threshold values and dynamic monitoring could increase computational complexity even more and increase the processing requirements imposed on a node with limited resources. The algorithm endorses cooperative detection of malicious behavior and vehicles' resilience. Simulation and evaluation of the ARBD algorithm indicate enhanced accuracy and efficiency in the identification of gray-hole attackers, thus securing and boosting VANET performance.**

Keywords:* *VANET, AODV, GHA, DPGHA.

I. INTRODUCTION

A. Vanet

Broadly defined, Vehicular A d-hoc Networks are a type of mobile wireless network where vehicles are the Considered nodes. The idea is that any vehicle might serve to relay messages. This creates mobile networks spread out quite large in dimension, as distances of about 100-300 meters between vehicles may be bridged. When a vehicle exits the transmission range, which signifies its network exit, a bunch of new vehicles may enter into the network, creating the chance of mobile networks out there. These networks facilitate real-time data exchange regarding safety, traffic management, and driver assistance.

Fig 1: Vanet Design

For example, alerts concerning road conditions, accidents, and traffic congestion may be forwarded via VANET so as to raise efficiency and road safety. But associated with an increasing complexity and functionality of it is security problems. One of the huge devastating threats to VANET is the Gray-Hole Attack. A Gray-hole attack is fundamentally selective dropping of packets while forwarding others that makes detection even harder. A Black-Hole attack drops packets without executing any forwarding. Gray-Hole attacks cause hefty consequences, more so in safety-critical applications, such as collision avoidance and emergency messaging, where vehicular-to-vehicular and vehicular-to-infrastructure communications may be in jeopardy resulting from packet loss and/or delayed messaging, thus compromising safety.

B. Vanet Architecture And Functioning

A vehicular network consists of a number of vehicles known as vehicular nodes. As a prerequisite for the vehicular node system, the authority involved is the certification authority. Such vehicular nodes are designed to communicate each other by 5.9GHz radio frequency over a kilometer. This signal has a forged connection whereby it provides a good wireless access infrastructure to move around freely [1]. Every vehicle has this on-board unit, OBU. It communicates through radio signals between nodes or routers, thus making it easy for them to talk to one another. In the vehicular network, roadside units will act as routers and will usually mount physically near the roads while it connects the vehicles further on to other nodes as depicted in every individual on board. It also has a Tamper Proof here could be information such as driver identity, vehicle speed, trip information, route information, etc. Another such element is the Electronic License Plate (ELP), which is a special number for each vehicle and identification for vehicles. GPS is used for determining location nodes in vehicular networks. Each automobile utilizes GPS. The purpose of RSU is to stockpile all these vehicle-related data.

C. Gray-Hole Attack in VANETs

The Gray-Hole Attack utilizes the dynamic nature of VANETs, whereby nodes (vehicles) are highly mobile and topology changes in the network very fast. The fluid environment makes it even harder for traditional security mechanisms in the network because the node might take advantage and deliberately or selectively drop packets based on type, destination, and even time while pretending to be normal in other instances. Because the attacker is not interfering with all the incoming traffic, the malicious activities of the attacker go unnoticed very quickly by other nodes. The impact of this attack may be from causing slight delays in delivering any data to significantly affecting the reliability throughout the network. For example, critical information such as accident warnings, hazard notifications, or traffic signals may be selectively dropped, leading to communication failure and potential for accidents or the misdirection of traffic flow. The selective nature of the Gray-Hole Attack renders it especially pernicious since its greyness enables it to fly under the radar of most monitoring mechanisms, which would expect nodes to be either completely good or completely bad.

D. Need For Security In Vanets

Given the importance of VANETs for modern transportation systems, security and integrity of data become a prime concern. Attacks like Gray-Hole pose deep risks not only on the performance of the network but also to public safety. Therefore, solutions for securing VANETs have to detect malicious behavior robustly against various attacks, prevent such attacks, and ensure confidentiality and integrity of data without significant overhead and impact on performance. Given that designing adaptive, scalable, and efficient security mechanisms specifically tailored to the vulnerabilities of VANETs is challenging, a combined approach representing a detection, prevention, and secure communication mechanism that would prove appropriate in the highly dynamic environments of VANETs is necessary for successful protection against Gray-Hole attacks. This paper presents an Enhanced Security Framework for the prevention of Gray-Hole attacks in VANETs through combining several techniques for detection and prevention, with secure communication. It uses:

1) Reputation-Based Systems

Nodes are assigned reputation scores based on the behavior exhibited, like successful forwarding of packet. If a node continues dropping packets or acts abnormally, then its reputation score is reduced, and it becomes easier to discover Gray-Hole attackers.

2) Collaborative Detection

The nodes in this network collaborate with one another to verify the behavior of neighboring nodes. Using redundant paths and acknowledgments, they can detect whether a node is selectively dropping packets. Cross-verification techniques help to pinpoint malicious nodes by comparing received and forwarded data The framework uses secure versions of the routing protocols AODV (Ad hoc On-demand Distance Vector) and DSR (Dynamic Source Routing), along with enhanced security features. The protocols are then modified to monitor and validate node behaviors so as to identify the Gray-Hole attackers.

3) IDS

Intrusion Detection Systems (IDS) monitor the network for unusual behavior by identifying potential Gray-Hole attacks based upon traffic patterns and routing anomalies.

II. RELATED WORK

Gray hole attacks on VANETs are stealthy and targeted attacks, prompting significant research toward their detection and mitigation. The Gray-Hole attack consists of the situation where one in a series of routing or data packets is dropped in transit by an adversarial node; proper packet loss analyses render detection near impossible. A host of techniques ranging from intrusion detection systems (IDS) to secure routing protocols were touted over the years for their ability to thwart or even detect such attacks. Herein is discussed some of the key related work on the topic.

1. Intrusion Detection Systems (IDS) for Gray-Hole Attack Detection IDS generally intends to detect Gray-Hole attacks in VANET by monitoring the network traffic and its associated anomalies in nodes. IDS packets forward looking at their forwarding pattern also detect malicious behavior, such as selective packet dropping.

2.Hossain et al. (2016) proposed IDS-based solution to detect Gray Hole attacks with packet dropping ratio analysis. They monitor the nodes' packet forwarding behavior pattern and compare this with the patterns of expected ones. Nodes which have abnormally long packet dropping intervals are marked as potential Gray-Hole attackers. The main challenge for the method is scalability in large-scale networks with high vehicle mobility.

3.Tushar et al. (2018) proposed an IDS that applied machine learning in identifying anomalies in packet forwarding behavior. The model was designed with adaptation to various attack patterns for improving detection abilities. However, it suffers from resource consumption and complexity.

III. TECHNOLOGIES USED

A. Intrusion Detection Systems (IDS)

Intrusion Detection System (IDS) is perhaps the most critical in observing the behavior of network nodes in a vehicle ad hoc network. Detection of irregularities in basic functions is taken as having a suspicion of Gray-Hole attacks. IDSs typically engaged consist of: Traffic Monitoring. These tools monitor routing behavior and search for anomalies in network flows and packet movement patterns that may reveal a Gray-Hole attack, two examples being packet sniffers and network analyzers. Anomaly Detection Algorithms. Intrusion Detection Systems recognize abnormal packet dropping or packet forwarding behaviors by modelling normal behavior through machine learning or statistical techniques. Signature-Based IDS: This policy uses signatures of existing known attacks to detect known attack patterns. The IDS would discover Grey-Hole attacks by checking sensed traffic flows against known attack signatures for packet dropping or selective forwarding.

B. Trust and Reputation-Based Systems

A trust and reputation-based system, on the other hand, tries to evaluate the trustworthiness of nodes based on their past behavior, such as successful packet forwarding. Those malicious nodes, which perform selective packet dropping behaviors, would have low trust values, thus making it easier to detect them as Gray-Hole attackers. A trust-based method was put forward by Qin et al. (2013), wherein each node calculates its neighbor's trustworthiness based on the successful delivery rate of packets. Malicious nodes will come to be isolated and excluded from the network. Although trust-based systems have a great potential to mitigate Sybil attacks by the generation of multiple identities from an attacker to manipulate trust metrics, when two colluding nodes exchange dubious reputation information, Zhou et al. (2016) put forward an improved reputation system whereby nodes were allowed to exchange feedback about other nodes, depending on their interaction with them. Such a collaborative reputation model is indeed supposed to enhance detection accuracy further, but still, the malicious nodes would seek ways to manipulate reputation data.

C. Secure Routing Protocols

Secure routing protocols are designed to increase the efficacy of resilience against Gray-Hole attacks and facilitate the trustworthiness of the nodes that take part in the routing process for VANETs. Several protocols have been suggested for the protection of the two famous AODV and DSR routing protocols. Sharma et al., 2015 described a modification at AODV so as to ascertain Gray-Hole attacks against an improperly operating part of the protocol. Due to this alteration, a node is required to be put on careful observation for the censoring of packets while it is already informationally in possession of those packets for further forwarding, or terminate its routing. Such modification assists in identifying Gray Hole attackers before they perpetuate their harmful operations into the routing process. In 2014, Bhattacharyya et al. proposed a certain modification of the DSR protocol to counter Gray Hole attacks. Their proposition blocks non-trusted nodes during the route-finding operation; therefore, it diminishes the chances of making Gray-Hole attacks. This approach certainly tends to introduce another burden on communication as now-route validation is needed.

D. Multi-Path Routing

Multi-path routing, on the other hand, deals with forwarding data packets using several paths to enhance network resilience. This means that peering attacks of Gray- Holes could not stop the transmission toward the destination because the packets would be dropped along one path, and the other paths are likely to deliver the messages in the right direction. Santos et al. (2016) proposed a multi-path routing protocol that allows transmission over multiple disjoint paths. Along the entire route, a path is validated against a crosscheck of integrity as packets are forwarded along it. This way, the destructive nodes do not have any capability in jamming communication by dropping packets along only one path. The disadvantage of it is the additional overhead involved by the need to maintain and verify multiple paths concurrently in the network.

1) Collaborativedetection Mechanisms

Distributed Trust Models: In collaborative detection, there is mutual sharing of trust data, feedbacks, and behavior analysis of nodes with neighboring nodes for the collective detection of malicious behavior. Usually, distributed databases or peer-to-peer (P2P) networks are used for these sharing purposes. Data Aggregation: Nodes discuss information regarding the nature of behavior of other nodes and aggregate them in order to take decisions based on a good amount of data.

2) Machine Learning And Artificial Intelligence (Ai)

Anomaly Detection: ML algorithms are used in the form of SVM, decision trees, and neural networks. These algorithms learn normal and abnormal behavior patterns like selective packet dropping or malicious routing. This data is learned from network traffic over time with an improvement in the ability to identify Gray-Hole attacks. Reinforcement Learning: The essence of reinforcement learning in the case of adaptive security in VANETs is that it will learn to optimize the security parameters, such as attack thresholds and node behavior evaluation, relying on the ongoing observations and rewards from correct detection.

3) Cryptography

PKI is a special method of authentication offered in networking for confirming that nodes on the network are just the nodes that are supposed to be legitimate for participation in a routing process. Also, PKI prevents attacks on Gray-Hole since malicious nodes cannot masquerade as the legitimate ones in this case. Digital signatures are used primarily for integrity, to ensure that data has not been tampered with. A node forwarding a packet may sign it to authenticate itself and to ensure that attackers cannot modify it in mid-transmission. Cryptographic hash functions are being used in many secure routing protocols for detection of any changes in data and for ensuring data forwarded by nodes has not been altered.

4) Vehicular communication Technologies

Dedicated Short Range Communication (DSRC): DSRC is a vehicular communication medium developed for such applications as rain sensing, electronic toll collection, etc. It allows ultra-low latency information exchange causing most vehicular-to-vehicular and vehicular-to-infrastructure models of communication for real-time awareness of anomalous behaviors like Gray-Hole attacks. 5G and C-V2X: With the evolution of 5G connectivity and C-V2X, the most attention is drawn toward increased bandwidth, lesser latency, and improved reliability of communication related to vehicles. These technologies support real-time data dissemination for collaborative detection and mitigation of Gray-Hole attacks. Wi-Fi and Bluetooth: Wi-Fi or Bluetooth technologies are used in a short-range communication scheme among an unfortunate few car.

IV. PROPOSED SYSTEM

An integrated system combining multiple technologies and strategies is proposed for enhancing the safety of VANETs against Gray-Hole attacks. We will combine IDS, Reputation Management, Secure Routing Protocols, and mechanisms for Collaborative detection into one unique framework, making it more resilient to attacks while optimizing the use of network resources. The proposed system is designed to identify Gray-Hole attackers-sending nodes that selectively drop packets-by real-time monitoring, trust-based evaluations, and enhancements for secure routing. The system also allows mechanisms to work properly in the dynamic and mobile environment of VANETs without encountering significant overhead or performance degradation. Key Features of the Proposed System Dynamic Trust and Reputation System Intrusion Detection System (IDS) with Anomaly Detection Enhanced Secure Routing Protocol (AODV/DSR) Collaborative Detection Mechanism Adaptive Detection with Machine Learning Low-Overhead Multi-Path Routing

A. Dynamic Trust and Reputation System

Trust and reputation models are at the heart of identifying malicious nodes, especially Gray-Hole attackers, in a VANET. This proposed system employs a dynamic trust assessment mechanism based on packet forwarding node behaviors.

Trust Metrics: Each node will compute a trust score for its neighbors based on their past behavior, focusing on packet forwarding success rates and responsiveness to routing requests. Nodes that consistently drop packets (selectively drop certain packets while forwarding others) will have a lower trust score.

Adaptive Thresholds: These trust thresholds will be adaptive-they will change upon changing network conditions like mobility and density. False positives will be avoided as network conditions may sometimes cause loss of packets.

Reputation Sharing: Trust scores will be shared by neighboring nodes. Nodes can update and propagate trust values within their communication range, enabling them to detect Gray-Hole attacks based on collective data.

Sybil Attack Mitigation The system employs public-key cryptography (PKI) to authenticate nodes and their reputation data. Each node's identity will be validated by certificates issued by a trusted authority, and the update to their reputation will be signed digitally.

B. Ids With Anomaly Detection

An IDS will complement this reputation system by monitoring network traffic and detecting anomaly indicators of a Gray-Hole attack.

Packet forwarding monitoring: IDS will monitor packet forwarding behavior on each node and track dropped packets if these are being dropped at higher rates than normal. This will include the comparison of observed packet dropping behavior to baseline metrics for the detection of nodes that behave with selective packet dropping.

Anomaly Detection: The IDS will utilize machine learning to apply algorithms for example Support Vector Machines SVM or K-means clustering that detects abnormal packets that do not forward according to normal patterns. These models will be trained to recognize attack signatures and automatically classify behavior as normal or anomalous.

Collaborative IDS: The nodes will collaborate with each other by exchanging detection alerts to verify and improve the accuracy of the detection of attacks. Nodes with higher trust scores relied upon to a greater extent in the detection process.

C. Advanced Secure Routing Protocol (AODV / DSR)

The routing schemes, AODV and DSR, are thus prone to the Gray-Hole attack, which, in turn, involves the selective discard of packets by the malicious nodes in the route discovery and maintenance phases. The proposed system develops the protocols with enhanced security measures-Packet Forwarding Verification: A node will not pass on a packet toward a neighbor if it refused to forward it-up and thus, will be suspected and rejected from further consideration as a route. Route Integrity Validation: It will also check for integrity according to this protocol, where all nodes in the path can have trust values sufficiently above a pre-defined

TABLE:I Vanets Simulation Parameter

Parameter	Values
Area size	1000*1000
Nodes	100
Communication range	250 m
Mobility Model	Srinagar Highway
Simulation Time	900 seconds
Packet Transmission Parameters	512 bytes
Type of Traffic	CBR

threshold, any node with a low trust value will be suspected of being a Gray-Hole attack node and thus filtered from the routing table.

Security-Enhanced AODV/DSR: The protocols of the secure versions of AODV and DSR will encompass digital signatures for route authentication; all nodes participating in the route are authenticated by means of digital signatures. In such a case, only those nodes having authentic signatures will be utilized in route formation and maintenance.

D. Collaborative detection mechanism

The proposed system has a collaborative detection mechanism to enhance the accuracy and robustness of detection against Gray-Hole attacks, where nodes cooperate with each other. Feedback Exchange: Nodes exchange feedback about their experience with interactions from their neighboring nodes. A node that discovers it is being targeted by a neighbor node which persistently drops packets will disseminate a warning regarding the malicious node.

Voting Mechanism: A voting mechanism would be used to confirm the suspicious nodes. If independent nodes flag a node as malicious multiple times, it will be marked as a Gray-Hole attacker. This minimizes the chances of false alarms and ensures cooperation in the detection of malicious behaviors by the network.

Collaborative IDS: The collaborative detection system will also be integrated with the IDS. Nodes will cross-check the anomalies detected with neighboring nodes, thus increasing the overall accuracy of attack detection.

E. Adaptive Detection with Machine Learning

The proposed system uses machine learning (ML) to adaptively detect and respond to changing network conditions and attack patterns.

Fig:2 Architecture Diagram for Gray Hole Attack

Adaptive Detection Thresholds: It learns adaptively through reinforcement learning, adjusting the detection thresholds according to changes in the network conditions, such as mobility of nodes and network density. Under these varying conditions, this approach ensures that the system does not give too many false positives or negatives. Behavioral Prediction Machine learning models, especially in particular, supervised learning, predict future node behavior based on historical packet forwarding data. These would be trained to detect emergent Gray-Hole attack patterns for updating detection algorithms at run time.

F. Low Overhead Multi-Path Routing

To nullify the effects of Gray-Hole attacks, which rely on selective packet dropping, the proposed system incorporates multi-path routing to increase resilience. Multiple Routes: Unlike a single path, the system will send packets along multiple paths concurrently. If a Gray-Hole attacker disrupts one path by dropping packets, the other paths will ensure successful delivery. Route Selection: Multi-path routing algorithms will use trust-based metrics to select the most reliable paths for data transmission, minimizing the risk of relying on paths involving malicious nodes. Load Balancing: Multi-path routing also provides opportunities for load balancing across the network, reducing congestion and improving overall network performance.

V. SYSTEM ARCHITECTURE OVERVIEW

Node Communication: Each vehicle (node) communicates with other vehicles and infrastructure through DSRC or C-V2X communication technologies. Trust Management: The nodes dynamically compute and publish trust values based on the behavior of packet forwarding; neighbors are notified with trust information. IDS and Collaborative Detection: The IDS is monitoring the behavior of the packets forwarding to raise alerts. Nodes share feedbacks in peer-to-peer mode to collaborate to identify misbehavior. Secure Routing: The modified version of AODV/DSR is used so only trusted nodes are included within routing paths, and has cryptographic verification in addition to packet forwarding validation. Machine Learning and Adaptation: The system adapts the detection thresholds at runtime using real-time network conditions with the help of machine learning algorithms, continuously learning from data. Here is the detailed description of the simulation parameters for a DPGHA approach in

VANETs, using MATLAB and network simulators, or other custom MATLAB scripts. These parameters
will help you set up the simulation, evaluate performance, and compare those against any benchmark protocols**.**

VI. RESULT AND DISCUSSION

A simulation process on how to prevent a gray-hole attack (GHA) in vehicular ad-hoc networks using MATLAB will involve a step-by-step design of the simulation environment, attack implementation, and application of the dynamic prevention of gray-hole attack. Below is the broad outline of what one could do in MATLAB. Through MATLAB, one is further able to create and simulate VANETs and the possible network behaviors, which are

Let us discuss the simulation parameters for the approach of DPGHA against a gray-hole attack in VANETs with the help of MATLAB as well as network simulators like NS-2, SUMO, or custom MATLAB scripts. Such parameters will help you set up your simulation, evaluate performance, and compare the results against benchmark protocol

A. Performance Evaluation

The performance of the proposed DPGHA approach is assessed by comparing it to existing benchmark methods. To ensure a fair evaluation, the following performance metrics were considered: Routing Overhead. By focusing on this key metric, the study aims to quantify how efficiently the proposed approach manages the overhead associated with routing in the system. The comparison highlights the effectiveness of DPGHA in optimizing routing processes while minimizing additional communication costs, offering valuable insights into its practical applicability and advantages over traditional approaches. • Packet Delivery Ratio

- Throughput
- End-to-End Delay
- Packet Loss Ratio
- Detection Ratio

1) Routing Overhead

Routing overhead is defined as the number of Control packets (CPs) sent in comparison with the total number of Data packets (DPs) received at the destination end. The metric indicates the number of CPs required to send for a given the number of DPs. The major CPs of AODV routing protocol consist of RREQ, RREP, RERR (Route Error), and Hello messages.

$$ROH = \frac{\Sigma CP_{Transmitted}}{\Sigma DP_{Transmitted}} \quad \dots (1)$$

Increased overhead is measured. More number of RREPs will be desired routes to accommodate the increased number of malicious nodes in the network when routing overhead becomes very huge. More packets, due to a large number of malicious nodes, hence leads to loss more in conventional AODV. Hence average routing overhead of traditional AODV is about 5508.33.

2) Packet Delivery Ratio (PDR)

The PDR is referred to the ratio of the total number of Number of data packets sent by the source node to the total number of data packets received by the destination node. Calculated by

$$PDR = \left(\frac{\Sigma DP_{Received}}{\Sigma DP_{Sent}}\right) * 100 \quad \dots (2)$$

Fig 3: Comparison of throughput

Fig 4: End To End Delay

VII. CONCLUSION

This proposed framework for Enhanced Security Framework for Gray-Hole Attack Prevention in VANETs provides a comprehensive and adaptive solution in the endeavor to tackle one of the most subtle and disruptive security threats in VANETs. The proposed framework is comprehensive, taking into account the various layers and security mechanisms: multiple layers of Intrusion Detection Systems (IDS), Trust and Reputation Management, Collaborative Detection, Secure Routing Protocols, and Machine Learning-based Adaptation, providing a strong defense against Gray-Hole attacks while maintaining efficiency and scalability in dynamic and high-mobility environments. Gray-Hole Intruders would be caught in the early stages through continuous monitoring and real-time analysis of packet forwarding behavior. IDS work effectively even in highly dynamic and large-scale VANETs. Prevention from Reputation-Based System: The framework reduces the dependency on any single node, and then by having a distributed trust and reputation management system, it makes the attack difficult and unnoticed to the attackers. Collaborative Defense: This framework improves detection since nodes can be in cooperation to exchange feedback for the identification of malicious behavior, thus ensuring higher accuracy and reliability in detecting Gray-Hole attacks. Adaptive Security: The system introduces machine learning to allow dynamic adjustments of detection thresholds by updating corresponding changes in attack patterns and network conditions to continuously improve protection against emerging and new threats. Efficient Routing: The advanced routing protocols with security mechanisms, such as AODV/DSR, will ensure that only trusted nodes take part in the forwarding of packets. This reduces the risks due to malicious nodes. Scalability and Flexibility: It is scalable to the VANETs growth and accordingly adaptable to diverse topologies and mobility patterns; thus, it is suitable for large and changing networks of vehicles constantly. Conclusion The Enhanced Security Framework has enhanced significantly the security posture of VANETs against Gray-Hole attacks. As a result of the integration of detection, prevention, and adaptive learning, vehicular communication systems will remain resolute, reliable, and secure in the real-world environment. More complex mechanisms can be further developed concerning the security requirements of VANETs, ensuring safe and efficient vehicular communications in the future.

VIII. FUTURE ENHANCEMENT

A. Integration with Blockchain for Trust Management

Others may evolve into integrated blockchain systems in the future for leveraging the Trust and Reputation Management system even better. A Decentralized Trust Ledger: Using a blockchain-based ledger for reputation scores of nodes tampered-proof and transparent can prevent manipulation of the trust system through an attacker to alter the reputation scores. Security with Smart Contracts: Security policies can be executed through blockchain-supported smart contracts. An example of this is the automatic exclusion of malicious nodes from the network or initiation of pre-programmed countermeasures when the occurrence of Gray-Hole attacks is detected. Benefits- Increased transparency and immutability in trust management. A better resisting-protection against Sybil and other trust-based attacks.

REFERENCES

[1] Rasheed Hussain, Fatima Hussain, Sherali Zeadally "*Integration of VANET and 5G Security: A review of design and implementation issues*" Elsevier Future Generation Computer Systems (Volume 101, December 2019).

[2] Xiaobo Wang; Yu Weng; Honghao Gao "*A Low-Latency and Energy-Efficient Multimeric Routing Protocol Based on Network Connectivity in VANET Communication*" IEEE Transactions on Green Communications and Networking (Volume: 5, Issue: 4, December 2021).

[3] Maryam Gillani, Hafiz Adnan Niaz, Muhammad Umar Farooq, Ata Ullah "*Data collection protocols for VANETs: a survey*" Springer Nature - Complex & Intelligent Systems (Volume 8, January 2022).

[4] S Vimalnath, G Ravi (2020) "*Optimized Geographic Routing in Mobile Ad Hoc Network using Bees Swarm Optimization*", Journal of Scientific & Industrial Research, Publishe: NISCAIR-CSI,Vol. 79, pp. 727-729.

[5] Abdul Malik, Muhammad Zahid Khan, Saeed Mian Qaisar, Mohammad Faisal, Gulzar Mehmood "*An Efficient Approach for the Detection and Prevention of Gray-Hole Attacks in VANETs*" IEEE Access (Volume: 11, 09 May 2023).

[6] Pooja Rani, Kavita, Sahil Verma, Gia Nhu Nguyen "*Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network*" IEEE Access (Volume: 8, 25 June 2020).

[7] Vimalnath. S, Ravi. G., (2020). "*Optimized Geographic Routing in Mobile Ad Hoc Network Using Gray Wolf Optimization,*" EAI endorsed transaction. (Research Article-EAI.EU).

[8] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, Joarder Kamruzzaman "*Survey of intrusion detection systems: techniques, datasets and challenges*" Springer Nature - Cybersecurity (Volume 2, article number 20, July 2019).

[9] Dr. T. Ananth Kumar1, A. Devi1, N. Padmapriya, S. Jayalakshmi1, P. Divya "*A Survey on Advance Black/Grey hole Detection and Prevention Techniques in DSR & AODV Protocols*" International Journal on Wireless, Networking & Mobile Communication Innovations (Volume 5, Issue 1 – 2021) ISSN: 2581-5113.

[10] Jeong-Kyu Bae, Myung-Chul Park, Eun-Ju Yang; Dae-Wha Seo "*Implementation and Performance Evaluation for DSRC-Based Vehicular Communication System*" IEEE Access (Volume: 9, 14 December 2020).

[11] Gurtej Kaur, Meenu Khurana, Amandeep Kaur "*VANET Cluster Based Gray Hole Attack Detection and Prevention*" Springer Nature – Computer Science (Volume 5, article number 186, January 2024).

[12] Vimalnath, M. S., Priyanka, S., & Sandhiya, M. (2020). "*Vehicle as vehicular networks for big data transfer between data centers in ICF".* (2020) International Research Journal of Engineering and Technology (IRJET), (e-ISSN: 2395-0056).

[13] Thabiso N. Khosa, Topside E. Mathonsi, and Deon P. Du Plessis "*A Model to Prevent Gray Hole Attack in Mobile Ad-Hoc Networks*" Journal of Advances in Information Technology, (Volume 14, No. 3, 2023).

[14] Kaoutar Ourouss, Najib Naja, Abdellah Jamali "*Defending Against Smart Gray hole Attack Within MANETs: A Reputation-Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol*" Springer Nature - Wireless Personal Communications (Volume 116, January 2020).

[15] Usama Arshad, Munam Ali Shah, Nadeem Javaid "*Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture*" Science Direct - Vehicular Communications (Volume 31, October 2021).

[16] Sparsh Sharma, Ajay Kaul "*VANETs Cloud: Architecture, Applications, Challenges, and Issues*" Springer Nature - Archives of Computational Methods in Engineering (Volume 28, June 2021).

DVD ISBN: 979-8-3315-2138-7

https://icvadv.com/

Certificate of Presentation

Presented to

Dr. S Vimalnath

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Midhun R

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Kavinesh A S

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Karvendan P

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Kishore K

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.