**ABSTRACT**

The  Vehicular Ad hoc Network(VANETs) has a greater significance in Vehicle to Vehicle Communication without relaying much on the Infrastructure.Though they are used in variety of applications they are vulnerable to attacks.In this proposed approach we have to detect greedy nodes  by incorporating various metrics like Number of times the node makes an Attempt, Connection Duration , Waiting time, Packet Delivery Ratio and Average Delay. These metrics are used by the benign nodes to learn more about malicious node behavior.In order to detect greedys nodes our proposed model has two phases namely Uncertainty  State and Resolution State .The Uncertainty  State is based on linear regression concept and Resolution state is based on Fuzzy Logic Scheme.The effectiveness of our approach is proved by extensive simulations. This proposed work can be applicable for variety of applications as they provide high level of trustworthiness by detecting greedy nodes in the network

i

**LIST OF ABBREVIATIONS**

* VANETs 🡪Vehicular Ad hoc Networks
* DOS 🡪Denial of Service
* WLAN 🡪Wireless LAN
* MANETs 🡪Mobile Ad hoc Networks
* GDVAN 🡪Greedy Detection for VANETs
* EDCA 🡪Enhanced Distributed Channel Access
* DCF 🡪Distributed Coordination Function
* CCH🡪Control Channel
* SCH🡪Service Channels
* DSRC 🡪Dedicated Short Range Communication
* WAVE 🡪Wireless Access in Vehicular Environments
* CSMA/CA 🡪Carrier Sense Multiple Access with Collision Avoidance
* AC🡪Access Categories
* BK🡪Background traffic
* BE🡪Best Effort traffic
* VI🡪Video traffic
* VO🡪Voice traffic
* AIFS 🡪Arbitration Inter-Frame Space
* CW🡪Contention window
* FLSAC 🡪Fuzzy Logic based Scheme to Struggle Against Adaptive

Cheaters

* WIBSS🡪Wave Independent Basic Service Set

**ii**

**LIST OF SYMBOLS:**

* T 🡪 Monitoring period
* N 🡪 Total number of vehicles
* TCA 🡪 Connections attempts during T.
* TCD 🡪 Total connections duration of all vehicles during T.
* P1nca 🡪First Threshold of connection attempts .
* P2nca 🡪Second Threshold of connection attempts.
* P1cd 🡪First Threshold of connection duration.
* P2cd 🡪Second Threshold of connection duration.
* P1wtbc 🡪 First Threshold of waiting times
* P2wtbc 🡪Threshold of waiting times between connections
* V1 🡪 Number of connections attempts.
* V2 🡪 Connection duration.
* V3 🡪 Average of waiting times between connections.

**iii**

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| FIGURE NUMBER: | FIGURE NAME | PAGE NO: |
| 1 | Wireless Adhoc Networks | 2 |
| 2 | Fuzzy Logic Based Decision Scheme | 16 |
| 3 | The Proposed Detection Algorithm | 16 |
| 4 | Wireless Network Setup | 17 |
| 5 | Calculation of Connection Attempt, Connection Duration And  Waiting Time | 17 |
| 6 | Fuzzy Control | 17 |
| 7 | Data Transmission | 45 |
| 8 | Malicious Node | 46 |
| 9 | Connection Duration | 47 |
| 10 | Detection Result | 47 |
| 11 | Behavior of Node | 48 |
| 12 | Comparison Result | 48 |

iv

**1.INTRODUCTION**

* 1. **Aim**

The aim of the project is to detect and identify the greedy nodes in

Vehicular ad-hoc networks(VANETs).

* 1. **Objective**
* Data plane of ad-hoc network suffer from greedy node.To Overcome the security problem the suspicious phase and decision are implemented to detect greedy node
* The availability of greedy node is calculated by using linear regression concept
* The behavior of node is detected by using fuzzy logic.
  1. **Wireless Adhoc-Network**

The word ―ad hoc‖ comes from Latin. Language which means ‗for this purpose only‘, Ad hoc Networks are the small area networks, especially designed with Wireless/Temporary connections to the different computer assisted nodes. Basically, an ad hoc network is the temporary network connections made to the information transferring purpose, so hence if the networks are designed for longer period connections then it acts as plain old network connections.

* + 1. **An overview of Wireless Adhoc Networks**

A mobile ad hoc network is a collection of mobile nodes forming an ad hoc network without the assistance of any centralized structures. These networks introduce a new art of network establishment [Das 2000, Jinyang2000] and can be well suited for an environment where either the infrastructure is lost or where an infrastructure is not very cost effective. The whole life-cycle of ad hoc networks could be categorized into the first, second, and the third generation ad hoc network systems. Present ad hoc networks systems are considered to be the third generation

A Wireless ad hoc network is a collection of heterogeneous network node forming the temporary networks without the aid of any infrastructure or any centralized administrator. In such an environment, it may be necessary for one wireless host to enlist the aid of other hosts in forwarding a packet to its destination; this is because of the limited range of each wireless host‘s transmission. Wireless ad hoc networks (WANETs) Figure 1.0 do not rely on any fixed infrastructure but communicate in a self-organized way.



Fig 1:Wireless Adhoc Networks

The above figure 1depicts the information about the different kind of application of WANETs. As the number of applications of wireless ad hoc network grows, the size of the network varies greatly from a network of several mobile computers in a classroom, to a network of thousands of mobile units deployed in a battle field. The variability in the network size is also true for a particular network over the course of time; a network of a thousand nodes may be split into a number of smaller networks of a few hundred nodes or vice versa, as the nodes dynamically move around a deployed area.

**1.3.2 Wireless Communication Characteristics**

**a) User Mobility:** Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the organization. The Wireless users are provided with access to the real time information even when they are away from their home/offices and even from their society.

**b) Rapid Installation:** The time required for installation is reduced as network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or by making modifications to the infrastructure cable plant.

**c) Flexibility:** Enterprises can also enjoy themselves the flexibility of installing and taking down wireless devices in locations as necessary. Users can quickly install small wireless devices for temporary needs such as a conference, trade show, or standards meeting. The Wireless users are provided with access to the real time information even when they are away from their nativity.

**d) Scalability:** Wireless network topologies can easily be configured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming in a broader area. Wireless networks offer more and adapt easily to changes in the configurations of the networks.

**e) Cost:** Networks can be extended at any level with limited cost or almost no cost, as this facility is not available with wired system and hence setting up a wireless networks are so much easy and fast that it eliminates the need for pulling out the cable through walls and ceilings

* + 1. **Attacks :**

**Attacks** are an attempt to have control over the security of any system or organizations. The attack may alter, release, or deny data. The success of an attack depends on the vulnerability, and the effectiveness of existing technology. Examples of attacks include actions such as spoofing, obtaining illegitimate privileges, inserting false information, modifying information, analyzing and modifying network routes, obtaining illegitimate access to systems through social engineering, or disrupting network operation using malicious software. Although the attacks are of many categories but the every concerns with two main categories of Attacks on Wireless ad hoc Networks []. Hence we divides them into two main categories:

a) **Passive Attacks:** In such types of attack an attacker passively listens to the packet or a listener is just the wireless medium by sniffing the mode of route. Since an attacker only listens to the packets that are passing by without modifying or tampering with the packets, these attacks mainly target the confidentiality attributes. Typically such kind attacks are much easier to launch than the next type of attacks.

b) **Active Attacks:** such type of active attacks are those attacks where the attacker takes malicious action in addition to passively listening to on-going route. For example an attacker might choose to modify packets, inject packets, or even disrupt network services. Ad hoc networks that make extensive use of wireless links are vulnerable to several types of attack due to the inherent nature of the network.

Hence some technical thoughts of mechanisms such as encryption and authentication can greatly mask the vulnerabilities on the wireless communications, but these are not the only insufficient but also vulnerabilities in ad hoc networks. Since wireless ad hoc networks cannot depend upon infrastructure-based resources or centralized form of resource, such as stable power source, high bandwidth, continuous connectivity, or fixed routing, so it become more easy to launch attacks on them.

**1.3.4 Applications of Wireless ad hoc Networks**

* Tactical Networks
* Military Communications and operations controls in the battle field environment
* Sensor Networks
* Collections of embedded sensor devices used to collect real time information to automate every functions of the system.
* Weather Monitoring.
* Earth movement sensing activities
* Ocean Engineering or well known as Underwater Sensor Networks
* Emergency Services
* Search and rescue operations and disaster recovery.
* Patient record retrieval system.
* Catastrophic disaster.
* Commercial Environment
* E-Commerce and online bill payment system
* Access the customer records from the fields
* Vehicular ad hoc Networks system.
* Educational Applications
* Video conferencing system and Virtual class room system
* Entertainment Applications
* Video on demand
* Other Applications
* Cellular Phone
* Bluetooth System

**2.LITERATURE STUDY**

The literature study is organized into several different sections. These sections explore about the attacks and defenses in the data plane of ad-hoc networks. Fuzzy trust evaluation and credibility development in multi-agent systems.

**2.1 Attacks and Defenses In The data Plane of Networks**

In [1] Security issues in computer networks have focused on attacks on end-systems and the control plane. An entirely new class of emerging network attacks aims at the data plane of the network. Data plane forwarding in network routers has traditionally been implemented with custom-logic hardware, but recent router designs increasingly use software programmable network processors for packet forwarding. These general purpose processing devices exhibit software vulnerabilities and are susceptible to attacks.

The attack that exploits vulnerability in packet processing software to launch a devastating Denial-of-Service attack from within the network infrastructure. This attack uses only a single attack packet to consume the full link bandwidth of the router’s outgoing link.

The hardware based defenses mechanism that can detect situations where malicious packets try to change the operation of the network processor. A recovery system can restore the network processor to a safe state within six cycles. This high-speed detection and recovery system can ensure that network processors can be protected effectively and efficiently from this new class of attacks.s

**2.2 Survey on VANET security challenges and possible cryptographic solutions**

In[4]VANET is an emergent technology with promising future as well as great challenges especially in its security. In this paper, VANET security frameworks presented on three parts. The first presents an extensive overview of VANET security characteristics and challenges as well as requirements. The second focuses on a novel classification of the different attacks known in the VANET literature and their related solutions. The third is a comparison between some of these solutions based on well-known security criteria in VANET.In this paper, they have specified certain research challenges and open questions which may be future research directions. Thus enable VANET to efficiently implement a system for trusting vehicles and protect it from any malicious node.

**2.3 Performance analysis of the conﬁdant protocol**

In [6]the CONFIDANT protocol works as an extension to a reactive source-routing protocol for mobile adhoc networks. Mobile ad-hoc networking works properly only if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. We propose a protocol, called CONFIDANT, for making misbehaviour unattractive; it is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behaviour of other nodes. The detailed implementation of CONFIDANT in this paper assumes that the network layer is based on the Dynamic Source Routing (DSR) protocol. We present a performance analysis of DSR fortified by CONFIDANT and compare it to regular defenceless DSR. It shows that a network with CONFIDANT and up to 60% of misbehaving nodes behaves almost as well as a benign network, in sharp contrast to a defenseless network.

**2.4 Detecting greedy behaviors by linear regression in wireless ad hoc networks**

In [8], the greedy behavior of some misbehaving nodes can try to lower their waiting time in order to access the channel earlier and penalize the other nodes. In order to avoid this misbehavior.The model based on measuring the linear regression of nodes access time to the channel. This result has been also confirmed by simulations. In this , each deviation from the estimated slope is considered as a source of cheating from a corresponding node.the presence of correlation between the different access times to the channel of nodes in order to detect the cheaters in IEEE 802.11 DCF MAC layer for ad hoc networks. The correlation is defined here as a measure of the association between two random variables.

**2.5 Fuzzy Control**

In [10]Fuzzy control is a practical alternative for a variety of challenging control applications since it provides a convenient method for constructing nonlinear controllers via the use of heuristic information.Fuzzy control provides a user-friendly formalism for representing and implementing the ideas we have about how to achieve high-performance control.Fuzzy control provides a formal methodology for representing, manipulating, and implementing a human’s heuristic knowledge about how to control a system.The fuzzy controller is to be designed to automate how a human expert who is successful at this task would control the system

**3.SYSTEM STUDY**

**3.1 Scope:**

The scope of the project is to detect and identify the greedy node in Vehicular ad-hoc networks.

**3.2 Novelty**

* Compared with existing model the implementation model is able to detect the greedy nodes in high mobility, increasing bandwidth.
* Benefiting from the flexibility of fuzzy reasoning in ex-tending and adapting empirical rules, the evaluation result could be more objective.
  1. **Procedure**
     + - The first step in the system is to creating the wireless network setup.
       - Generating the node movements in the network.
       - Introducing the malicious nodes in the simulated network.
       - Calculating 3 parameter.Behaviour of node is based on these parameter.
       - Based on fuzzy rule we can determine the node is greedy or not.
  2. **Proposed Algorithm**
* Collete the trace file by creating node in NS2.Trace file consist,time,node id,paket id,port address,IP address,from node,to node.We going to use from node,to node,time only.
* Using time we calculate Connection Duration,Average Waiting time,Connection Attempt using AWK file.
* In first step,calculating the correlation coefficient .If the coefficient is closer to 1,calculate the slope of linear straight.If slope close to 1 then presence of greedy is nil.If coefficient not close to 1,greedy is persent in network.so we determine the malicious node.
* Next,we generate fuzzy rule for each parameter for making the decision .Output of the fuzzy rules are low or medium or high.Now we have 3 file.
* Then , generate class rule for those 3 file .After generating class rule we got output as normal or greedy or suspected.
* Calculate crisp value.If value is greater than 50% and then output of class rule is greedy ,then node is greedy.If class output is suspected then node is suspeted.else the node is normal.

**3.5 System Requirements**

The Software and hardware requirements of the system are as follows.

**3.5.1 Hardware Requirements**

* Intel Core i3 preprocessor @ 1.90GHZ
* 4 GB RAM
* 400 GB Hard Disk

**3.5.2 Software Requirements**

* Linux 3.0.7
* NS2

**3.6 Technology Used**

**3.6.1 NS2**

NS is an event driven network simulator developed at UC Berkeley that simulates variety of IP networks. It implements network protocol such as TCP and UDP, traffic sources behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ routing algorithm such as Dijkstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations.

The NS project is now the part of the VINT project that develops tools for simulation results display, analysis and converters that convert network topologies generated by well-known generators to NS formats. Currently, NS (Version 2) written in C++ and OTcl (Tcl script language with Object-Oriented extensions developed at MIT) is available.

NS is written not only Otcl but in C++ also. For efficiency reason, NS separates the data path implementation from control path implementation. In order to reduce packet and event processing time (not simulation time), the event scheduler and the basic network component objects in the data path are written and compiled using C++. These compiled object are made available to the Otcl interpreter through an Otcl linkage that creates a matching Otcl object for each of the C++ objects and makes the control function and the configurable variable specified by the C++ object act as member function and member variables of the corresponding Otcl object.In this way, the controls of the C++ objects are given to OTcl. It is also possible to add member functions and variables to a C++ linked to OTcl object.

When a simulation data finished, NS produces one or more text-based output files that contain detailed simulation data,if specified to do so in the input Tcl(or more specifically, OTcl) script. The data can be used for stimulation analysis or as input to a graphical stimulation display to called Network Animator(NAM) that is developed as a part of VINT project.NAM has a nice graphical user interface similar to that of a CD-player(play, fast forward,rewind,pause and so on),and also has a display speed controller.

**File Name:**

File name must have the extension “.tcl”.

**Running The Program:**

The command for running the tcl program is “ns filename.tcl”

**3.6.2 C++:**

C with Classes was renamed to "C++" (++ being the increment operator in C), adding new features that included virtual functions, function name and operator overloading, references, constants, type-safe free-store memory allocation (new/delete), improved type checking, and BCPL style single-line comments with two forward slashes (//). Furthermore, it included the development of a standalone compiler for C++, Cfront.  The C++ Programming Language was released, which became the definitive reference for the language, as there was not yet an official standard. The C++11 standard was released, adding numerous new features, enlarging the standard library further, and providing more facilities to C++ programmers. After a minor C++14 updated.

The C++ language has two main components: a direct mapping of hardware features provided primarily by the C subset, and zero-overhead abstractions based on those mappings. Stroustrup describes C++ as "a light-weight abstraction programming language [designed] for building and using efficient and elegant abstractions";[[6]](https://en.wikipedia.org/wiki/C%2B%2B#cite_note-Stroustrup1-6) and "offering both hardware access and abstraction is the basis of C++.

C++ supports four types of memory management: static storage duration objects, thread storage duration objects, automatic storage duration objects, and dynamic storage duration objects Static storage duration objects are initialized in two phases. First, "static initialization" is performed, and only after all static initialization is performed, "dynamic initialization" is performed. In static initialization, all objects are first initialized with zeros. Variables of this type are very similar to static storage duration objects. The main difference is the creation time is just prior to thread creation and destruction is done after the thread has been joined.

C++ templates enable generic programming similar to generics in Java. C++ supports function, class, alias and variable templates. Templates may be parameterized by types, compile-time constants, and other templates. Templates are implemented by instantiation at compile-time. Templates are different from macros while both of these compile-time language features enable conditional compilation, templates are not restricted to lexical substitution. Templates are aware of the semantics and type system of their companion language, as well as all compile-time type definitions, and can perform high-level operations including programmatic flow control based on evaluation of strictly type-checked parameters.

**FILE NAME:**

File name must have the extension “.cpp”.

**Running The Program:**

The command for running the c++ program is “c++ filename.cpp”

**3.6.3 AWK SCRIPT:**

AWK is a programming language designed for text processing and typically used as a data extraction and reporting tool. It is a standard feature of most Unix-like operating systems. The AWK language is a data-driven scripting language consisting of a set of actions to be taken against streams of textual data – either run directly on files or used as part of a pipeline – for purposes of extracting or transforming text, such as producing formatted reports. The language extensively uses the string datatype, association arrays (that is, arrays indexed by key strings), and regular expression.

AWK is a language for processing text files. A file is treated as a sequence of records, and by default each line is a record. Each line is broken up into a sequence of fields, so we can think of the first word in a line as the first field, the second word as the second field, and so on. An AWK program is a sequence of pattern-action statements. AWK reads the input a line at a time. A line is scanned for each pattern in the program, and for each pattern that matches, the associated action is executed.

Variable names can use any of the characters [A-Za-z0-9\_], with the exception of language keywords. The operators *+ - \* /* represent addition, subtraction, multiplication, and division, respectively. For string concatenation, simply place two variables (or string constants) next to each other. It is optional to use a space in between if string constants are involved, but two variable names placed adjacent to each other require a space in between. Double quotes delimit string constants. Statements need not end with semicolons. Finally, comments can be added to programs by using *#* as the first character on a line.

**File Name:**

File name must have the extension “.awk”.

**Running The Program:**

The command for running the awk program is “awk -f my.awk life.csv >output.txt”

**4.DESIGN**

**4.1 System Architecture**

**4.1.1 Detecting the Greedy Node**



Fig 2: Fuzzy logic based decision scheme

**4.1.2 Detection Algorithm**

****

**Fig 3:The Proposed Detection Algorithm**

**4.2 PROJECT FLOW**

This section contains overall flow of proposed system

**4.2.1** Wireless Network Setup**:**

**C:\Users\TEMP.it-mml042.003\Downloads\wns.jpg**

**Fig 4: Wireless Network Setup**

**4.2.2** Calculation of Connection Attempt, Connection Duration, Waiting Time.

**C:\Users\TEMP.it-mml042.003\Downloads\wns (1).jpg**

**Fig 5: Calculation of Connection Attempt, Connection Duration, Waiting Time.**

**4.2.3** Fuzzy Logic

**C:\Users\TEMP.it-mml042.003\Downloads\wns (2).jpg**

**Fig 6.Fuzzy Control**

**7. CONCLUSION AND FUTURE WORK**

**7.1 Conclusion**

The greedy behaviour detection method was proposed for securing the data plane of adhoc network .Fuzzy logic is employed to find the behaviour of the node, which is able to formulate the imprecision of empirical knowledge and is suitable for distributed network. AODV framework demonstrate that the implementation detecting the greedy behaviour system is flexible and easy.

**7.2 FUTURE ENHANCEMENT**

The proposed approach will be extended by considering extra parameter for detecting the greedy node and thereby accuracy of the greedy node detection in precision manner.