Volume 3, Issue 4
August 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Using the Grades Mechanism to differentiate the Behavior of Attacker Users and Normal Users in Vehicular Adhoc Network (VANET)

Irshad Ahmed Sumra[1], Halabi Bin Hasbullah[2]
[1,2]Computer and Information Sciences Department
Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750, Tronoh, Perak, Malaysia.
[1]isomro28@gmail.com, [2]halabi@petronas.com.my

Jamalul-lail Ab Manan[3]
[3]Advanced Information Security Cluster, MIMOS Berhad
Technology Park Malaysia Kuala Lumpur, Malaysia.
[3]jamalul.lail@mimos.my

ABSTRACT

Potential application of Vehicular network ensures the solution for the traffic issues and makes journey more comfortable. Due to open nature of wireless medium and dynamic topology of network, the behavior of end user has an important role in vehicular network. In this paper, we make analysis of an end users and differentiate the attacker user from the normal user. We also propose two grades for normal traffic and attacker traffic on the basis of behavior analysis table. The aim of assigning propose grades to differentiate the attacker user from the normal user.We hope that the proposed grades are helpful to identify attacks and understand behavior of attackers. It is difficult to detect and control attackers but in future work we would like to develop a prototype system to analyze the behavior of attackers in network. This would make it possible to reduce the negative impact of attacker in future life saving network.

Keywords:*Application, Attackers, Attacks, Behavior, Grades.*

1. INTRODUCTION

Safe and comfortable journey is the main requirements of end users and potential applications of vehicular network must meet these requirements. But the security requirement of these applications is also one of the key important factors for successful implementation of network in real life. User, vehicle and Road Side Units (RSU) are the major entities of vehicular network and they should perform their task accurately and will help us achieve the goal of vehicular network. Attacker is becoming an important entity for its behavioral impact on vehicular network and hence making it necessary to analyze its behavior for secure communication in network. The main motive of attacker is to create problems for users of network and they achieve this through different kinds of attacks. If the vehicular network fulfils all security requirements then it would make it difficult for attackers to achieve their objective.

Trust is also one of the key element of security and the definition of trust is "A system or component that **behaves** in **expected manner** for the **particular purpose**" [1]. Considering this definition in the context of VANET, we may define that all components of the network (**User, Vehicles and RSU**) are behaving in an expected manner and serve users which subsequently help us to save human lives. In practice, there are two types of users in network, namely, normal user and attacker (bad user). The attacker could change the behavior of whole communication network through his/her possible attacks. Due to dynamic topology of vehicular Network and high mobility of network nodes, it is difficult to identify the attacker/faulty nodes in network. It is necessary for user to take the benefits of safety and non-safety applications during their journey if the system is secure and all components of network trusted. Maxim Raya et al. [2] described the attacker model. Insider attack, malicious and active attacks are some examples of serious attacks. Types of attacks can be different depending on the behavior of attackers. Our focus point is to save the communication medium by controlling the attackers. Active and passive safety applications [3] are used to provide safety to users. The role of active safety application is high and it sends warning messages to other vehicles. If attackers change these messages then accidents could be the consequences and users' life can be at risk. In this paper, we attempt to analyze the behavior of attacker in VANET by differentiating the attacker from the normal user. We also propose two grades for normal traffic and attacker traffic on the basis of behavior analysis table. We hope to make it possible to reduce the role of attacker in future

Volume 3, Issue 4
August 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

lifesaving network. Figure 1 shows the basic architecture of VANET and smart vehicle (node) communicates with other smart vehicle and also with roadside unit (RSU). End users have key role while using safety and non-safety applications in

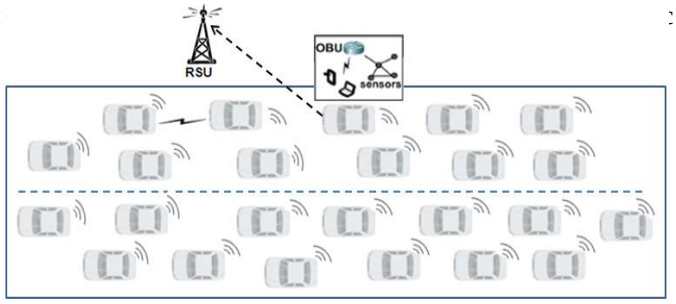


Figure 1. Basic architecture of VANET

This paper is divided into seven sections; Section 2 describes the classification of attackers. Section 3 describes the different types of vehicular network behavior. Section 4 explains the related work in this field. Section 5 explains the proposed attacker's grades, followed by its analysis using attacker behavior analysis table. Section 6 provides the detail description of analytical analysis through Poisson distribution and then using NS-2 simulates our proposed scenarios. Section7 concludes the paper.

2. CLASSIFICATION OF ATTACKER IN VEHICULAR NETWORK

Attacker create problem in the network by getting full access of communication medium DSRC. In this section, we discuss some properties and capability of the attackers which has been mentioned in following studies [4, 5].

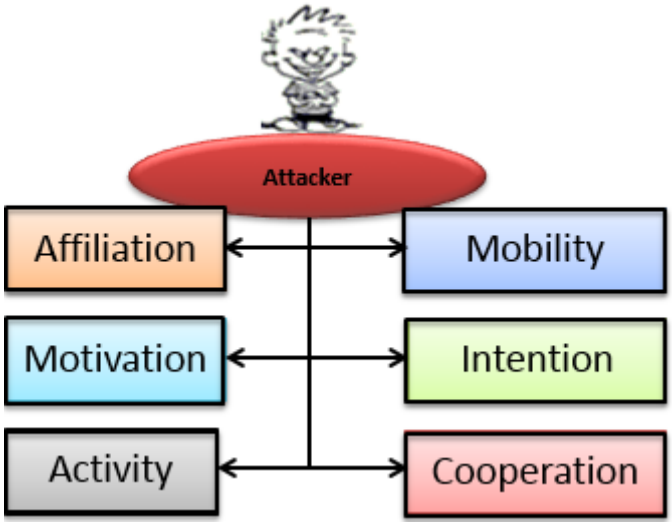


Figure.2 Attacker's role classification

A. **Mobility**

Stationary and mobility are two possible behavior cases of the attacker. In first case, an attacker sits near the bridge over the highway and launch possible attacks. Stationary attack is limited in scope and range because attacker is in static position. Mobility attacker is more serious and move around in network while launching vehicle to vehicle and vehicle to roadside unit attack in network.

B. **Affiliation**: Affiliation of the attacker is classified into insider and outsider attacker.

- **Insider Attacker** is an authentic user of the network and can create problem in the network by changing the certificate keys with the intention of attacking from inside. Insider attacker might have access to insider knowledge and this knowledge will be used for understanding the design and configuration of network. When the attacker have all information about the configuration then it would be easy to launch attacks and create more problems as compared to outsider attacker. We can also say that insider attacker is the right man doing the wrong job in the network.
- **Outsider attacker** is also an authentic user of the vehicle or the network. It is a kind of intruder which aims to misuse the protocols of the network and the range of such attacks are limited. Outsider attacker also has a limited diversity for launching different kind of attacks as compared to insider attacker.

C. **Intention:** intention of the attacker can either be intentional in launching the attack in network. Attacker intentionally disturbs the network operation and creates problems for other legitimate users and gain access to network. Another possibility could be just violation due to malfunction or errors in the network operation.

D. **Motivation**: There are two possible motivation of attacker. *Malicious attacker* who has no personal recompense for launching the attacks, but they want to achieve their following goals:

- To harm the other vehicles by sending wrong information or alter safety related applications information.
- To create problem by agitating the right functionality of the network by sending of unnecessary frames to other vehicles. *Destructive/ Just for fun*: attacker may have some personal profit such as having less road traffic on his/her own traveling route.

E. **Activity**: Active and passive are two possible conditions for attacker. *Active attacker* creates problems in the network while working into two possible dimensions.

- Attacker creates malicious packets and sends them to other nodes of the network and as well as to the infrastructure.
- Attacker sends harmful signals in the network and disturbs the main frequency band. Passive attacker aims to just eavesdrop on the wireless medium among the vehicles and infrastructure (RSU) of the network. It is a kind of privacy violation of users on the road.

F. **Cooperation**: This can either be a single attacker or a group of attackers (Cooperative).The group of attackers intentionally wants to attack the network as a coordinated group. Here, the attackers are dependent on each other and share the same interest. Single attacker launches the attacks and may not be dependent on the other vehicles in achieving a particular goal.

Volume 3, Issue 4
August 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

3. TYPES OF VEHICULAR NETWORK BEHAVIOUR (VNB)

The behavior of the attacker will affect the vehicular environment. Both of the behavior of the attacker and the vehicular environment are interrelated with each other. The dynamic topology of a vehicular network shows the positive behavior of the entities of the network. An attacker creates and affects the negative behavior of the network i.e. if an attacker launches any attack then the behavior of the network will be changed negatively. Figure 3 shows the relationship between vehicular network behavior, attacker's behavior is directly related to the behavior of the other components of the network i.e. user, vehicle and RSU.

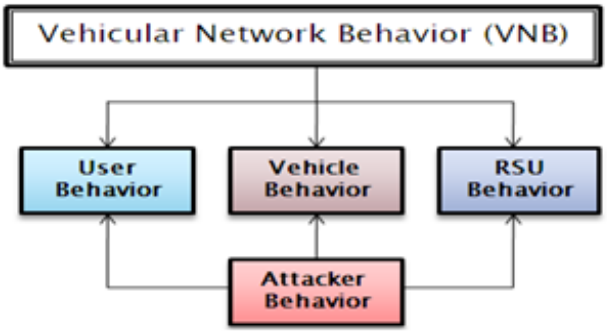


Figure.3Types of Vehicular Network Behavior

Attacker Behavior (AB): Attacker is one of the strongest entities of the vehicular network and this entity directly affects the behavior of the other components of the network. Time (T1), Location (L1) and Attack (A1) are three parameters associated with the behavior of attacker, and these values could be static or also dynamic. Figure 4 show the behavior of the attacker in which attacker node X received message "**Road is clear**" from other node B. The attacker could intentionally change the contents of this message to become "**Warning!!! Traffic Jam**" to node C.

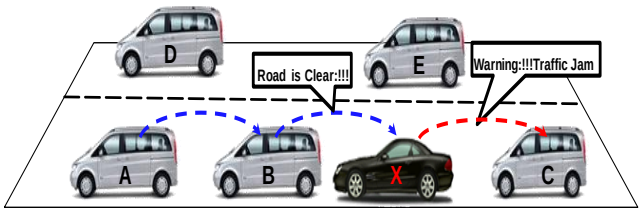


Figure.4 Attacker behavior in network

User Behavior (UB): Malicious users could potentially be an active attacker and launches different attacks that can be of high intensity. Denial of service attack (DOS), Sybil attack and sending wrong messages are some example of such types of attacks. Figure 5 explains the complete scenario in which an attacker X can break the integrity of message and change the content of the message. For example, the original message is "Parking slot available" and attacker node X receives this message from RSU. The attacker then intentionally changes the content of this message and broadcast this message "No empty parking slot:!!!" to other users in network. So in this way other nodes B, E, F will have to change their plan according to received message.

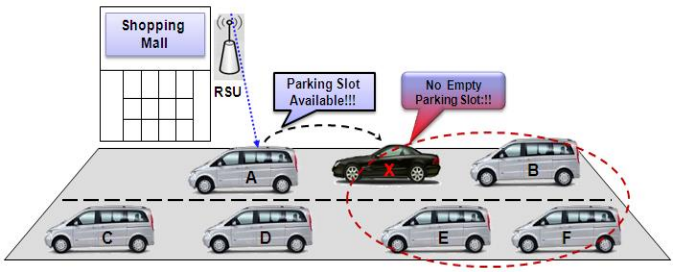
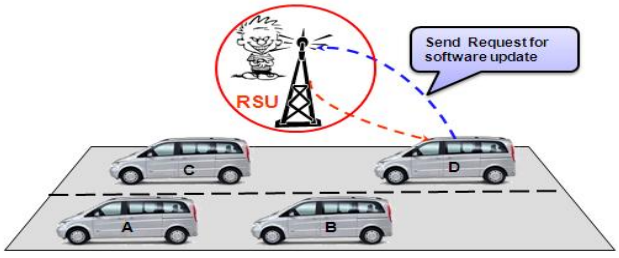


Figure.5 Attacker sending wrong non-safety messages

Vehicle Behavior (VB): Vehicle has a key role in vehicular communication because vehicle communicates with other vehicle and also with RSU. In VANET, and from computing point of view, the Vehicle is a combination of software and hardware and it is necessary that all components of the vehicle to perform their task properly. There is also possibility that the software or hardware may have changed its behavior. An on-board unit (OBU) in the vehicle communicates with other OBU of other vehicles and also with RSU. If it does not perform its task properly then it would be difficult for other users and also for RSU. Malicious user can send malicious program to other user of vehicles and it can create problem for users while communicating in network. Trojan horse or any other types of virus are some types of examples of malicious program.

Malware Attack: Vehicle has its own software and Application Unit (AU) which perform its task and communicate with other users and as well Road Side Unit (RSU). Virus or worm could possibly enter into the vehicle software and disturb the operation of the network. We discuss below some possible scenarios.

- **Scenario 1**: Attacker (malicious user) put virus infected memory stick (i.e. USB) into vehicle AU and then vehicle operating system could change its behavior due to it. An insider attacker could perform this attack easily as compared to outsider attacker.
- **Scenario 2**: When vehicle Onboard Unit (OBU) communicates with infrastructure (RSU) and wants to update software and RSU and vehicle operating system are infected by the virus. Figure 6 shows the scenario in which node D sends request to RSU for software updates, but because it has been hijacked and controlled by attacker through the malicious software, it creates problems for users.
- **Scenario 3**: As soon as a user uses the Internet and any viruses could enter into the vehicle system and causing it to change the behavior of vehicle software.



Volume 3, Issue 4
August 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Figure.6 Malware Attack

RSU Behavior (RB): Attacker may also send some malicious program to Road side unit (RSU) and user may unknowingly update software from the infected RSU. Another possible scenario is when an attacker modifies the message exchange in V2V or V2R communication.There are two possible cases:

- **Falsify Transaction Application Request:** User send false application transaction request to business transaction part in the RSU (most attacker will send this kind of request in non-safety application). For example, Figure 7 shows how the attacker X sends wrong message "Lane change warning" to RSU which is for collection of tolls although the RSU is not responsible for this kind of task.
- **Forge Response:** Forge Response occurs when user communicates with RSU and suddenly the RSU show unexpected behavior to user. For example, Figure 7, shows user B, who wants to send his/her personal information for toll collection, communicates with RSU, but the infected RSU gives forge response to user.

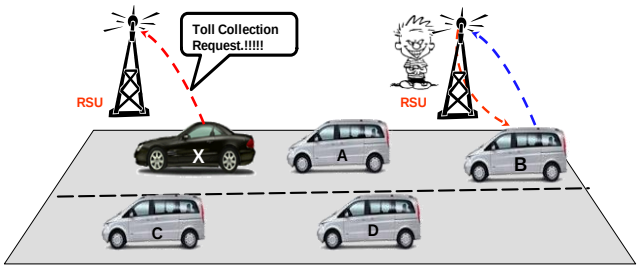


Figure.7 Message Tampering Attack

4. RELATED WORK

Robert et al. [5] proposed a framework which is called VEhicle Behavior Analysis and Evaluation Scheme (VEBAS) which aims to analyze the behavior of other vehicles in network. VEBAS framework consists of multiple modules and each vehicle is assigned a trustworthiness value which is exchanged among all vehicles, thus building up reputation on the output of these modules. Vehicles are classified into trustworthy, untrustworthy or neutral based on the information given and this trust rating is helpful for other users of the network in order to react appropriately on incoming information. For behavior analysis in network, beacon packets are used and these packets contain the vehicle position and movement information. Through receiving a sequence of beacon messages from any particular vehicle, the receiving vehicles are provided with a sufficient amount of data that allows for a meaningful analysis. The result of this analysis leads to the per-vehicle behavior evaluation.

Components of Vehicle Behavior Analysis and Evaluation Scheme (VEBAS) are given below.

A. Basic Modules of Behavior Analysis
   - Positive-Rating Modules:
     Movement Analysis (MA+), Sensor-Proofed Position (<X>PP), Minimum Distance Moved (MDM
   - Negative-Rating Modules:
     Acceptance Range Threshold (ART), Movement Analysis (MA-), Map-Proofed Position (MPP), Sudden Appearance Warning (SAW), Maximum Beaconing Frequency (MBF)

B. Module Output Aging Function
C. Aggregation of Module's Output - The Compound Module
D. Recommendations
E. Final Aggregation of Local Trust and Recommendations
F. Trustworthiness Thresholds

Tim Leinmuller et al. [6] described the modeling of attackers and also identified asset threats and potential inter-vehicle communication. The author conducted a security analysis to understand how attackers could endanger security, which pointed that the highest risk for the system originates from roadside attackers that are sending forged warning messages. This finding motivates more detailed investigation of attacks from roadside attackers. At first stage, they discussed potential options for different attack strategies and emphasized on position forging attacks which turned out to be a major vulnerability of the system. By bringing the applications into consideration, they identified the most promising attack on the each application. The result is that for event driven applications single position forging is the best choice. For cooperative awareness applications, the forging of multiple vehicle movement paths shows significant attraction for attackers and the analysis shows the different efforts needed to succeed in attacking the application. For attacking cooperative awareness applications the effort is quite high and a high motivation is needed behind the attack e.g. a profit-oriented or malicious attacker. Figure 8 shows the format of warning message.

Node ID	Node Position	Time	Warning

Node ID: It is a non-zero number and its range is within available node IDs.

Node Position: Position of the attacker where malicious messages are distributed.

Time: It is message time; it should be always fresh. If message does not have fresh time frame, it is discarded.

Message Type (Warning): This part could be empty ,or it could either be a wrong beacon or malicious warning messages send by attacker.

Figure.8 Warning Message Format

Golle et al. [7] proposed a general approach to evaluate the validity of VANET data and this sensor-driven technique that allows nodes to detect with high probability the incorrect information and identify nodes that are the source of incorrect information. In this approach a node searches for possible explanations for the incorrect information and it collects data based on the fact that malicious nodes may be present in other nodes. The major component of proposed approach is that each node maintains a model of the VANET and itcontains all the knowledge that the node has of the VANET. Given

approach generate and score explanations rely on two statements:

- Nodes know the right information of "at least some" other nodes.
- A parsimony argument accurately reflects adversarial behavior in a VANET.

M. Raya et al. [8] proposed a framework that is able to identify misbehaving or faulty nodes, and then expel them from the system. We explain below the main components, protocols and their functions as follows:

- Infrastructure-based revocation protocols, the Revocation of the Trusted Component (RTC) and Revocation using Compressed Certificate Revocation Lists (RC2RL).
- Misbehavior Detection System (MDS) enabling the neighbors of a misbehaving or faulty node to detect its deviation from normal behavior and initiate.
- Local Eviction of Attackers by Voting Evaluators (LEAVE) protocol to safeguard the system operation, until the attacker is revoked by the CA, partially or fully based on the evidence LEAVE provides.

The author can distinguish between two types of misbehavior in vehicular network as given below:

- Known misbehaviors in network can be identified by monitoring specific parameters of node or network behavior in vehicular environment.
- Data anomalies that do not follow any known pattern and when the adversary modifies or injects safety messages according to its specific needs.

Author believes that the framework is feasible and achieves sufficient level of robustness.

In [9], Schoch et al. collected and categorized envisioned applications from various sources and then classified the unique network characteristics of vehicular networks. For each pattern they concluded the following characteristics:

- **Purpose**: Describes the overall goal of this pattern.
- Communication Mechanism: Describes generic communication mechanisms and presents examples of mechanisms conforming to this pattern.
- **Trigger**: Describes the circumstances under which the communication is typically initiated.
- **Direction**: Communication can be either unidirectional, bidirectional with response(s) to the sender or without clear direction.
- **Data**: Outlines typical communicated data.
- **QoS**: Describes typical capability and requirements of the communication patterns regarding metrics like message distribution success or latency.

Based on this analysis, they proposed five distinct communication patterns that form the basis of almost all VANET applications. This is shown in Table I, which gives the short overview of proposed communication patterns [9].

In our previous work [10], we proposed attackers states (grades) and on the basis of these states, determine the normal users and attacker from congested vehicular network. In this paper we extend our work and define the key factors to differentiate the normal and attacker user in network.

Table I. PROPOSED COMMUNICATION PATTERNS [9]

No.	Pattern Name	Pattern Description
A	Beaconing	Permanent, periodic single-hop broadcast messages.
B	Geo broadcast	Sender (S) initiates multi-hop dissemination of a message within a geographic destination region.
C	Unicast Routing	Communication between two endpoints like node S and node D, single-hop or multi-hop, possibly bidirectional.
D	Advanced Information Dissemination	Time-stable store-and-forward dissemination of a message, restricted by destination region or contextual relevance.
E	Information Aggregation	Abstracts from packets, concentrates on efficient distribution of information.

5. PROPOSED GRADES FOR BEHAVIOR OF ATTACKER (BOA)

This is also one of the challenging tasks to identify the attacker in communication network. So here we can discuss some possible states of attacker, in the view to differentiate between normal and the attacker in network. We take this decision on the basis of communication packets and each node maintains its own analysis table. So now we discuss the proposed grades which are given below.

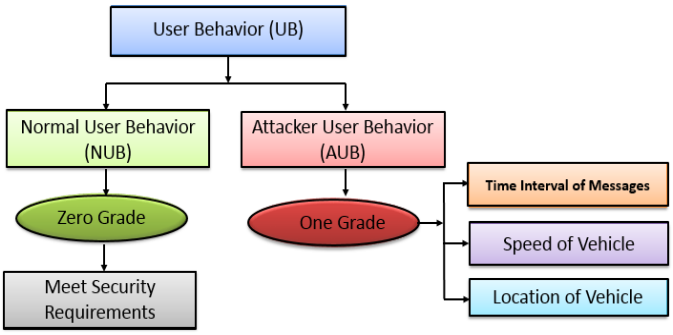


Figure.8 Propose Grades for attacker behavior

Zero Grade:A user with this grading meets all of the security and acts in a manner that is expected in the network. Therefore, he/she is considered to be a trusted user who carries out his/her responsibilities in a proper manner. Some other likely characteristics of a trusted user are discussed below.

- A trusted user who has received a message from another user or the RSU, whether related to safety or not will ensure that particular message meets all the security requirements and then carries out the task involved.
- A trusted user will create an appropriate message related to a specific situation; for example, in the case of an accident and then pass it on to other users and to the infrastructure in that network.

So, Zero Grade is assigned when a driver in a network is considered to be a trusted user. However, caution must be applied as in some special cases, an attacker may masquerade as a trusted user to join a network and subsequently, change its

Volume 3, Issue 4
August 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

behavior and begin launching various types of attacks. In this case, the Zero Grade will be changed to another grade which is described in the next section.

One Grade: A change Zero Grade to One Grade takes place if a user that is trusted alters his/her behaviour and begins initiating attacks in the network. An attacker such as this causes trouble for other users. In reality, this is actually a non-trustworthy user in the network and his/her goal is to cause disruption in the network's basic functionality. Anytime a user alters his/her behaviour and begins initiating attacks, he/she will be considered an attacker, and therefore, will be assigned One Grade. After that, every time that he/she sends a message to other users, his/her packets will be simply dropped. The following section describes a few characteristics that can be used to identify a One Grade user or attacker user.

(a) Time interval of messages (transmission frequency): One of characteristics used to differentiate an attacker is its packet transmission frequency in any given time slot. A flooding attack is a type of denial of service (DoS) attack and the attacker sends false packets in a network with the purpose of consuming the resources of the network. As a result, the resources and services of the network become weighed down and legitimate users are not able to perform their tasks. In a network, it is common for every vehicle to send and receive message; however, if one particular vehicle only receives many messages from a particular vehicle and the time interval of these messages is higher than usual, then the sender vehicle can be considered an attacker and its communication should be blocked or cut off.

(b) Speed of the vehicle: This is a very important characteristic and is directly connected to the ratio of road accidents. If a user's increases his/her speed beyond the safety limit, then it will be considered as an attacker. That particular vehicle will remain part of the network, but it will not be able to receive any services from the network.

(c) Location of the vehicle: VANET mostly focuses on the road and the node of the VANET only provides services for specific ranges of the road. If a user sends any message without any specification on his/her location then it should be considered as an attacker message and assigned a One Grade.

If a message is received with a different format or any particular field is missing, then it should be considered as an attacker message. Since it is not testable, it should be marked as One Grade. For example, in the time interval T1, a normal user B sends 10 packets and vehicle X sends 30 packets in the time interval T2. It means user X is an attacker vehicle and is flooding the network with useless packets. Figure 9 presents this scenario in which vehicle A and vehicle B send out normal traffic messages whereas vehicle X is flooding the network.

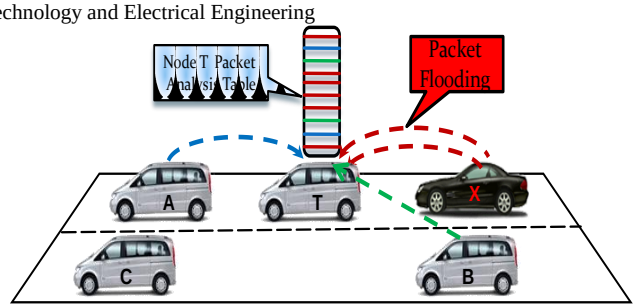


Figure 9. Attacker behaviour in T1 time interval

Table IIshows a Behaviour Analysis Table (BAT) for node T, which shows an analysis of user behaviour in a network. Each vehicle has its own analysis table and marks the packets that do not comply for four possible key features: Node ID, Node Location, Time interval and frequency of packets (P). Node ID and other fields are dynamic and will change according to the dynamic behaviour of the network.Node A (Na) and Node B (Nb) behave as normal users and meet the security requirements of the network. But Node X (Nx) is consider as an attacker, shows negative behaviour and cannot meet the proposed features of normal users. Nx has its packets marked as 1 and is considered an attacker vehicle.If we receive any message whose format is different or any field of message is missing, it should be considered as attacker's message. Since this is not a trustable packets it should be marked as value one (1).

Table II.BEHAVIOR ANALYSISTABLE (BAT)

Node ID	Node Location (*L*)	Time Frame (*T*)	Packets (*P*)-Message	Normal 0	Attack 1
Na	L1	T1	10	0	
Nb	L2	T2	10	0	
Nx	**L3**	**T3**	**20**		**1**
Nb	L4	T4	5	0	
Nx	**L5**	**T5**	**50**		**1**
Na	L6	T6	20	0	
Nx	**L7**	**T7**	**100**		**1**

6. SIMULATION RESULTS

Simulation work has divided into two section: In first section, we have provided the analytical analysis on behavior of attackers through Poisson distribution. In second section, simulatesthe propose three scenarios using NS-2 simulator. Detail description of each section is given below.

Analytical Analysis Section: For attackers, specific locations in the network and time intervals are two important factors to effectively launch more attacks. Thus, it makes sense to find the number of occurrence of a particular event in a specific time interval or in a specific area, for example, the accidents on a particular stretch of road in a day. The Poisson distribution was used to find out the number of events occurring within a given time interval. In a vehicular network, the Poisson distribution is used to find out the behaviour of attackers in any specific time interval and specific area of the network. The basic formula for the Poisson distribution is given below in equation (1) [11].

Volume 3, Issue 4
August 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

$$P(X = K) = f(k) = \frac{e^{-\lambda}\lambda^{k}}{k!} \qquad \text{Eq.(1)}$$

where

- X is a random variable and it denotes the number of successes in the whole interval.
- λ is the average number of events in the given time interval.
- e = 2.71828 (Fixed value)

Figure 10 shows the scenario in which an attacker launches a denial of service (DoS) attack from somewhere near the sport complex. Many users are affected due to this attack and cannot communicate with the RSU.

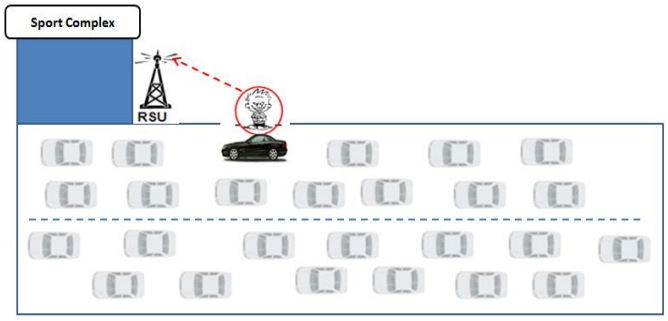


Figure 10.Attacks in specific location

In city areas, a network traffic is dynamic; sometimes the road is very congested and other times, the same road is empty. Figure 11 shows the scenario in which an attacker uses specific time intervals to launch attacks. As the road is more congested during office opening hours and lunch break, these are the best time intervals for the attacker to attack and create problems for the whole network. More users will be effected due to the peak time of the network.

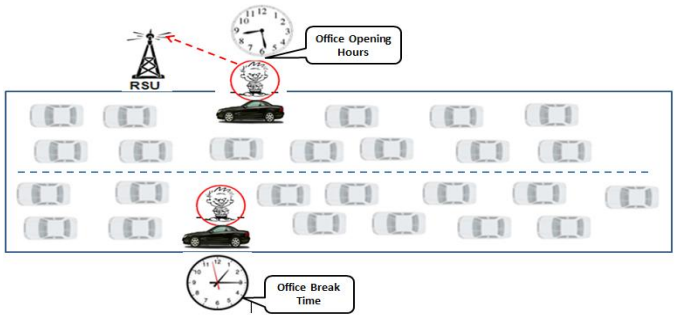


Figure 11.Attacks in different time interval

Case 01: In Case 01, a malicious attacker has dropped 10 communication packets in 1 hour. So, what is the probability that the malicious attacker continues his/her negative behaviour and will drop 15 packets in the next 2 hours in the network?
μ (λ) = 10, e = 2.71, K = 15. These values were entered in the Poisson distribution equation and the result is shown in Figure 4.6.

$P(X = K) = f(k) = \frac{e^{-\lambda}\lambda^{k}}{k!}$ $P(X = k) = \frac{(10)^{15} \times (2.71)^{-10}}{15!}$	P(X = k) = 0.0347

In this case, the value of K indicates the number of communication packets dropped in the network due to the malicious behaviour of the attacker. If the malicious user drops 15 packets then the value of Poisson distribution is 0.0347.

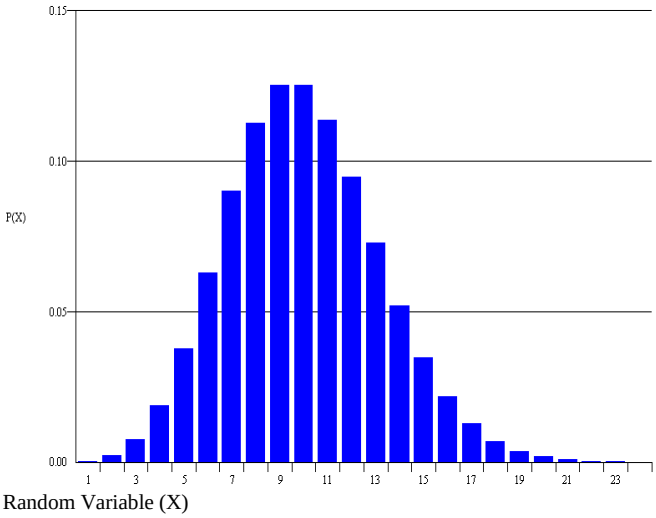


Figure 12. Random variable vs mean value of Poisson

Case 02: In Case 02, an active attacker dropped 15 communication packets in 2 hours. Based on this, the probability of the active attacker continuing his/her negative behaviour and dropping 25 packets in the next 3 hours was calculated using the Poisson distribution (μ (λ) = 15, e = 2.71, K = 25). The result is shown in Figure 4.7.

$P(X = K) = f(k) = \frac{e^{-\lambda}\lambda^{k}}{k!}$ $P(X = k) = \frac{(15)^{25} \times (2.71)^{-15}}{25!}$	P(X = k) = 0.0050

As compare to case one, the value of k (25) has been increased in this case, it also shows that more communication packets have been dropped in network. It also affected the results values of Poisson distribution 0.0050.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

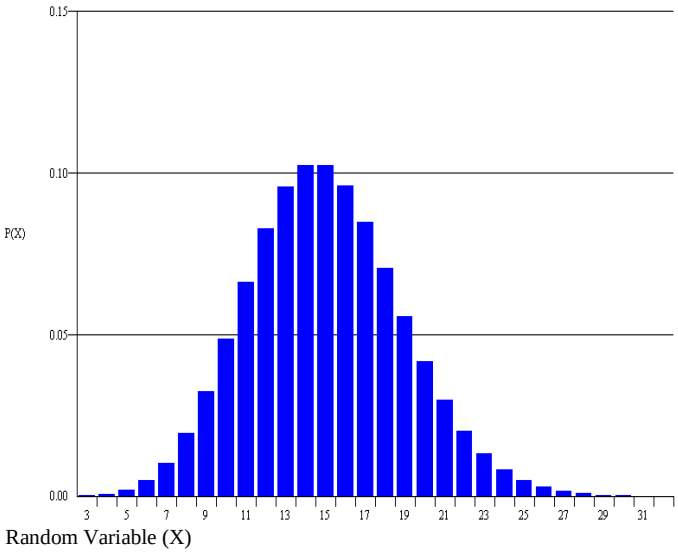


Figure 13.Random variable vs mean value of Poisson

Case 03: In Case 03, an insider attacker dropped 20 communication packets in 3 hours. So, what is the probability that the insider attacker will continue his/her negative behaviour and drop 35 packets in next 5 hours in the network? The following values (μ (λ) = 20, e = 2.71, K = 35) were inserted in the Poisson distribution and the results are shown in Figure 14.

$P(X = K) = f(k) = \frac{e^{-\lambda}\lambda^{k}}{k!}$ $P(X = k) = \frac{(20)^{35} \times (2.71)^{-20}}{35!}$	P(X = k) = 0.0007

In this case, the insider attacker dropped the maximum number of packets in the network; as a result, the values of the mean and standard deviation also increased compared to Case 01 and Case 02.

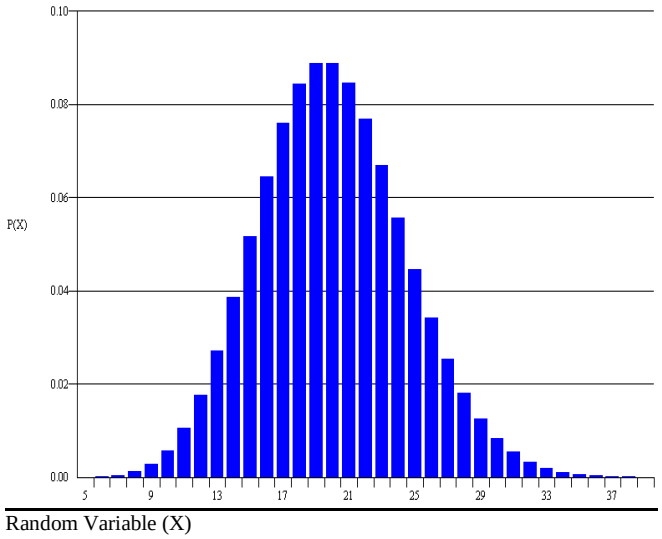


Figure 14. Random variable vs mean value of Poisson

Analysis of three Cases: In analyzing the three cases in table III, we can see that the other users of a network are affected due to the negative behaviour of an attacker. The more packets dropped (higher value of K), the lower the final value of P (X = k) becomes.

Table III ANALYSIS OF DIFFERENT VALUES OF **K**AND **λ**

Cases	Value of K	Value of λ	P(X = k)
01	15	10	0.0347
02	25	15	0.0050
03	35	20	0.0007

Network Simulator (NS-2) Simulation Section: NS-2 [12] is an open source discrete event network simulator and it provides the simulation environment for wired as well as wireless network. Academic researchers mostly use this simulator for their experiments and it is written in the C++ language. However, tool command language (TCL) is also suitable for communicating with this simulator. Many other simulators can be used to generate vehicle (node) description using any mobility simulator and mobility traces used in NS-2. Table IVprovides details of the simulation parameters of NS-2 in the proposed grades.

Table IV. SIMULATION PARAMETERS

Parameter	Values
Traffic	CBR
Transport Protocol	UDP
Packet size	512 bytes
Routing Protocol	AODV
Interface Queue Length	100 Packets
Propagation Model	Two-Ray Ground
Frequency Band	5.18 GHz
Inter vehicle distance	Maximum 1000 m
No of Lanes	3
Number of Nodes per Lane	50, 100, 150
Node distribution	Random
Number of Runs	20

Normal Communication: In a normal communication in the vehicular network, it only shows the user communicating with other users and there are no attackers in V2V and V2R communication. This is an ideal situation in the future vehicular network, where all the modules of the network work properly and users are able to send and receive safety and non-safety messages in V2V and V2R communication.A

communication which contains attackers was used to analyse the differences between attackers and normal users.

The behaviour of attackers on the basis of the proposed key features was used to differentiate normal users and attackers. Whenever a vehicle received any messages (safety or non-safety) from other vehicle or from the RSU then that message was checked against some proposed criteria. If that particular message fulfilled the proposed criteria, then it was considered a normal message and assigned Zero Grade (0); otherwise, it was assigned One Grade (1) and identified as an attacker message. Some of the criteria are given below.

Message Interval Time: In the vehicular network, the normal message interval time is 300 ms; if any user changes this time interval and holds the communication channels, he/she should be considered as an attacker.

Figure 4.9 explains in detail the Behaviors of a normal user and an attacker with respect to time intervals. In this case, a 300 ms threshold value was set for all users; some users changed their behaviour and held the communication channels, sending messages non-stop in the network. So the other users of the network dropped messages received beyond the threshold value and considered them as originating from a negative user (attacker).

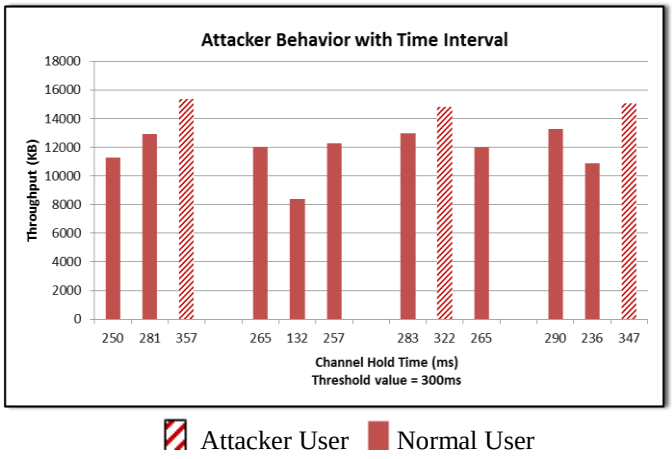


Figure 15. Attacker user with time interval of message

Speed of the Vehicle: This is a very important factor which is directly connected to accidents. Users who increase their speed over the safe limit will remain part of the network but will be considered as an attacker and network services will be made inaccessible to them.

Figure 16 shows the attacker behaviour with respect to speed. Node A started the communication but after 31 sec into the simulation, node A increased his/her speed; as a result, this user was allowed to remain part of the network but was considered an attacker, their packets were dropped and their throughput become zero. Whenever that particular node reduced his/her speed, then he/she became part of the network again.

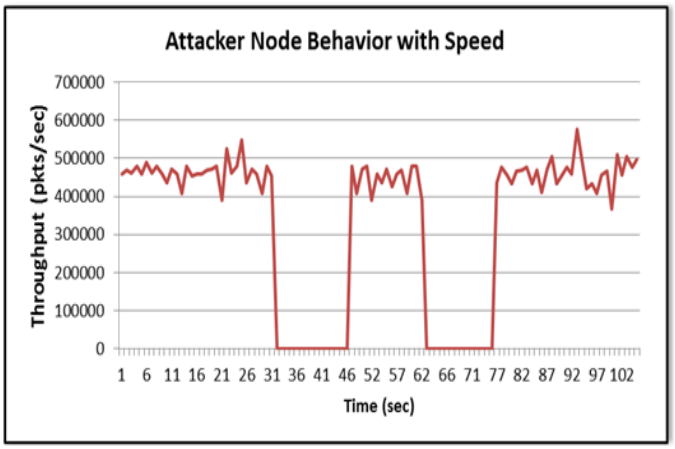


Figure 16Attacker user with speed of vehicle

The Figure 17 explains the scenario in which two users' behaviours were monitored throughout the whole simulation period. One of the users never changed their behaviour and maintained their speed but the other user changed his/her speed three times during the stimulation period. During the simulation time of 21 sec to 41 sec, this user's behaviour changed and his/her throughput value during this interval remained zero. At the simulation time of 41 sec, the user changed again his/her behaviour and remained so until 46 sec. In last time interval (66 sec to 81 sec), the user again increased the speed of his/her vehicle and the throughput value registered zero. Although the user remained part of the network but due to the change in speed, the proposed method dropped their throughput. Through this technique, the likelihood of road accidents can be controlled.

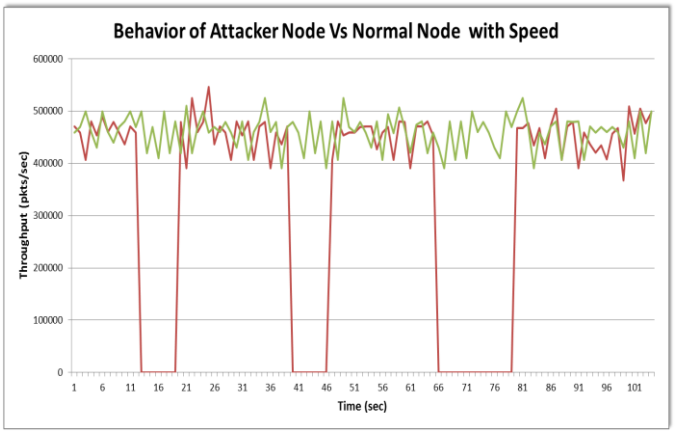


Figure 17Normal and Attacker user with speed of vehicle

Location of the vehicle: VANET mostly focuses on the road and its nodes only provide services in specific ranges of the road. If a user sends any message whereby the location of the sender is not specified then it should not be considered as a normal message and assigned a One Grade.

Figure 18 shows the third parameter used to differentiate normal users and attackers in a network. The first and second time slots showed normal packets but in the third time slot, there were some packets which were considered as originating from an attacker. In the simulation time of 70 sec, users

received many packets from attackers and this is the maximum number received throughout the whole simulation period. In the simulation time of 90 sec and 100 sec, users did not receive any packets from attackers. So, there is variation in receiving normal and attacker packets at different time intervals and also at different locations.

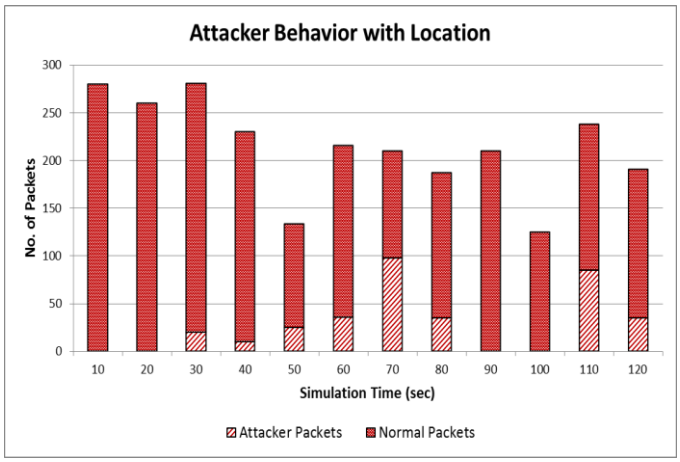


Figure 18. Attacker user with location

7. CONCLUSION

In this paper, we have analyzed the behavior of attacker in VANET by differentiating the attacker from the normal user. We also proposed to categorize traffic into two grades, i.e. normal traffic and attacker traffic on the basis of behavior analysis table. We hope that the proposed grades are helpful to identify attacks and understand behavior of attackers. It is difficult to detect and control attackers but in future work we would like to develop a prototype system to analyze the behavior of attackers in network. This would make it possible to reduce the negative impact of attacker in future life saving network.

ACKNOWLEDGMENT

This work is funded by Universiti Teknologi PETRONAS Postgraduate Assistantship Scheme.

REFERENCES

[1] B.Balacheff, L.Chen, S.Pearson, D.Plaquin, G.Proudler. In, S.Pearson ed, Trusted Computing Platform: TCPA technology in context. Prentice Hall PTR, Upper saddle river, NJ, 2003.

[2] M. Raya, J. Pierre, Hubaux,"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, january 2007, pp: 39-68.

[3] J. Cheambe, J. J. Tchouto, M. Gerlach "Security in Active Safety Applications" 2nd International workshop on Intelligent Transportation (WIT) 2005, Germany.

[4] A.Weimerskirch,J.J.Haas,Y.C.Hu,K.P.Laberteaux,"Data security in vehicular communication networks", chapter no.09, pp309-310.

[5] R. K. Schmidt, T. Leinmuller, E. Schoch, A. Held, and G. Schafer, "Vehicle behavior analysis to enhance security in vanets," in Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008), 2008.

[6] T. Leinm¨uller, R. K. Schmidt, E. Schoch, A. Held, and G. Sch¨afer, "Modeling roadside attacker behavior in vanets," in Proceedings of 3rd IEEE Workshop on Automotive Networking and Applications (AutoNet 2008), 2008.

[7] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," in Proceedings of the First ACM Workshop on Vehicular Ad Hoc Networks (VANET). Philadelphia, USA: ACM Press, Oct. 2004.

[8] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, 2007.

[9] E. Schoch, F. Kargl, M. Weber, T.Leinmuller, "Communication patterns in VANETs" IEEE Communications Magazine, Date:Nov 2008, Vol. 46, issue: 11, pp: 119-125.

[10] Sumra, I.A. Hasbullah, H.; bin Ab Manan, J.-L,"Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET)", 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 5-7 Oct. 2011.

[11] Y. Jiang; W. Tang, "Poisson distribution-based page updating prediction strategy", International Conference on Computer Science and Network Technology (ICCSNT), vol.2, pp.953,956, 24-26 Dec. 2011.

[12] NS-2 Available at http://www.isi.edu/nsnam/ns/

AUTHOR PROFILES

Irshad Ahmed Sumra received his Bachelor Degree in Computer Science from Islamia University Bahawalpur in 2001. He pursued his MSC and MS in communication and network from Bahria University Islamabad, Pakistan in 2002 - 2007. Currently he is PhD student in Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Perak, Malaysia. His research interest includes Intelligent Transportation System (ITS), Security and Trust in Vehicular Ad hoc Networks (VANET).

Assoc. Professor Halabi Bin Hasbullah received his Ph.D. degree in Electrical, Electronics and System Engineering from National University of Malaysia (Universiti Kebangsaan Malaysia), Malaysia in 2007. He is currently faculty member in the Department of Computer and Information Sciences at Universiti Teknologi PETRONAS. In the recent years, he has been involved in 4 research projects, inclusive VANET and VoIP. Dr. Halabi's current research interests include wireless sensor networks, Bluetooth radio networks, ad hoc wireless networks, mobile computing, and VANET.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Jamalul-lail Ab Manangraduated from the University of Sheffield, UK with a Bachelor in Electrical Engineering (B.Eng). He pursued his Master of Science (MSc) in Microprocessor Engineering from University of Bradford, UK and PhD in Communications Engineering from University of Strathclyde, Glasgow, UK. He is currently a Senior Director at Advanced Information Security Cluster, MIMOS Berhad. He has 18 years of experience in teaching Electrical and Electronics, Microprocessor Engineering and Network Security. He has many years of industrial experience as Network Engineer, Senior Manager and Senior Vice President in ICT based government lined companies in Malaysia. In MIMOS Berhad, his current research focus is Information Security, particularly in Trusted Computing and Privacy Enhancing Technologies.