Impersonation Attack Detection in VANET Using Kalman Filter and Watermarking

Academic Internship
MSc Cyber Security

Dinesh Kumar Jagadeesan
Student ID: x18170064

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Dinesh Kumar Jagadeesan
Student ID:	x18170064
Programme:	MSc Cyber Security
Year:	2019
Module:	Academic Internship
Supervisor:	Imran Khan
Submission Due Date:	12/12/2019
Project Title:	Impersonation Attack Detection in VANET Using Kalman Filter and Watermarking
Word Count:	6396
Page Count:	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	12th December 2019

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Impersonation Attack Detection in VANET Using Kalman Filter and Watermarking

Dinesh Kumar Jagadeesan
x18170064

Abstract

VANET is a Vehicular ad-hoc Network where short rage network is formed among the VANET node. VANET nodes is to connect and share messages with other network nodes in infrastructure or infrastructure less network. Due to absence of secure infrastructure, VANET is prone to wide-ranging attacks. In Impersonation attack, attacker can easily capture the origin node. Attacker breach will impact on integrity, confidentiality and authenticity. In this paper, establishing a secure connection in VANET using Kalman filter against impersonation attack by detecting accurate position of the legitimate node. Watermarking is used to secure the data during the communication in the network. The proposed scheme is analyzed using metrices like node detection, SNR, PDR, delay. Once the false node is found, it will be isolated from other networks in the environment. These protocol aims to protect VANET against impersonation attack.

Keywords: VANET, Kalman Filter, Watermarking, Impersonation attack

1 Introduction

Wireless technology plays a key role in the modern world. The demand for wireless technology increased day by day by having an enormous number of users. In this wireless technology, VANET (Vehicular ad-hoc Network) is derived from MANET along with In-Vanet and iMANET. VANET is an Adhoc network, deployed in the communication for safety enhancement in driving. VANET is one of the innovative technologies which inherits with new wireless networks on vehicles Panichpapiboon and Pattara-Atikom (2011). In the middle of the 2000s, the study about VANET gradually increased and it reaches a peak in 2007. VANET takes over all the noticed and unnoticed security and confidentiality exposures associated with MANETs. It works with two types of components are a roadside unit (RSU) and Onboard Unit (OBU). The main three properties need to be satisfied are confidentiality, integrity, and availability.[La and Cavalli (2014)]

VANET is established with the security and efficiency in the network over traffic management which establishes a connection with all nodes automatically without any prior knowledge of the user [1]. VANET is efficient to provide security over roadside communications with all vehicles over inefficient infrastructure. Kaur et al. (2018).VANET is much better than MANET even it is the subclass of MANET in few cases like Network disconnected frequently, fast topology changes, battery capabilities, communication atmosphere, and mobility.[Rawat et al. (2012)]

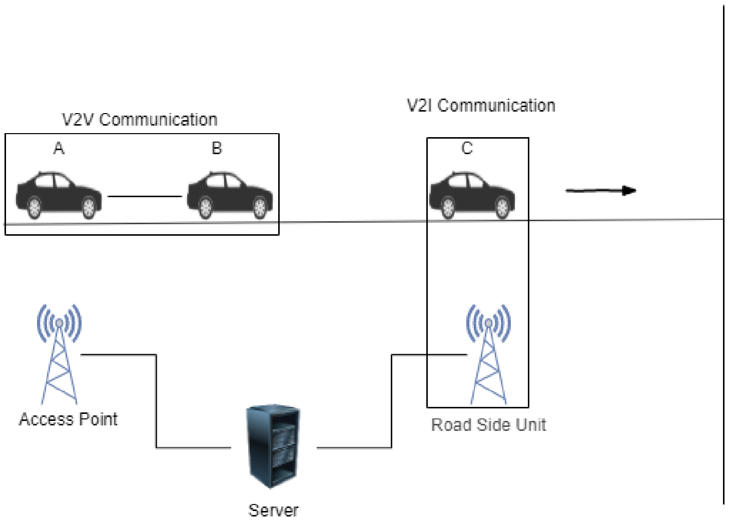

Figure 1: Basic VANET network

VANET has the potential to communicate warning messages to the user over natural hazards, traffic and road conditions which work on two entities are access points and wireless communication between vehicles V2V and infrastructure V2IPanichpapiboon and Pattara-Atikom (2011). There are few routing protocols are described as Ad-hoc, Beacon, overlay, geocast based, cluster-based, and broadcast-based which has both pros and cons based on their working functions. The attacks were executed by the insider was more when compared to the outsider. The VANET is described with few applications over safety and traffic monitoring over to avoid the collision, public safety, information from other vehicles, vehicle diagnostics with more objectives.

The security requirements in VANET are authentication, message nonrepudiation, access control, and privacy. In the meantime, there are few security issues in vanet over attackers can easily attack over the network, fast-moving network topology required to eliminate false positive messages over the network, session hijacking during setting up connection leads the user at risk. To prevent the vehicle from the security attack along with the IDS system for making the user alert Rawat et al. (2012)]. Even the technology grows, the vulnerability over the system are increasing and makes the attacker to invade loopholes in the technology. The security requirements for VANET is to protect the network and improve the privacy of the information to reduce its vulnerability for attacks. There are few familiar challenges in VANET are:

- Mobility
- Instability
- Network Adaptability
- Fast change in Topology
- Security and Privacy

After discussing in detail about VANET on their pros and cons. Security issue plays a significant role in Vehicle communication. VANET is vulnerable to several types of security attacks. They are listed below:

SYBIL ATTACK:

One vehicle pretended itself to be in distinct positions at the same time to create a security risk in the network. Attacker steals the identity of the vehicle and interrupt the functions providing false information to another legitimate user in the network.

BOGUS INFORMATION:

The attacker sends incorrect information for its own benefit. The attacker will isolate the node in the network, and it will not create a severe impact in-network because of fast topology. At times, the data sent by an attacker will not affect much in the network.

DENIAL OF SERVICES (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS):

The legitimate user cannot able to use services provided into the network. The attackers transmit false messages to block the services in the network and to reduce the efficiency of the network. The RSU and OBU cannot communicate properly to provide the services upon the request sent in the large amount. DOS attack is to target one node and sent many request. DDOS is sending multiple request to a particular vehicle from different vehicles to disable the service.

GPS SPOOGING ATTACK:

In this attack, the attacker tries to modify the current location and update the GPS system with fake location information using such a technique to hide his current location in the network. This makes the legitimate user gets confused and it could be done through multiple vehicles or single vehicles.

BLACK HOLE ATTACK:

The attacker changes the routing function for finding the shortest path. The legitimate user will use the wrong path modified by the attacker and stuck in the middle. The attacker breaks the availability security function and it has a high impact over the network. Among the above attacks in VANET, impersonation attack has a key role in security issues since it produces high impact of sending a false message which makes the individual to get into a trap or do not reach his/her destination.

IMPERSONATION ATTACK:

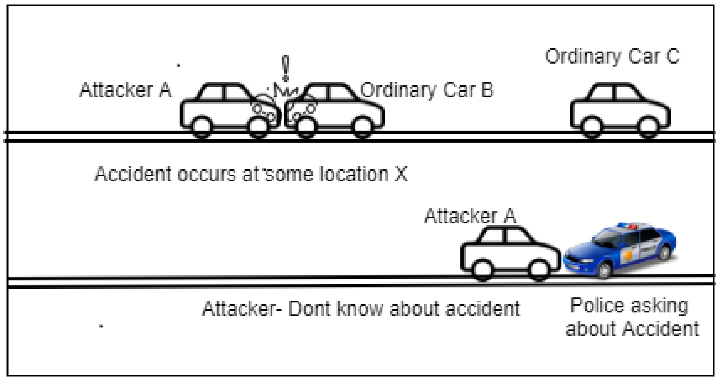
Attacker A
Ordinary Car B
Ordinary Car C
Accident occurs at some location X
Attacker A
Attacker- Dont know about accident
Police asking about Accident

Figure 2: Impersonation attack image

In wireless communication, each node communicates with each other based on the range and their functions. In VANET, each vehicle has a unique id and IP address, it is much more important when accident occurs. The attacker steals their MAC and IP address to corrupt the network and communicates with the legitimate user by sending false information by updating packets for his convenient. In a short-range network, an Impersonation attack occurs in the transport layer and physical layer most of the time. It will not seriously affect the user communication, but the integrity of data is broken by the attacker during the communication which reduces the ability and quality of the wireless communication.

Such that the to protect the vehicle and secure the communication, we need an effective detection system in VANET. Kalman filter is one of the improved methods to detect the impersonation attack by measuring trust estimate values and watermarking to secure the packet's data while communicating with each other. Kalman filter is used to detect the exact location of the vehicle. The upcoming section is about discussing in detail the work done previously to detect and prevent the impersonation attack secure the communication between the vehicles in VANET.

1.1 Research Question

The question raised to develop my research in VANET by comparing the existing method:

- Is it possible to improve the detection system in VANET from impersonation attack?
- How to secure the data from the attacker even when the attacker get access?

The papers related to existing proposal used different technique like bloom filter, buck filter, authentication factor to detect attack in VANET. In the existing method, the detection of impersonation attack was done by trust estimate during communication. They used Buck filter to spread beacons signals in a short range with (100-200ms). The existing method can predict the node location with low bacons.

In the proposed method, Kalman filter works in linear measurement which has capability to predict the node location in the network. There are two suggests of hygenberg [24] which declares that two vehicles cannot occupy the same space at the same time and one vehicle can occupy only one space at a given time. The proposed scheme predicts the neighbor vehicle presence using Kalman gain and verify each vehicles identity (i.e. MAC address, IP address). Authentication is done through watermarking technique to secure the packets by hashing the data with SHA-1 encryption method. A city scenario is taken with 4 RSU unit 24 vehicles and it is further analyzed based on various matrices.

2 Related Work

2.1 Methods available to secure the transmission of data in VANET

Yılmaz and Arslan (2013) has discussed identifying impersonation attacks in wireless communication for the safety and security of the information transmission. Since the wireless technique has an increasing demand for its reliability and advantage with the ease of working and structural installation. The better solution lies with the secured media access control (MAC) by end-to-end encryption. The physical layer security focuses on eavesdropping, jamming, impersonation. In the case of impersonation, these activity of spoofing can be detected by using the hypothesis test method carried by power delayed profile (PDP) of the channel, wherein if the distance between the authorized and an unauthorized transmitter may vary and the signal passing through a channel to be rapidly decaying. If the distance of the transmitted information varies, the delay profile get vary and this difference provides alert on the external attack leads to conclude with the probability of detection and probability of false alarm of received signal to secure the network from the impersonation attack.

Sheshasaayee and Sujatha (2017) exposed his thoughts on the evolution of security while communicating in general. The digital communication has transferred the data which copies data itself and saved in the different part which makes the attacker misuse it. To protect this issue, the security in transferring data is classified into cryptography, watermarking and steganography. The cryptography technique is used to encrypt the data into cipher-text using encryption algorithm and decrypt the algorithm at the receiver end. The watermarking method is modified by changing the image into text or another format without changing the original image. The output of the image has the decryption key and algorithm without losing its robustness, capacity and imperceptibility. Watermarking works in the application with the features like content authentication, copyright protection, fingerprinting and covert communication. As comparing the different techniques, digital watermarking is the right solution to protect from a various attack in the network.

Faisal et al. (2018) proposed a method to detect identity technique in ad-hoc networks. The author suggested this method to detect the dos attack and Sybil attack done by the attacker while forging the identity. The detection of a malicious node is done by using the received signal strength without any external device such as GPS and other certificates. In VANET, forging the node and providing a false route over the traffic to legitimate users will gain more forged messages over the network. Some attacks are detected by cryptographic techniques and are not much effective over the detection process in infrastructure. RSS (Received signal strength) uses distance parameters to identify the attacker, they classified into two phases are single radio range and local global network. For example, if no RSS is not received from the attacker node, then it will mitigate beacons over periodic frames to improve the topology. Even the proposed method is effective but not up to the level using periodic beacons. This method proved without any external device the false positive rate is much effective shown in the simulation result.

Wang et al. (2018) were added few schemes to trace the anonymous vehicle in the network and this author implemented a lightweight anonymous trace of the vehicle using a superposition watermarking based anonymity traceback scheme (SWATS) method. This method resolves the problem between traceability and anonymity by using code division multiple access (CDMA) to rebuild the path.It has compatibility for existing method, applying probabilistic packet marking (PPM) to trace vehicles, avoiding space restriction for PPM, eliminate spoofing and man in the middle attack. The SWATS function will watermark the data before sending and the verification process starts to check the data and then the IP address and timestamp were marked in watermarking. If not successful, it will consider as a malicious file. Timestamp and IP address are to record the vehicle path. The simulation and results obtained from SWATS implementation shown on the traceability and anonymity are detecting using the watermarking technology, but it is not feasible to large scale environment.

Ahmed and (2005) proposed to check the hybrid watermarking technique using both symmetric and asymmetric extraction. It can be extracted by embedding using public and private watermarks. The digital watermarking adds digital data to detect user identification and ownership in a multiple user network. They used two watermarking are public and private watermarking. Public watermarking is to possess to gather knowledge using the public key. The private watermarking is used to verify the user with their provided data to check their identity if any attacker is involved during the process.In this digital watermarking verifying the user they use public watermark technique if attacker in the network. Then after breaking public watermarking, private watermarking will allow the user to verify his identity to a legitimate user. ICA technique is used in watermark for extraction. This method is effective, but it must be improved by improving the watermarking algorithm and its protocol.

2.2 Cryptographic Technique to detect Impersonation attack

Glynos et al. (2005) discussed detecting impersonation attack in MANET, which is the broadcast the network used for communication purpose through wireless connections. Thus, the mobile nodes in manet pose to be more susceptible to various attacks likewise in secured routing, safer transmissions of messages and in addition to intrusion detection and the solutions regards the handling of the broadcast access medium.The security relays on the authentication and identification of the legitimate nodes to reduce the vulnerability, since the manet requires multi-factor authentication rather than single-factor authentication in which the entity is cryptographically linked to the physical node device of the desired identity. To supply better authentication under severe conditions, this method demands the requirement of sensing capability from manet for additional support. The authentication factor uses the joint digital certified signature key identification and certified attributes for physical node connection which helps in enhancing the security of the network.

Shang and Gui (2015) discussed a method on Data Flag Byte to identify impersonation attacks that insists on the physical layer security for the data transformation. Diffie and Hellman defined the key generation method which used noise over layer to assure its security. The wireless communication is increasing for the feasibility of data transmission, though it is messed up with some security issues. The frame contains flag byte as the initiative, and it uses the differential flag byte (DFB) for the determination of the user data (or) identification. Thus, analysis is done by simulating the point to point communication of the single user and reveals that the application of the DFB can help to restore the data from attack. This is affected by the signal to noise ratio (SNR) as it is unable to set the threshold value for the users when it is unstable.

2.3 Node positioning and detect malicious node in VANET

Grover et al. (2011) discussed the node location detection types and finding malicious using different methods proposed by different authors. This technique is used to overcome RSSI (Radio Signal Strength Indicator) method which lacks infrastructure communication, and which provides limited accuracy even when the two nodes are closer. The proposed method will estimate the distance received by comparing the time of arrival on a chosen node between the RF beacons and paired ultrasound beacon. The important thing is to analyze and identify the attack pattern to find the location over the network. Easy to find the attacker with different patterns when the node detection rate is combined with the data between the RF beacons over the positioning verification method. The attack rate is detected by using CAS (Context-Aware Security) models and reduce the false node rate.

The position of the node is detected using its identity, time and geolocation in beacon packets. In the position forging, the attacker can add many false nodes to divert the legitimate node and might cause a serious impact for the legitimate node and at times will impact the service provided by VANET. Khurana and Yadav (2018) proposed a method to prevent detect the position forging with the data over vehicle speed, packets delivered ratio and number of collisions. The researcher explained in detail about the classification of forging nodes in the network are for Forging Random Positions using Single ID(FRPSI), Forging Random Positions using Multiple IDs (FRPMI), Forging Path using Single ID (FPSI), Forging Path using Multiple IDs (FPMI). The attacker performs using virtual functions with fake id's and position which change the legitimate user's behavior depends on the information user received.

Welch et al. (1995) have discussed on detect the position in vanet based on authentication scheme against bogus attack for secure communication [23]. The bogus attack is detected by analyzing the false position detection and mitigate from the network. The digital signature works on two features are routing protection mechanism works with end-to-end encryption method and node evaluation mechanism works with forward and backward position where forward methods used to find dropped malicious node and backward method used to find out tampered malicious node. After analyzing the simulation result over security and performance the researcher came out with the solution for finding drop and tamper node in network without cryptographic system. The lose level and throughput were discussed are not much and confidentiality is not satisfied in this method over finding position of the node.

Han et al. (2017) discussed on vehicle positioning system is being used in the framework for the execution of the vehicular area. The vehicular arranging redesign is implied for the issues caused by the short-range exchanges. The positioning of the vehicle is the principle for routing and thus stabilizes the mobile vehicle's data availability. The vehicle's development state is addressed with the position and speed. The Kalman filter here is used for adjusting the blunder in odometric by outside recognition to produce the numerical premises, the design of the filter uses the loop-back protocol. Prachi Kulkarni and Rekha Labade [2018] along with Vinh Hoa LA and Ana CAVALLI [2014] shows their result simulation using NS2 to detect the position in VANET considering the security protocols over authentication, data integrity and non-repudiation[La and Cavalli (2014)].

2.4 Modern Techniques proposed to detect and authenticate during impersonation Attack

Tanabe et al. (2013) proposed a secure method against impersonation attacks in wireless sensor networks (WSN). WSN is used in many onsite applications like recording climate, disaster notification and in agriculture, though it is susceptible to some attacks and creates threats to the users. Bloom filter technique have been proposed to determine the attacks and to secure the data. The bloom filter is a data structure within which the hash function is employed to compress the data's actual size and it protects the source node by identifying the path of the routing node and authenticating it. Another method of dispersed data transfer technique encrypts the node and provides confidential data sharing to the destination node. Bloom filters are better in finding impersonation attacks in the source node, but it lacks in finding impersonation attacks in relaying nodes.

Khurana and Yadav (2018) discussed an idea of preventing malicious node using the generic algorithm in vehicular ad hoc networks. VANET works with ITS (Intelligent Transportation Systems) which highlights the path, node, and traffic . In the existing methods, the packets are identified as pseudo reply packets, and all the logs are saved under push pop series in ascending order. If any node are less than the threshold value, it is considered as a malicious node that will improve the performance of the network. The generic algorithm works on two paths are source and destination. The crossover and mutation method were carried out between two paths where the new nodes are fitted with values that are replaced with low values. If they are below the threshold value, are considered as fault node which improves the performance of the network.

Iwendi et al. (2018) proposed an algorithm known as the spider-monkey technique to detect the Sybil attack in the network. It is detected by using multihop networks for energy consumption, detection ratio and estimating accuracy. Node impersonation attack occurs with multiple false identities with some functions added in RSU, vehicles, DMV (Department of Motor Vehicles) and CA (Certification of authority). The spider-monkey technique extends with communication interface and fictitious identities. The legitimate user position is detected by verifying its node topology, message authentication, analyzing vehicle count, accessibility verification and location overlapping. By using the algorithm, it shows clearly that the detection of Sybil attack in the existing method lags in long-distance detection where spider-monkey technique is efficient to detect the attack in dynamic path with proper detection rate and energy efficiency.

Chhatwal and Sharma (2015) were discussing detecting impersonation attack in VANET using buck filter. They used the VANET content fragile watermarking (VCFW) technique to secure the data during transmission to protect the authentication. The author majorly focused on fault node detection, short route detection, and vehicle location detection. By using buck filter, author broadcasting beacons around the vehicle in the network for every 100 ms to detect the nearby vehicles. Mobility data are verified by timestamp. The hashing method is used to verify the signal generated by RSU. VCFW is an advanced level cryptographic technique used to encrypt the data by using the watermarking system. Data is hidden in the image file and sharing the image without breaking its pixel. It is only possible by the legitimate user to decrypt the data. If any malicious node found, the beacon table will isolate the data from the network. The simulation results show the location detection is 86% using buck filter. The author explains there are few delays in the parameter, and it is because of high topology.

Bhargava et al. (2015) proposed a method for the Kalman filter estimation using trust prediction to overcome the lags with the security system and to protect nodes from illegitimate users. Celes and Elizabeth (2018) discussing that the malicious node which acts as the user and alters the alert messages for its own cause, thus incorporation of trust finds out that malicious node in short span of time. The computation for finding the trust value in vanet combines the existing trust value with the node behavior to get the actual trust. The predicted trust value has variance with the actual trust value, the mono dimensional Kalman filter is used to minimize the error due to the short interaction of nodes. Since the obtained trust value is used as a time instant to predict the upcoming trust value. Kalman gain is employed in estimating the weight to be given to existing trust for estimating future prediction. It is shown that the trust value with constant time will provide a low error.

The cyber-attack is one of the consequences of the network transformation system. This attack is being found in networks and transportations. This cyber-attack causes the intrusion with the communication which also damages the physical processors and spoofs the sensors in the network. Chang et al. (2015) came up with the countermeasure with the secure estimation of the system state using the Kalman filter with fixed attacked nodes whereas it improves the security and controls the attack. Under this attack, researchers proposed an approach to design the algorithm for a secure estimation model with an attack signal as a process. Though in this paper, it is taken that the attacked nodes change over time and which is being used computationally for attack signal and uses Kalman filter to make its efficiency under adversarial attack.

After having an intense analysis of the papers related to VANET attacks, location forging and watermarking technique. I got a better understanding of the VANET functioning method and model related to the proposed technique. In the next section, there will be a detailed analysis of the filter, simulation, system model, performance analysis and evaluating the result.

3 Methodology

VANET nodes are often moving their location due to high mobility which leads to the high topology. Kalman filter is a set of a mathematical equation that provides a derived solution to estimate the state of a process which reduces the error in the system. It provides the solution for the past, present and future states of the system. Based on differential equations, the vehicle position updating model was designed and the algorithm predicts the neighborhood node distance to optimize its prediction process. The trust factor plays a significant role in this project to find the faulty node in the network. In VANET, the packet loss is a major factor that is considered the delay and prediction method in the network. PDR not only refers to the total number of packets received that the total number of packets sent ratio. It does not represent the packet ratio. It also signifies the maximum throughput and the integrity of the vehicle position. Kalman Filter works on the two-step process:

- The Filter predicts the next position depends on the measured value.
- The updated prediction was depending on the current position and the gain value for the vehicle along with the frequency of the vehicle.

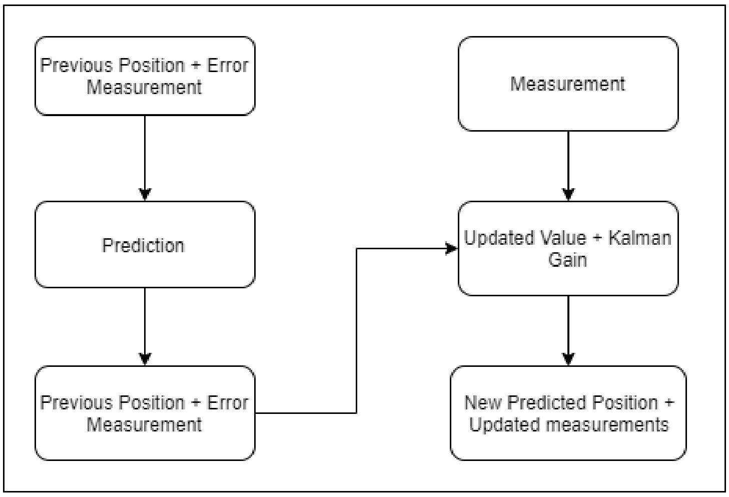
Previous Position + Error Measurement
Prediction
Previous Position + Error Measurement
Measurement
Updated Value + Kalman Gain
New Predicted Position + Updated measurements

Figure 3: Kalman Filter Working Process

3.1 Vehicle Position Prediction based on Kalman Filter Algorithm

Kalman filter try to estimate the mean of discrete value with the constant formula Rana et al. (2009):

Kalman Filter equation:
X= A(n-1) + P (n-1) . . . . (1)
The filter works on two groups are: time update and measured update where Time update will forward the vehicle current position and error covariance reckons to obtain a priori approximate the value for next vehicle location. The measured update works with

the priori approximate value to achieve an enhanced posteriori valuation.

Prediction with Error Covariance Equation:
p(n—n-1) =A2*p(n-1—n-1) +q . . . . (2)
where n-1 represented to estimate the past position respective to the time t. The term Q represents the process noise covariance and predicts the error and noise respective to P(n-1). The predicted value was directly proportional to the process covariance. Mostly the prediction error occurs due to estimate using the variables. The intermediate predicted valuable and variance matrix is applied to update the estimate values to update a new value. The predicted value of the vehicle location with error covariance was added in the Kalman gain and the below equation forms as below:

Kalman Gain Equation:
Gain = P*HT [r + H * p * HT]-1 . . . . (3)
The word HT refers to the measurement matrix which is used to predict the state vector A(n-1). Kalman gain is directly proportional p(n-1) where HT is indirectly proportional to the error covariance r and noise measurement n.

Updating the estimated measurement:
x(n—n) = x(n—n-1) + gain(n) * [z_measure - H(n)*x(n—n-1) . . . . (4)
Once the gain value obtained, it will be added with initial variables A and P to obtain by using the updated value equation.

Updated value:
p(n—n) = [I - gain * H] * p(n—n-1) . . . . (5)
where, n- variable represents to noise measurement and z- State of measurement (Bayes Rule)

The Kalman filter predicts the trust value between the matrix [-1,1] where -1 as lower bound trust and 1 as upper bound trust involving the trust of the vehicle. The value of X with respective time t get extended within the interval where the trust value lies in-between trustee and trust over the VANET. These trust values are verified by using the Kalman filter algorithm and move the node to the desired point. The algorithm will verify the MAC address of the sender vehicle and verify its watermarking technique compared with the key to send the data to the desired destination. Mostly the predicted value is equal to the updated value in this method.

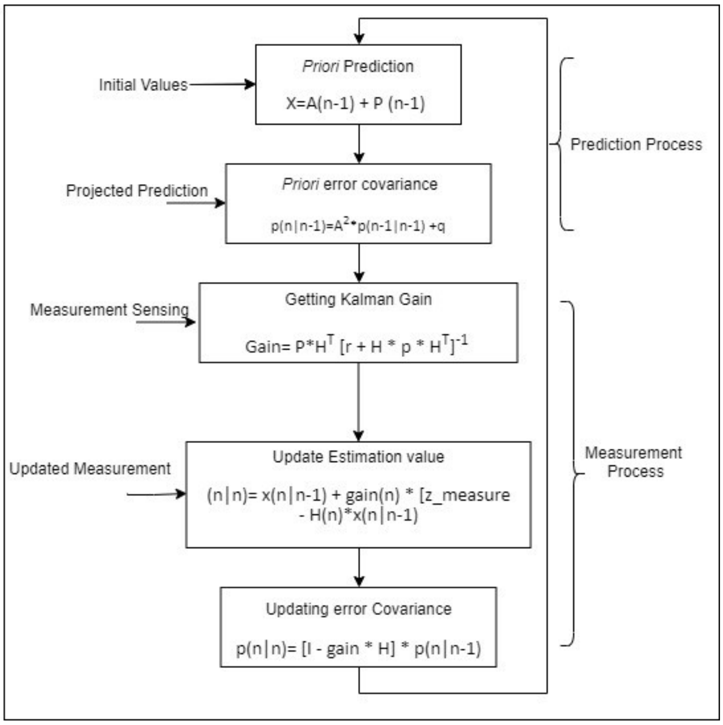

Figure 4: Block Diagram of Kalman Filter Algorithm

After getting each location point, it will repeat the process up to a certain time limit given in the parameters. If the algorithm finds the values are less than the threshold, it will isolate from the network and alert the user about the false node with respect to time t. Even if there is a large variation in the value of A, there will be a slight change in trust value. In such a case, the predicted value and trusted value almost equal and the difference should lie between the trusted parameter. So that Kalman filter has been proposed to detect the impersonation attack in VANET using its trust estimation value with respective noise and error co-variance acts as a control parameter for predicting the vehicle location.

Watermarking is an added technique in the project to secure the integrity of the data. In the proposed idea, it was implemented by sharing the shared secret key between the vehicle. Even if the attacker able to access the packet, he cannot decrypt it. Each vehicle has a unique identity to verify its IP and MAC address to deliver the message in a destination. This watermarking technique will verify its identity and check for the key to decrypt the packet.

3.2 SYSTEM Model

1) VANET Model:

It consists of two components are 1) RSU and 2) OBU where RSU is fixed and OBU are fixed in-vehicle and each vehicle consists of OBU, GPS receiver, data monitoring, and radar. The central authorities are responsible for managing vehicle identity based on their geo-location. The standard IEEE 802.11 wireless is used in the data link layer. It has the range to communicate with vehicle from 250 to 1000m with the speed of 5-30mbps.

2) Communication Model:
The Vehicle in VANET communicate are three types are 1) V2I 2) V2V and 3) V2R. In vehicle-to-vehicle, they communicate with the other nodes for popup alert message and safety messages.V2V classified into two divisions are single-hop and multi-hop, where single hop is for broadcast safety messages and multi-hop, is the area where the attacker tried to get in between and stop the services. V2R is for the vehicle to access the internet and special request depends on the location.

3.3 Security Requirements

Identity Authentication: It is required to authenticate the message which is transferred in VANET has a valid user.

Non- Repudiation: It is to verify the legitimate node who forwards or transmits the message should not deny that it is not from that node. It is very important to verify the location of the node during multi hop communication in the network.

Data Integrity: Data integrity is to protect the packets from tampering and prevent the malicious node.

3.4 Performance Analysis

Estimation Analysis

1. Detection Ratio: The proportional of nodes in the network and malicious node are compared with a condition to find the detection ratio.

2. True Negative Ratio: The condition applies when the node is not detected based on the absence of a condition.

3. False detection Ratio (FDR): It is the ratio of detecting false value in the network over a period.

4. Delay: The amount of time required by a node to complete its action is compared with the number of nodes in a network to find the delay rate.

5. Packet Detection Ratio: It is the ratio of total packet delivered successfully to the total packet sent in a unit distance.

6. Throughput: It is the rate at which the data is sent through the network.

3.5 Design Specification- Simulation Process

From the figure 5, the simulation process steps as follows as:

Step 1: Select the simulator tool and determine the parameters for simulation.

Step2: Extract the vehicles parameter into the network simulator with certain frequency and run the file to generate impersonation attack.

Step 3: Initial position of vehicle values are received from step 2 into Kalman predictor to predict the value with equation (2)

Step 4: The original position value is received from step 3 helps to predict the node position, difference predictor equation (3) added the to get the updated estimated measurement value in the equation 4.

Step 5: The input values from step 2 and step 3 are combined in equation 5 to calculate the updated value. Comparing the updated value with present threshold value to move further in updating message.

Step 6: After predicting the node, the packet transfer happens with watermarking technique.

Step7: All the simulation process and packets transmission are recorded for analysis.

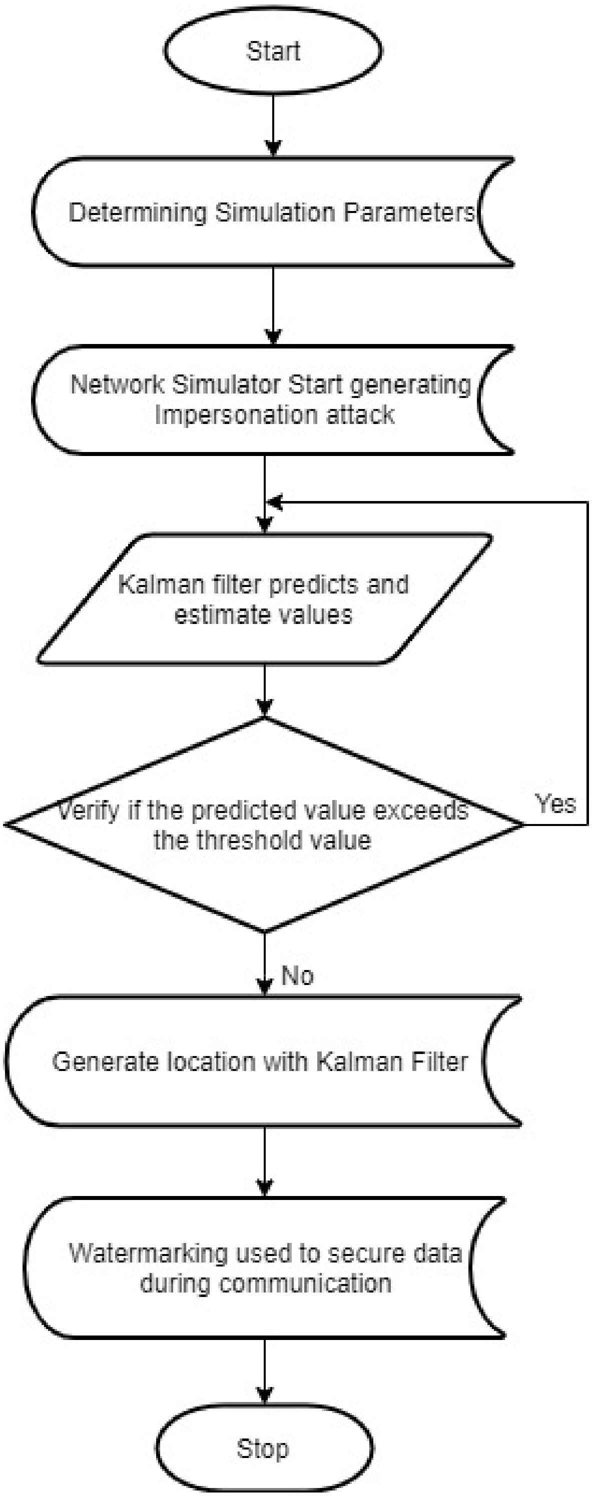
Start
Determining Simulation Parameters
Network Simulator Start generating Impersonation attack
Kalman filter predicts and estimate values
Verify if the predicted value exceeds the threshold value
Yes
No
Generate location with Kalman Filter
Watermarking used to secure data during communication
Stop

Figure 5: Simulation Flow Chart

3.6 Implementation

The plan was executed in Network simulator 2. It is an open-source simulator runs on ubuntu/Linux/fedora operating system and used to simulate the network performance over a given set of rules.

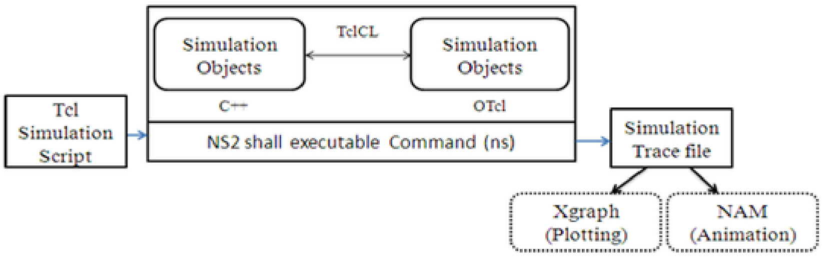

Figure 6: NS2 Basic Architecture

Figure 6 explains about NS2 simulator architecture consists of an executable script file with .tcl and they used two languages are C++ and Object-oriented Tool Command Language (OTcl). The functionalities are mapped in C++ objects and front-end are defined with OTcl objects. The NS2 version 2.34 was compact for running the simulator depends on our requirement when compared to another version

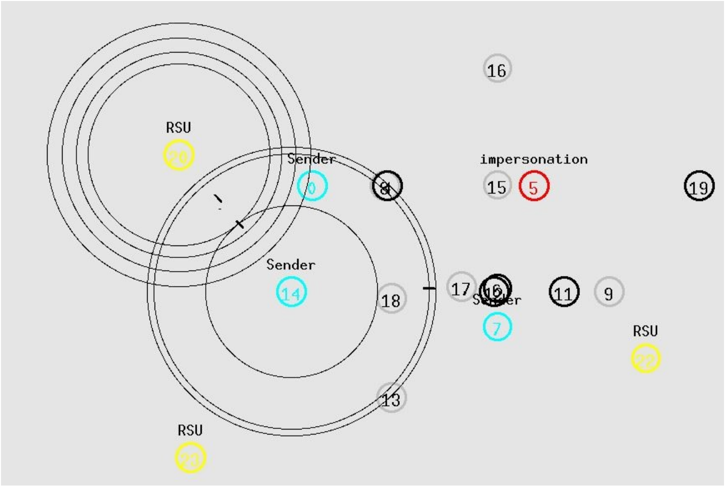

Figure 7: NS2 Simulator Environment

The simulation area in the scene was about 3000m x 3000m. The vehicles(nodes) are moved on their path with respective traffic. The simulation protocol is installed based on Adhoc OnDemand distance vector (AODV)protocol in NS2 Simulator.

The nodes are indicated with small black circle numbers, RSU indicates with yellow color and malicious node with red color in the network and big circle for radio waves to communicate visually. The nodes are moved wireless in the defined path. Xgraph is used to generate graph for the parameter's values.

The network parameters in the simulators having the overall simulation time of 300s. Each packet's size is 64 bytes with the packet rate of 2 packets per second. The radio

Items	**Value**
Simulation Time	300ms
Rate	2 packets per second
Radio Radius	100mts
Maximum speed of node	10m/s
Data Flow 1	From node 22 to node 7
Data Flow 2	From node 14 to node 2
Processors allocated	2
Malicious Node Number	2
Total Number of Nodes	24
Antenna Used	Omni Antenna
MAC type	IEEE 802.11

Table 1: Network Parameters

radius was 100m and the maximum speed of the vehicle was 10m/second and they have 24 nodes in the radius of network 3000m.we added two data flows that were added from node 22 to node 7 and node 14 to node 2.During the simulation, two malicious nodes were added to the network as a package. The losing packets and delay during transmission in the network where considered as malicious node and named as “impersonation attack node”.

4 Evaluation

The simulation output graph was analyzed with different scenarios and varying nodes. The results are compared with the existing methodology for better efficiency. For this evaluation, a city scenario was taken with faulty node as maximum of 10 and the detection ratio was compared with the existing method having same parameters.

4.1 Detection Ratio (Kalman Filter VS Existing Method)

The detection ratio is represented as the ratio between true positive and false negative values identified by the identifier. The successive rate of node detection using Kalman filter was 90% which is better compared to the existing method.

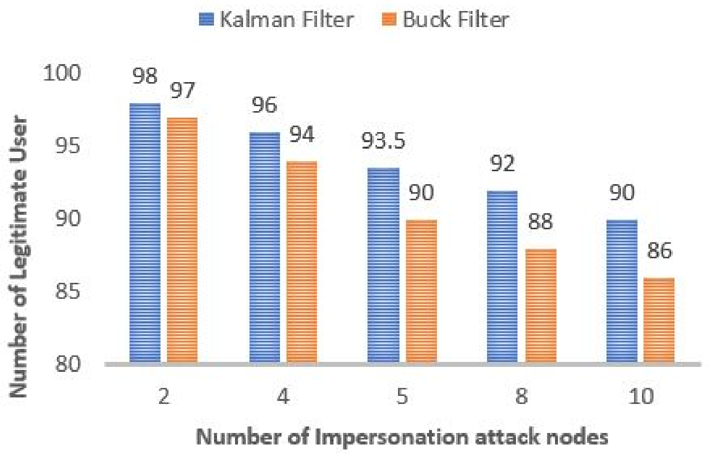

Figure 8: Detection Ratio

The above graph shows the detection rate by increasing the impersonation attack node. Even by comparing both the existing and proposed method, the detection rate was high up to 90% for proposed method even when 10 attacker nodes placed in the network.

4.2 False detection Ratio using Kalman Filter (FDR)

False detection Ratio is measured by comparing the number of negative values wrongly detected in the network along with the actual negative value ratio. The below figure and table with the parameters are recorded by increasing the number of nodes during the simulation.

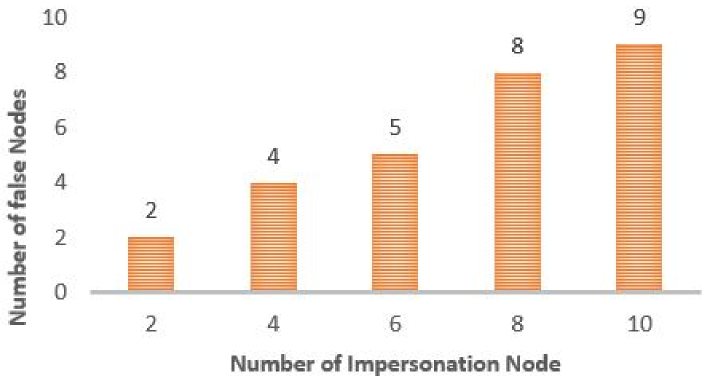

Figure 9: False detection Ratio using Kalman Filter

The above graph shows the false node detect by increasing the faulty node gradually. This graph shows the false detection rate was 97% accurate using Kalman filter.

4.3 True Negative Ratio using Kalman filter

The True Negative Ratio is compared by counting the number of true negative values is divided by adding a total number of a true negative and false negative. The below graph represents the true negative value for each node is plotted using a Kalman filter by varying the number of impersonation attacks.

True Negative Ratio= True Negative value (True Negative value + False Negative value)

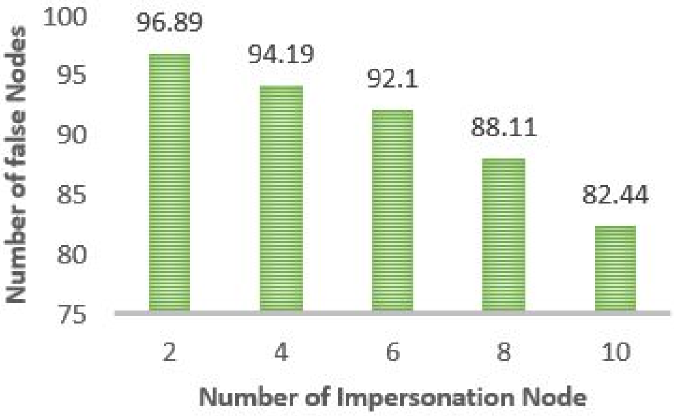

Figure 10: True Negative Ratio

The above graph shows the detection percentage for true negative was 96% accuracy as an average. Gradually increasing the impersonation node, it has capability to detect up to 82% accurate.

4.4 Packet Detection Ratio comparison between Filters

Packet detection ratio is the ratio of the total number of packets delivered successfully to the total number of packets sent in a unit distance. The below graph represents the parameters comparing between with and without Kalman filter by varying the number of impersonation nodes in the network for detecting the packets.

PDR= (No. of packets received/No. of packets sent) x 100

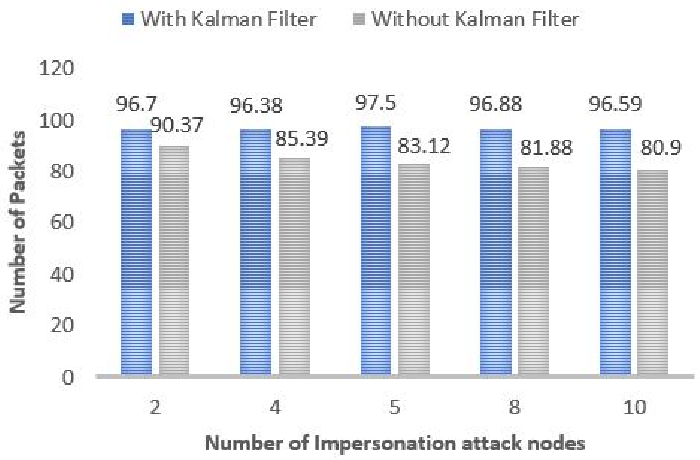

Figure 11: Packet Detection Ratio Comparison

The above graphs are about packet detection ratio by comparing with and without Kalman filter. The packet detection ratio was greater when using Kalman filter and the detection rate was much lesser in when using without Kalman filter. Even though increasing impersonation attack node, the detection rate was high by using Kalman filter.

4.5 Delay Comparing

The amount of time required by a node to complete its action is compared with the remaining number of nodes in a network to find the delay rate over a period. The below graph was compared with the Kalman filter and without Kalman filter over a period. The average output by using filter shows the delay was less than 0.2 seconds even increasing the number of impersonation nodes.

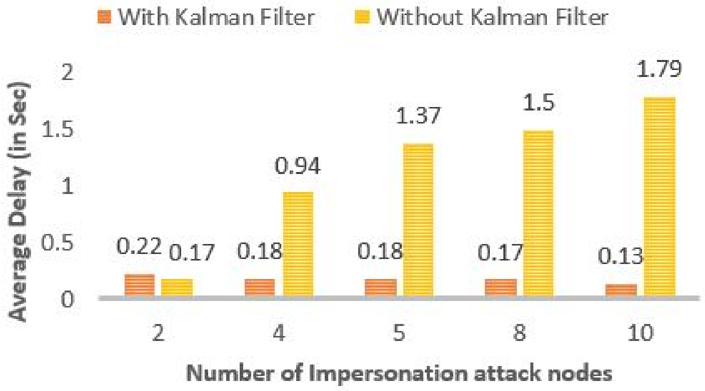

Figure 12: Average Delay

The above graphs indicate the average delay in network and the values obtained from simulation are differentiated by with Kalman filter and without Kalman filter. The table shows maximum of 0.134 sec delay generated after adding 10 impersonation attack nodes.

5 Conclusion and Future Work

From the related works and evaluation, we present a brief outline of the detection process for the impersonation attack. Detection process of impersonation attack constitutes the verification of range, speed of vehicle and assumes that RSU performs the verification which can reduce the computation time. Each roadside unit (RSU) calculates the speed depends on the packets delivered to a passing-by-vehicle. If there is a high loss in packet delivery and not in the range of threshold, it leads to be a malicious node. All the RSUs exchanges its surveillance intermittently.

we elaborated with various trust estimated values predicted using a Kalman filter to detect the attacker node within the range. The output results were shown in graphs for better understand. The watermarking technique was an added technique to secure the data even if the attacker tries to access the data, but the attacker cannot decrypt it.

The vehicle location detection ratio was 90% which is effective when compared to the existing method. We also investigated by adding more nodes to analyze the speed of the vehicle, packet delivery ratio, signal to noise ratio in VANET. The project can be improved in future by adding a strong hashing technique, short route detection, and broadcasting alert message to user in the network, isolating attacker node from the network. The security features in VANET can be improved by improving the detection technique.

6 Acknowledgement

I would like to thank my parents for their supporting throughout the academic internship. I would be grateful to my mentor Mr. Imran Khan for his encourage and supporting all the way throughout my research work.

References

Ahmed and, Fawad, S. (2005). A hybrid-watermarking scheme for asymmetric and symmetric watermark extraction, *2005 Pakistan Section Multitopic Conference*, IEEE, pp. 1–6.

Bhargava, A., Verma, S. and Chaurasia, B. K. (2015). Kalman filter for trust estimation in vanets, *2015 IEEE UP Section Conference on Electrical Computer and Electronics (UPCON)*, IEEE, pp. 1–6.

Celes, A. A. and Elizabeth, N. E. (2018). Verification based authentication scheme for bogus attacks in vanets for secure communication, *2018 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, pp. 0388–0392.

Chang, Y. H., Hu, Q. and Tomlin, C. J. (2015). Secure estimation based kalman filter for cyber-physical systems against adversarial attacks, *arXiv preprint arXiv:1512.03853* .

Chhatwal, S. S. and Sharma, M. (2015). Detection of impersonation attack in vanets using buck filter and vanet content fragile watermarking (vcfw), *2015 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, pp. 1–5.

Faisal, M., Abbas, S. and Rahman, H. U. (2018). Identity attack detection system for 802.11-based ad hoc networks, *EURASIP Journal on Wireless Communications and Networking* **2018**(1): 128.

Glynos, D., Kotzanikolaou, P. and Douligeris, C. (2005). Preventing impersonation attacks in manet with multi-factor authentication, *Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05)*, IEEE, pp. 59–64.

Grover, J., Gaur, M. S. and Laxmi, V. (2011). Position forging attacks in vehicular ad hoc networks: implementation, impact and detection, *2011 7th International Wireless Communications and Mobile Computing Conference*, IEEE, pp. 701–706.

Han, S., Ban, D., Park, W. and Gerla, M. (2017). Localization of sybil nodes with electro-acoustic positioning in vanets, *GLOBECOM 2017-2017 IEEE Global Communications Conference*, IEEE, pp. 1–6.

Iwendi, C., Uddin, M., Ansere, J. A., Nkurunziza, P., Anajemba, J. H. and Bashir, A. K. (2018). On detection of sybil attack in large-scale vanets using spider-monkey technique, *IEEE Access* **6**: 47258–47267.

Kaur, R., Singh, T. P. and Khajuria, V. (2018). Security issues in vehicular ad-hoc network (vanet), *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, pp. 884–889.

Khurana, C. and Yadav, P. (2018). Prevention of malicious nodes using genetic algorithm in vehicular ad hoc network, *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, IEEE, pp. 700–705.

La, V. H. and Cavalli, A. R. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey.

Panichpapiboon, S. and Pattara-Atikom, W. (2011). A review of information dissemination protocols for vehicular ad hoc networks, *IEEE Communications Surveys & Tutorials* **14**(3): 784–798.

Rana, M. M., Ahmed, K. E. U., Sumel, N. R., Alam, M. S. and Sarkar, L. (2009). Security in ad hoc networks: A location based impersonation detection method, *2009 International Conference on Computer Engineering and Technology*, Vol. 2, IEEE, pp. 380–384.

Rawat, A., Sharma, S. and Sushil, R. (2012). Vanet: Security attacks and its possible solutions, *Journal of Information and Operations Management* **3**(1): 301.

Shang, T. and Gui, L. Y. (2015). Identification and prevention of impersonation attack based on a new flag byte, *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, Vol. 1, IEEE, pp. 972–976.

Sheshasaayee, A. and Sujatha, D. (2017). Analysis of techniques involving data hiding and watermarking, *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, IEEE, pp. 593–596.

Tanabe, N., Kohno, E. and Kakuda, Y. (2013). A path authenticating method using bloom filters against impersonation attacks on relaying nodes for wireless sensor networks, *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, IEEE, pp. 357–361.

Wang, X., Jiang, J., Bai, L. et al. (2018). Swats: A lightweight vanet anonymous traceback system based on random superposition watermarking, *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, IEEE, pp. 748–755.

Welch, G., Bishop, G. et al. (1995). An introduction to the kalman filter.

Yılmaz, M. H. and Arslan, H. (2013). Impersonation attack identification for secure communication, *2013 IEEE Globecom Workshops (GC Wkshps)*, IEEE, pp. 1275–1279.