INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 3, Issue 7, (2013) E-ISSN: 2222-6990

Minimization of Denial of services attacks in Vehicular Adhoc networking by applying different constraints

Amjad Khan

KARDAN University, Parwan II, Kabul Afghanistan,

Email: amjad@aup.edu.pk

Phone No: +93777771611, +923219033960

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v3-i7/88

Published Date: 28 July 2013

Abstract

The security of Vehicular ad hoc networking is of great importance as it involves serious life threats. Thus to provide secure communication amongst Vehicles on road, the conventional security system is not enough. It is necessary to prevent the network resources from wastage and give them protection against malicious nodes so that to ensure the data bandwidth availability to the legitimate nodes of the network. This work is related to provide a non conventional security system by introducing some constraints to minimize the DoS (Denial of services) especially data and bandwidth. The data packets received by a node in the network will pass through a number of tests and if any of the test fails, the node will drop those data packets and will not forward it anymore. Also if a node claims to be the nearest node for forwarding emergency messages then the sender can effectively identify the true or false status of the claim by using these constraints. Consequently the DoS(Denial of Services) attack is minimized by the instant availability of data without wasting the network resources.

Key words: Black hole attack, Grey hole attack, intransient traffic tempering

1. Introduction

To make the journey on roads threats free and sound and to provide necessary assistant to drivers, the new emerging field in the world of networking and communication is known as Vehicular Ad hoc Networking or simply VANET. It is a type of mobile ad hoc networks and besides Bluetooth is the first commercial application of MANET. The purpose of this type of network is not only to provide safe journey on roads but warning for the surrounding environmental change (e.g road sides covered by snow), sudden alteration occurs in the kinetics (emergency braking), road condition (congestion and construction), tourist information download, financial transactions like e-tags on toll plazas are also included in its applications. Thus indeed the vehicular communication need more security and privacy than the wired infrastructure networks and other Mobile ad hoc Networks (MANET) as it involves the direct human loss in case of an insecure communication.

The automobiles companies started to embed the IT(information technology) in the Vehicle so that they can easily communication with each others on roads to make each other aware about the road conditions and environmental hazards. To establish secure communication among Vehicles will not only solve different traffic problems but will also convey the emergency messages to the road side's buildings. In world wide researchers are studying different aspect of such type of communication in order to provide security and remove the existing threats in the Vehicular communication. In the United States, the Federal Communication Commission has allocated a bandwidth of seventy five mega hertz (75Mhz) for these applications, usually referred to as Dedicated Short Range Communications, and similar dedication are expected in other parts of the world. A lot of work has been done on the media access control protocol and the first layer protocol. To give generalized rules and regulations under the umbrella of IEEE(institute of electrical and electronic engineering) 802.11, many of the researcher around the world agreed upon the secure Vehicular communication. Keeping in view the advantages and benefits which will receive from such type of communication it is not difficult to predict that Vehicular communication will be emerged in the near future. If the manufacturer appropriately embed the hard ware devices for storage and processing like memory and on board processor along with those which are used for position identification like GPS(global positioning system) will revolutionalized the business world in the field of automobiles. But at the same time there certain security related threats, issues and challenges which need to be addressed and resolved. One of such type of security related problem is the DoS(Denial of Service) attack in VANET(Vehicular Ad hoc Wireless Network). Using the DoS (Denial of Services) attack the attacker prevents the legitimate node(Vehicle) of the network from being using the resources and data messages by different ways and ultimately the result may be more harmful and disastrous.

In this work DoS (Denial of Service) attack, its different types in Wired and Wireless Networks and the causes which act as a source of originating such type of attacks has been discussed. Different constraints and checks has been introduced to minimize the injection of data packets from a spoof node in the network. By doing so the DoS attack can not be eliminated completely but to some extent minimize the probability of such type of attacks.

2. Literature Review

The purpose of this chapter is know about the wireless network, its different types and the real security related issues present in the Mobile Ad hoc Network specifically in VANET(Vehicular Ad hoc Networking). But before discussing the VANET and different security related problems in this network, especially DoS(Denial of Services) attack, first we need to know about the wireless network and its different types with respect to its infrastructure.

2.1 Wireless Network

It is that type of network in which the nodes (computers, network devices) are connected with each other without the need of wires. In this type of network the nodes uses the radio frequency signals for communication with each others.

Suppose we have two (02) computers each equipped with wireless adapter and we have set up wireless router. When the computer send out the data, the binary data will be encoded to radio frequency and transmitted via wireless router which is also known as access point . The receiving computer will then decode the signal back to

binary data. Mainly this wireless network can be categorized into two categories stated as under:

i. Structured Wireless Network
ii. Unstructured Wireless Network (Without proper infra structure)

2.1.1 Structured Wireless Network

It is that type of Wireless Network which have proper infra structure and before setting up such type of network, we need to conduct proper location survey. This location survey will help us to determine the exact location of the network nodes and the signals frequency rang that we will use for the communication purpose. There will be Wireless routers located at proper positions and will act as back bone for wireless communication. The communication of such type of network would be controlled by the proper nodes configuration. We need to configure each of the node for proper communication by the operating system.

2.1.2 Unstructured Wireless Network (Ad hoc)

It is that type of Wireless network which have no proper infra structure and thus termed as Ad hoc network. Using this network the devices can sense each other automatically and start communication with each other. Usually this type of network we deploy in the disastrous area on emergency bases e.g those areas hit by the earth quack or tsunami, or in the battle field where the whole available infra structure has already been destroyed. This type of network is also known as MANET(Mobile Ad hoc Network). So far there is only one commercial application of such type network, known as Bluetooth.

There are projects such as Berkeley PATH(2002) “California partner for advance transit and highways” in USA and Fleet Net(2002) “Internet on the road” in Germany on vehicular communication, but these projects possess lack of security and privacy, thus many projects were launched by the European Commission in this decade to make the VANET as secure as it should be. These projects includes PRevent (Preventive safety) (2003) “Preventive and safety applications”, SafSpot (Cooperation for road safety) (2003) “Cooperative Vehicles infrastructure for road Safety”, CVIS (Cooperation for traffic efficiency) (2003) “Cooperative Vehicles infrastructure System”, and COOPERS (seamless services along the travel chain) (2003) “Cooperative network for intelligent road safety”. These projects offer limited security and thus cannot be considered for implementation. Another European funded project named SEVECOM (Secure Vehicular Communication) is also trying to identify the security related issues, find ways to remove these problems and give it practical shape by implementing it in the real world. But much more work is still to be done in term of security and many more challenges are there need to be addressed and resolved.

2.2 Denial of Services attack (DoS):

In all kinds of network, availability of data and other resources is a big challenge and in case of VANET the unavailability of resources in emergency situation (e.g., in emergency breaking), leads to a disastrous situation. The unavailability of data packets or any other network resource by any mean is known as denial of services and if this Denial of services

is done by a node in the network intentionally then it becomes an attack which is called denial of services attack or simply DoS attack. This work will mainly emphasize to prevent the denial of service attacks or at least to minimize these attacks. The DoS attacks are mainly caused by the jamming problem, so also this problem is studied in detail and ways are suggested in the coming sections to eliminate or at least minimize the jamming problem and ensure the availability of data packets in the Vehicular Ad hoc Wireless Network by mean of introducing new fields in the packet type suggested in T.Leimuller et al (2006) "Improved Security in Geographic Ad hoc Routing through autonomous position verification", IEEE-2006. In this type of network the vehicles are moving at a very high speed so there will be contact among the vehicles for very short time so the strict time constraints in term of availability are also described in this work.

2.3 DoS (Denial of Services) attacks in Vehicular Ad hoc Wireless Network:

Denial of Services (DoS) attacks not only targets the wired Network but they are mostly occurs in the Wireless Network also, especially if the Wireless Network is ad hoc and having no proper infra structure. So such type of network is considered to be more vulnerable for DoS (Denial of Services) attacks.

C.Harsh et al (2007) "Secure Position based Routing protocol for VANET" IEEE-2007) described the most probably DoS (Denial of Services) attacks that occurs in the VANET and is summarized below:

a. Waste / Exhaust of bandwidth of the wireless Channel.
b. Create the false location table entries in the node (cars).
c. Physical Jamming
d. Black-hole attacks in which the DoS attack drop all of the packets.
e. Grayhole attack in which DoS attack drop selected packets and deny it from its destination.
f. Create routing sinkhole and drop messages.
g. Create routing loops
h. Inject fake reply with wrong position to a location.

M.Raya and J-P. Hubaux (November-2005) "The Security of Vehicular Ad hoc Networks", IEEE-2005 presented the attacker model in VANET and it will clarify the concept more for understanding the DoS type of attack in VANET.

2.3.1 Legal vs Non legal:

The legal is an authenticated member of the network that can communicate with other members.

M.Raya, J-P. Hubaux (March-2005) "Security Aspects of inter Vehicular communication", IEEE-2005 examined the legal node of the network having a certified public key and thus considered as legitimate user.

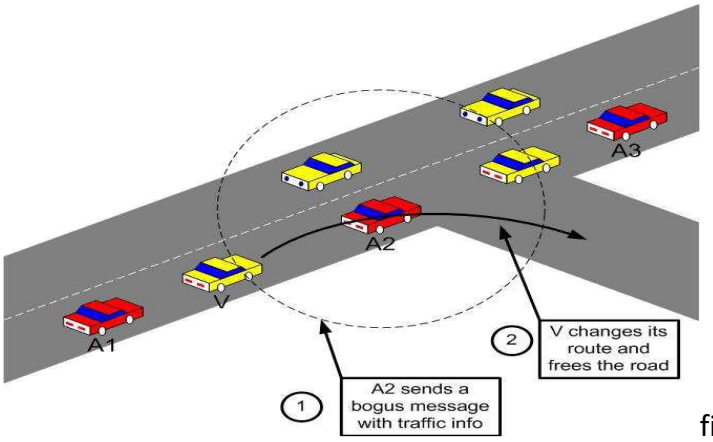


fig: 2.1

In the above diagram the attackers A2 and A3 passes false messages to each-others and in this way they tried to compel the legitimate user of and the network V to take wrong decision clear the road for another attacker A1.

If the legal node start misuses of network specific protocols then they will become the main source of unavailability of data and other resources rather than intruders who will be limited in the diversity of attacks.

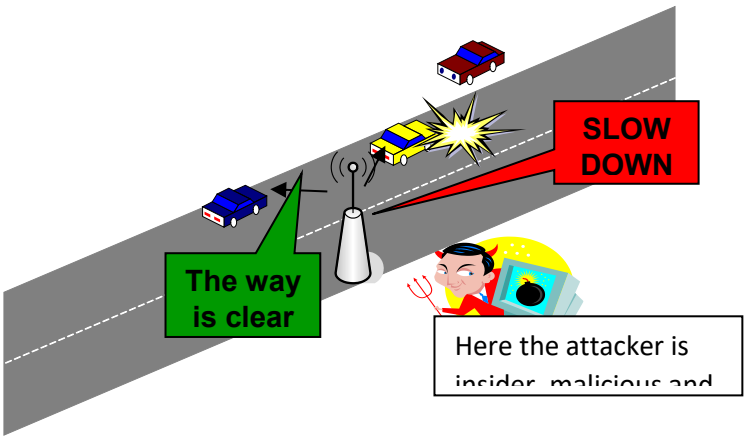


Fig: 2.2

The non legal will be an intruder which will enter into the network from outside.

2.3.2 Malicious vs Rational:

A problematic individual who don't seek any personal benefits but his aim is just to disturb the members of network by injecting data packets in the network on regular bases and its functionalities is called a malicious. An individual who seek his personal benefits and try for attack is called Rational and hence such type of attacker can easily be identified. On the other hand a malicious can adopt any mean for disregarding corresponding cost and consequences and thus would play an important and frequent role in DoS attacks.

2.3.3 Active vs Passive:

An active attacker can generate messages or signals and a Passive attacker just contents himself with eavesdropping on the wireless channel. Thus an active attacker can cause the jamming problem more frequently by generating packets repeatedly rather than the Passive attackers who will just listen and read the communication between two legitimate users without generating its own messages. The attacker launches the DoS attack to waste the network resources and prevent the data packets from reaching to its correct destination. These attacks include

2.3.3a. Jamming:

In this type of attack the problematic user of the network intentionally inject data packets at very high rate to occupy the available bandwidth and thus prevent other users from communication. A malicious node can create this problem for the network user at a very lower cost.

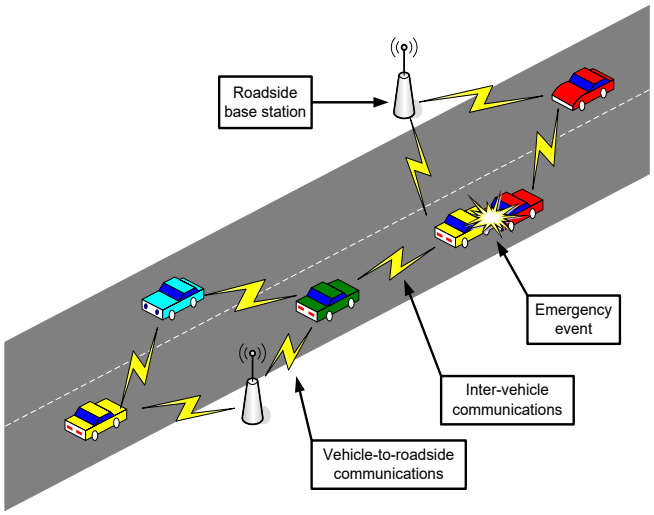


Fig: 2.3

2.3.3(b) In-Transient traffic tampering.

If a node (Vehicle) which acts as a message forwarder , intercept the message of other nodes and modify its meaning. It become more harmful if it modify the critical traffic related information. It can be viewed as a type of Black hole attack where a malicious node (vehicle in this case) show itself as the shortest path towards destination by sending false information and thus cause the problem of unavailability of valuable data.

2.3.3(c) Impersonation.

To intercept the message and prevent it from further forwarding, drop all incoming messages or change the meaning of the valuable information and give false reply to the sender will lead to impersonation. (E.g. To pretend as an ambulance)

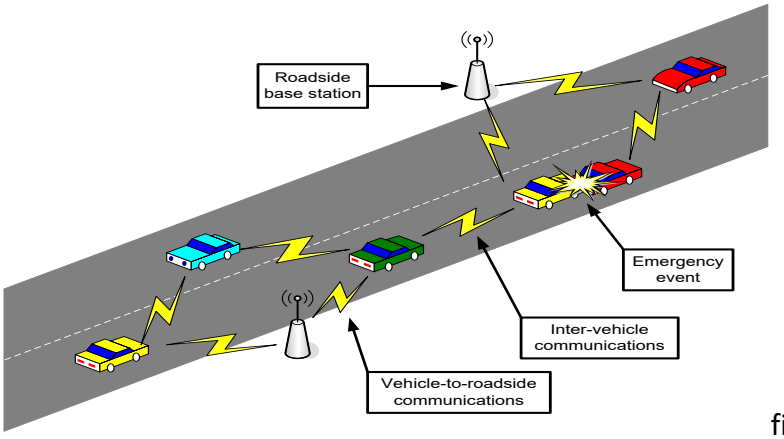


fig:2.4

Not much work had been done to solve the DoS (Denial of Services) attacks in VANET(Vehicular Ad hoc Wireless Network). Almost 80 percent of the work is done to identify the security threats, challenges and the issues arise at the time of implementation of such type of network. As it is the new emerging player of the team of Ad hoc wireless network so most of the researchers tried to find and identify those issues which are still unidentified and still possible if the network is implemented.

M.Raya et al(April-2006) “Securing Vehicular networks”, IEEE-2006, I. Aad, J-P.Hubaux (2006), “Impact of Denial of Services attack on Ad hoc Networks” emphasized on the solution of DoS (Denial of Services) attacks. They mainly concentrate on the authenticity of messages. Mainly uses the digital signature and certification for the authenticity to resolve or at least minimize the DoS(Denial of Services) attacks.

I.Aad, J-P. Hubaux (2006) “Impact of Denial of Services attacks on Ad hoc Networks” described two major DoS(Denial of Services) attacks i.e. JellyFish attack and Black hole attack. The key principle that JF use to facilitate the attack is targeting end-to end Congestion control. The authors also motioned the JF Reorder, JF Periodic Dropping and JF variance as subtypes of JellyFish attacks and their impacts on transmission throughput.

M.A.Sharman, S.M.YOO (2004) “Black hole attack on Mobile Ad hoc Networks” examined that type of attack in which a node intercept all incoming messages and completely drop them with out any further forwarding is another serious security problem. In which a malicious node uses the routing protocol to advertise itself as having the shortest path to node whose packet its want to intercept. If a legitimate node of the network advertises a request in search of shortest path towards destination and if a problematic node sends a reply to this node consist of false location then a bogus and unrealistic route will establish between the problematic and legitimate nodes. The legitimate node will send all messages to malicious node, now it’s the job of malicious node either to create the DoS(denial of services) attack by dropping all data packets or further broad cost these to disclose the privacy of the sender. The author also proposed two solutions to encounter the black hole attack. The first solution is to establish more than one route to destination for secure data transmission but the main drawback of this solution is the time delay.

The second proposed solution for black hole attack is based on the sequence number included in any packet header. This number is an increasing value i:e the next packet have higher value that the current packet sequence number. But the main drawback of this solution

is to have two extra tables. But in VANET this is not an issue as the vehicle can have not only large amount of memory but also fast computation resources and power.

S.Kurosawa et al(2005) "Detecting Black hole attack on AODV based mobile Ad hoc Network by dynamic learning" IEEE-2005, described the mechanism used for the detection of black hole attack is the usage of AODV (Ad hoc on demand wireless) protocol and dynamic learning method. In AODV, Dst-seq is used to determine the freshness of routing information contained in the message from originating node. When generating a RREP message, a destination node compares its current sequence number and Dst-Seq in RREP packet plus one, and then selects the larger one as RREP's Dst-Seq. Upon receiving a number of RREP, a source node selects the one with greatest Dst-Seq in order to construct a route. To succeed in the black hole attack the attacker must generate its RREP with Dst-Seq greater than the Dst-Seq of the destination node. It is possible for the attacker to find out the Dst-Seq number from the RREQ packet. In general the attacker can set the value of its RRDP's Dst-Seq based on the received RREQ's Dst-Seq. However, this RREQ's Dst-Seq may not present the current Dst-Seq number of the destination node. Sybil attacks have been regarded as a serious security threat to ad hoc networks and sensor networks. They may also impair the potential applications of VANETs (Vehicular Ad hoc Networks) by creating an illusion of traffic congestion that leads to DoS(Denial of Services).

B. Xiao (Sept-2006) "Detection and localization of Sybil Nodes in VANET" examined and tried to detect and locate the Sybil node in VANET. The authors proposed two algorithms based on the signal strength distribution of a suspect node over a period of time to locate the accurate position of a Sybil node.

The DoS(Denial of Services) attack is very critical and their effect can be devastating that is bringing down the whole network. Therefore one should find the way to eliminate or at least minimize these types of attacks. Existing solutions like frequency hopping don't completely solve the problem.

C. Harsch et al(2007), "Secure Position Based Routing Protocol for VANET", IEEE-2007 mainly emphasized on the protection and security of network operation by providing security to the position-based routing functionality and service .The author tried to achieve this by using the PBR (Position-based routing protocol) and by introducing new plausibility checks with those described earlier. These new constraints will impose such a restrictions on the network participating nodes so that no node would be in the position to occupy the whole bandwidth or produce the DoS(Denial of Services) attack easily. New plausibility checks need to be introduced to handle the DOS(DENIEL OF SERVICES) attack and to make the packet reach to its correct destination.

The author also introduced the concept of rate limitation for packet forwarding in which there must be a protocol specific threshold. If the rate of false multi-hop flood or broad or geocast exceeds from that specific threshold then those packets will not be forwarded any further. This will not only prevent the injection of false multi-hop flood but it will also prevent the network resource from wastage in a large network.

C. Harsch et al(2007), "Secure Position Based Routing Protocol for VANET", IEEE-2007, helped to prevent the network operation but did not reflect the real world scenario of roads .Using this of PBR, the vehicles must know its geographic position by GPS.While in congested area like high story buildings, valleys and jungles this device didn't show performance. Thus the question arises when the node don't know about its correct position by GPS, what will be the source that provide information to the node about its position? If no such sources available then its implementation and deployment will be almost impossible. Hence we need

not only the alternative means to be identified that provide the correct position to a particular node thus to avoid or at least minimize the DoS attack in VANET.

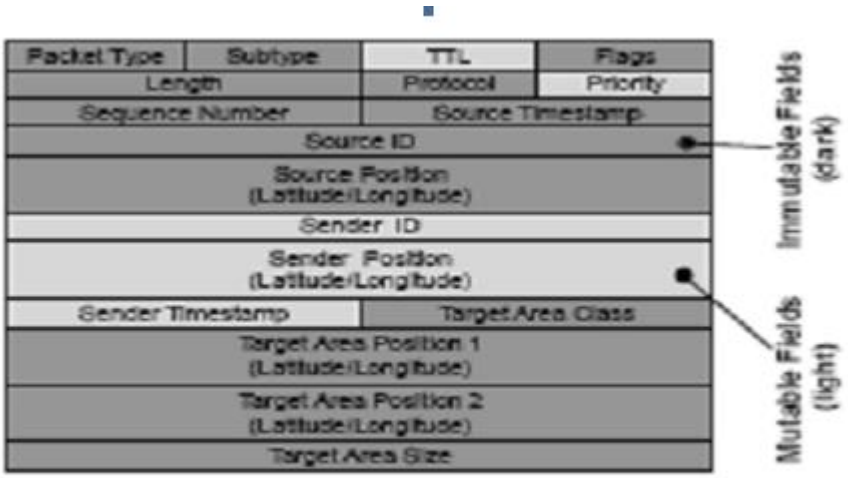


Table-1: 2.1 changeable and unchangeable fields

To eliminate or at least minimize the DOS attack in the VANET, it is necessary to authenticate the reply comes from a destination. When a node broadcast a message in search of a destination node it must validate the reply comes to it .Indeed the authentication mechanism in this case is the backbone of security in term of DoS attacks. For authentication each message must be signed by the sender and forwarders and must attach the digital certificate with the message transmitted to destination. There must be a certification authority CA and vehicles participating in the network must be registered with that CA.But usually in practice to apply the authentication mechanism based on pseudonyms help to provide authentication without losting privacy.

G. Calandriello et al (Sept-2007), "Efficient and Robust Pseudonymous authentication in VANET", IEEE-2007 assumed that each node V is equipped with a set of pseudonyms that is public key certified by CA without any information identifying V.The message format in this case will be

$$m, \delta kiv\ (m), kiv, CertCA\ (kiv\ )$$

Here in this pseudonyms will be provided to a node. When the message comes as mentioned above, the CA can only identify the signer of the message, as the CA maintains a map from the long term identity of V. As in this case the privacy of the particular signer will disclose, so the idea of group signature is introduced in the paper. In group signature each node have a secrete group signing key (gsk). There will be a group public key gpkCA which will be used for the validation of group signature generated by a group member. Intuitively, a group signature scheme allows any node V to sign a message on behalf of the group without revealing the identity of V (signer of message in this case). Although this mechanism is efficient and robust for authentication and it also kept the privacy of a node but the discrepancy lies in the group formation. All the registered nodes with CA will be the members of the group. There is no boundary for the group specified in the paper. Also it is not mentioned that the CA will be local administration or it will supervise a wide geographic area. If the CA is local administrative and control a small geographic area then the mechanism of

group signature can not be applied to those vehicles moving frequently from one geographic area to another or between two cities. In our work we will emphasize to form the group and apply the same group signature mechanism, but the group from those nodes which are in the transmission range of the sender and also register with the CA.

M.Raya, A. Aziz (Sept-2006), "Efficient Secure aggregation in VANET", IEEE-2006 work has been enhances for authentication of messages by applying the techniques of group formation and secure message aggregation. The security architecture proposed in this paper is based on symmetric, asymmetric and Mix cryptographic mechanisms in which every message would have to be signed for the receiver to provide maximum authenticity and thus reduce the chances of black-hole attack, wormhole attack and replay attacks.

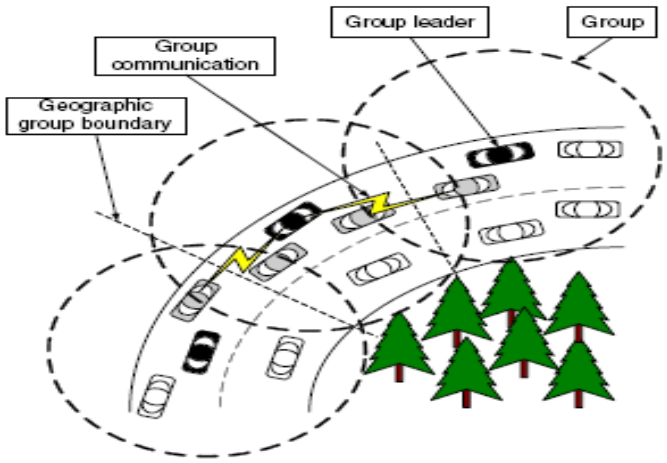


Figure 1.5: Efficient aggregation by means of overlap-ping groups. Communication between the two outer groups is possible because at least the leader of the center group is in reach of relaying vehicles (in grey) in both outer groups.

In the proposed system model, the most important is the SVGP (Secure vanet group protocol). In which instead of periodically broadcast a certified public key, the group leader (L) will distribute the group key k to members A, B and C encrypted with their respective public keys as follow

L →*: {K} PuKA, {K} PuKB , {K} PuKC ,
SigPrK L [{K} PuKA, {K} PuKB, {K} PuKC]

Subsequent message broadcast will include only HMAC in addition to message itself.

L→*:m,HMACk (m)

When a new vehicle D enter into cell it receives the group key from the group leader

L→D :{ k} PuKD ,SigPrK L[{k} PuKD]

Although this approach minimize the problem of secure position based networking but still we can assume that all the participant of the group will not be honest. Also no strick rules are defined for the group leader and anyone can become the group leaders who will at the center or near the center of the group–cell. Thus what would be the situation of the group leader is dishonest node of the network. Definitely again the same problem will repeat.

Another problem that arises at the time of deployment of this model is the static and dynamic behavior of the group-cell boundaries. If the boundaries of the group-cell are static

then speed at which the vehicles passes through a certain group-cell, the group leader will remains just for a few seconds and will pass through the center at any given instant of time. Thus in 1second two or more vehicles will play the role of a group leader and creating more overheads which certainly reduce the performance of network. To eliminate this problem a suitable and practical solution will be to select the group leader for each group-cell from the road side infrastructure which not only play the role of leader but also responsible for identifying dishonest node. We will describe the solution for this problem in detail in the next section (problem solution) in detail but in short to control the ad hoc vehicular network DOS attacks, the infrastructure network should be used, i.e. to provide the security to infrastructure less network by infrastructure network. Hence we need to adopt the unconventional methods for minimization of DoS attack and not only rely on the conventional protocol solution.

3. Methodology

VANET is a new emerging area of Ad hoc wireless network and so far no practical and secure model of the network is available to deploy it and implement it in today's world. This is just because of the security related threats and attacks that the network is planned to implement at the end of this decade. One of such type of problems is the DoS attack in which the critical information is made unavailable to the destination node and intercepted in the middle of the transmission. As Vehicles are the nodes in VAnet and if one vehicle try to send valid and critical information to another vehicle, it is not cent percent guaranteed that the information will reach to its correct destination without alteration in the middle. Consequently this will lead to the serious DoS problems described as under:

3.1 Attacks on Financial Transactions:
A considerable number of IVC (inter vehicular communication) applications will involve financial transactions e.g. for toll collection, payment for location-based services and insurance. A successful DoS attack will definitely leads to a set of serous financial frauds that leverage on the open nature of wireless communication.

3.3 Attacks on Driver Safety:
Safety related applications are major incentives behind the development of the VAnet and thus its security is most important. When a vehicle passes safety related information to another vehicle and due to DoS(Denial of Services) attack this information not reach to its destination , then a disastrous situation will arise that leads to an incident and losses of lives.
3.4 Suspicious user who receive packets:
In this type of attack a problematic user can show itself as the least displacement towards the receptor. Thus a legitimate user would like to send packet to some other user via the malicious node. Thus this malicious user can create the following two problems and prevent the packet to reach to its correct destination.

3.4.1 **Black hole attack**:
In this DoS(Denial of Services) attack the malicious node can drop all the packets that it can receive and thus can deprived the actual receiver of the packets from receiving the critical information.

3.4.2 Gray hole attack:

In this DoS(Denial of Services) attack the malicious node can drop selected data messages and can deprived the actual receiver of the messages from selected data packets.

3.4.3 DoS attack by Jamming:

In this type of DoS attack the problematic but the legitimate participant of the network present its false location and can inject the data packets in the network at such a large scale that it will occupy the whole bandwidth of the network and thus cause the problem of jamming. Due to this jamming problem, important information would not be able to reach to its destination.

3.4.4 To create false location table entries:

In this type of DoS attack, the malicious node can send a packet in which he can put false location information in its mutable field of the packet and then perform the following

i. Inject messages with false source or sender position
ii. Forward messages and alter source/sender ID's.
iii. Reply previous heard packet.

3.4.5 Routing Loop problem:

Another serious DoS problem in VAnet arises in order to create routing loop or

i. Forward data messages on non greedy route
ii. Inject data packets to show the wrong position of Node.

All the above mentioned DoS problems make it impractical to deploy the VAnet in its real since. Thus this work is an attempt to minimize these DoS attacks if not fully vanish.

The table-1 simplified the expecting DoS attacks in VANET.

1. Waste / Exhaust resources (OR)
   - 1.1 Waste / Exhaust bandwidth of the wireless Channel (OR)
   - 1.2 Create false location table entries in node (OR)
     - 1.2.1 Inject messages with false source or sender position ID
     - 1.2.2 Forward message and alter source or sender position ID
     - 1.2.3 Reply previously heard packets
2. Deter node from packet reception (OR)
   - 2.1 Physical jamming
   - 2.2 Drop all data messages
   - 2.3 Drop selected data messages
   - 2.4 Create routing sinkhole AND drop messages (AND)
     - 2.4.1 Inject different beacon messages with false position ID
     - 2.4.2 Drop data messages
   - 2.5 Create routing loops
     - 2.5.1 Forward data messages on non greedy route
     - 2.5.2 Inject beacons with false position
   - 2.6 Inject fake reply with wrong position to a location request

3.5 Methodology used:

The methodology used for the completion of this research work, consist on the following sequential steps.

3.5.1 Hypothesis (Research questions):

In this step a set of questions have been produced and checked the current available model for security from DoS type of attacks. After that the model has been modified and the same set of questions has been checked again. It has noticed that the modified model gave much satisfactory results as compare to the previous one. The set of questions are as under:

i. How much bandwidth has been consumed?
ii. How many packets have been dropped?
iii. How many packets reached to the correct destination?
iv. How many packets intercepted by the malicious node?
v. How many times the routing loop problem raise?
vi. The packets reached to the correct destination are modified or not, if modified then how much?

3.5.2 Design Experiments:

In this step different values are assigned to parameter list along with the condition of roads in city as well as on the highways/motorways. The parameter list and their values are summarized in the following table.

Table 3.2

Parameters List	Values
Transmission(Rmax)	250 meters
No of messages(packets) sent	100
Simulation per parameter set	15
Condition of City	
Number of nodes	100
Distance for nodes in square	1000---4000 meters
Number of Vehicles(density)	625 to 100
Maximum speed of Vehicles in meter per second	50
Break time in seconds	0.0
Mobility Model	Random waypoint
Time spent on each result in seconds	40
Highways / Motorways Conditions	
Number of Vehicles	Approximately 350
Each direction lines	2
Distance travelled on road in kilometers	12
Time spent on each result in seconds	120

3.5.3 Data Collection:

The data has been collected from the design experiment. Messages have sent from one node to anther using the Radio signal frequencies. On the sending end the data packets which were in binary form have been encoded into radio signals while on the receiving end these have been decoded. It has been checked that the receiving messages are correct or modified? Also it has been checked to which extent these messages are correct.

3.5.4 Data analysis:

The ns-2 simulator has been used for checking and analyzing the results. In chapter-V the result of false position and number packets reached to destination has be given. Also the number of packets received by problematic user is given over there in detail. From the analysis of these results obtained by ns-2 simulator, it is clear that the DoS attack in VANET has been significantly minimized.

4.1 Implementation:

Different solution have been proposed in order to completely eliminate or at least minimize the impact of DoS(Denial of Services) attack in VANET(Vehicular Ad hoc Wireless Networks).To check that the sender is a legitimate user of the network, different techniques and mechanism has been used. The digital signature and protocol identification are two of them. But in all these techniques there is little emphasize on the consumption of network bandwidth. Thus for the minimization of DoS(Denial of Services) attack in such type of network, first we should prevent the unnecessary bandwidth consumption. For this assume that a Vehicle is a node which have a location table where the vehicles can record its current location and the location of those nodes from where the packets originates. Also the packet header must consist of fields to store the sending time and receiving time.

4.2 Bandwidth Consumption Prevention:

if a problematic node in the network continuously injects false data packets in the network, will waste the network resources including bandwidth. In order to prevent the false packet injection in the network, the following constraint must be imposed in VANET (Vehicular ad hoc Networking).

4.3 Limiting Packet Injection Rate:

Let Np denotes the number of packets which we want to send from the source node to some destination and let T is the amount of time during which a node can transmit the specific amount of packets. The value of Np is different for different kinds of Vehicles so that to avoid the inconvenience of such type of checks.

For example the value of Np for private vehicles will be 1, for public Vehicles such as POLICE, ARMY and WAPDA(Water and Power development authority) its value should be 10 and in the same way the value of Np for rescue Vehicles like ambulances and Red cross should be higher than all these and it must be 20.

Initially Np=1 and T=1 (while T should be measured in minutes)

Let A is a type of node, Np is the number of packets, T is the amount of time in minutes then the algorithm for limiting the packet injection rate as under:

```
If(A==”private”)    \\   A may be either private , public or Rescue
{
        If(Np > T)        \\ private vehicle can transmit only one packet in one minute
                Drop Np;
}
Else
```

```
        {
         If(A==”public”)
                {
                If(Np > T+9)    \\ public vehicle can transmit 10 packets in one minute
                        Drop Np;
                }
         Else
                {
                If(A==”Rescue”)
                        {
                        If(Np>T+19)     // While Rescue vehicle can transmit 20 packets in one
minute
                                Drop Np;
                        }
                Else
            Allow(Np);
}
}
```

4.4 Defining Maximum Rang for accepting packets:

Another constraint to avoid the injection of false packets from a legitimate node is to specify the maximum range between vehicles where with in which they are allowed to communicate with each other. As we know that each transmission signal can travel up to certain distance after which the signal become weak and attenuation occurs. According we can assume that each radio signal have some strength with in which the nodes can communicate with each others and if this limit crosses then the nodes would no longer able to communicate with each others. Depend upon the facts that which frequency radio signal will be used for communication we can easily make an approximation for communication range between the nodes denoted by Rmax.

Suppose b is a packet received by a node X from the node Y. Suppose X knows the current position of node Y as well as its own current position with the help of GPS (Global Positioning System) and has stored these information in the location table of node X. Then the algorithm for maximum acceptance range is as under:

```
        X= receive(y)
        If (distance (y.location, X, position) < = Rmax)
{If (y.original != X.Tx)
{X.Tx= y. original;
X.Tx= y.location;}
else
X.Tx[i]=y.location;}
else
{trustY - -;drop (y);}
```

Where distance routine calculate the distance between the position of X and Y. Tx is the location table of node X and the drop ( ) routine ignore the packet forwarding.

By applying the above algorithm we can prevent the network from many types of attacks including the DoS. If the distance between two nodes is greater than Rmax and in this case one of the node show itself as a better forwarder then it is not trustful and will be

considered as malicious node. So its trust level will get drop automatically by this constraint and consequently will minimize the DoS possibility.

An important problem that usually occurs in such type of networks is when a node X wants to send data packets to node Z but through many paths the same data packets reach back to the sender X instead of node Z and thus create the routing loop problem. By the introduction of this constraint such a problem can also be resolved easily.

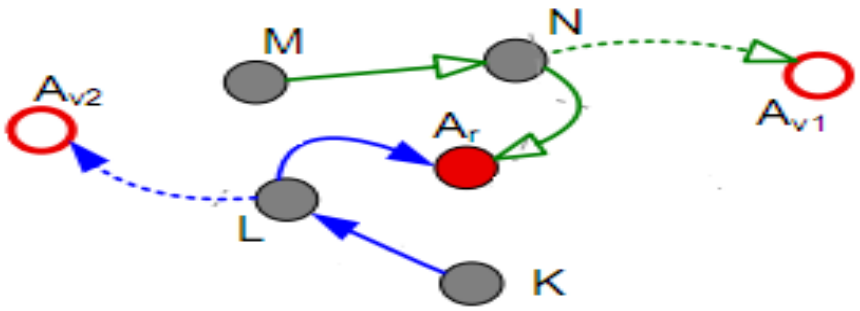
4.5 Defining Maximum Speed (Vmax):

We can also apply this constraint in order to prevent a node from injecting continuous messages in the network and consequently can prevent the bandwidth from unnecessary wastage. As we know that maximum speed has been fixed for all Vehicles on different roads. The vehicles moving on the Motorways and Highways have greater maximum speed while the Vehicles move inside the city and street having less maximum speed limit. Thus using this constraint if a node X receives a message from a node Y then it will record and store the time of the message. If node X receives another message from the same node Y, than it will check the time interval between the two messages. Depend upon the time interval between two message nodes X will calculate the speed of the Node Y. if this speed is greater than Vmax than the message of node Y will get discarded.

Fig 4.1: Maximum Speed

P1 packet from M toN

P2 Packet from K to L



For the clear understanding of this type of constraint, consider fig1. The maximum speed constraint can also prevent a node which constantly changes its location in order to intercept and then prevent the data packet from forwarding so that not to reach to its correct destination. For example in the above diagram a node M wants to send data packet to another node N. But a problematic node A whose real location is Ar, advertise its false location as Av1. Thus when N further forwards the same data packet, N will choose Av1 as the next forwarder. In the same way this problematic node can also change again its position to be at Av2 so that to intercept another packet and prevent it from further forwarding. Thus when we introduce such a constraint that each node will have some pre defined maximum speed so no node can change its location continuously and consequently will minimize the chances of packet interception and dropping.

The algorithm for such type constraint implementation is as under:

```
X. Receive(y)
    If (y.original does not belong to X Tx)
        X.Tx= y.original;
```

```
        X.Tx= y.location;
 ELT = find (y.original) in X.Tx;
V= disatnce(y.location, ELT.location) / (t-ELT . Time);
If (V< = Vmaximum)
                    ELT.location= y.location;
                  ELT.Time = t;
else
         trustY- -;
        drop(y);
```

Where Node X receives beacon y from node Y
y.original stands for the location of Vehicle Y
X.Tx stands for the location table of Vehicle X
ELT stands for entries in location table of a particular node
V denotes the speed between two different locations in the network.
Vmaximum is the pre defined maximum speed of the Vehicle which it shouldn't cross.
Where t shows current time and ELT. Time show the time in which, a particular Vehicle had sent last message.

4.6 Defining Higher density(HDHH):

As we know that Vehicles which have the same properties and dimensions in term of Vehicle type(car, bus, truck, trailer etc), model, colors and engine power usually less in number operating on a road or inside the city. If in a city or on the road the number of such Vehicles increase from a specified amount then it will show the higher density. Thus any message or request send by such Vehicles on the same road or in the same city will be rejected if their numbers increases from the higher density limit. The density of such Vehicles is usually low which are running at a higher speed. We should also consider the purchasing power of the citizen of a particular area. In the rich countries the purchasing power of people is mostly higher than those who are living the third world countries. Thus accordingly we must define the higher density limit.

4.7 The usage of map as a constraint:

We assume that each Vehicle on the road having navigation system where the maps of roads, cities and streets are easy accessible. Thus from the map a legitimate node of the network can easily predict the accurate location of the node which show its location ideal one i:e to be the best forwarder, while in reality that indicate its false and bogus location. Thus map technique can be used for the detection of a node which is not in the neighboring area or on the road.

4.8 Time Interval:

When a packet is received by a node then the mechanism to identify the packet as a new one is the Time. When a node receives the data packet, it records its time. When the same node receive the same packet again then it will check its previous time and will accept it for forwarding if it's new one and does lies in the past. If a packet header is not new then the node need not to update its time table. The table where the node record the time of the data packet should be modified if and only if all the information in the packet are new one and there is no previous entry in the time table of the node regarding data packet. Such a packet should be dropped and avoid its forwarding if the node time table having an entry related to the same packet one or two hours before.

Results and Discussion

5.1 Criteria for Simulation:

ns-2 simulator has been used for checking the results of the proposed constraints. The following criteria have been set for analyzing the simulation results.

5.2 Protocol:

For forwarding a packet the greedy routing algorithm has been used to choose the nearest node for forwarding a packet to its destination. If no closest node is available for forwarding then the packet is temporarily stored in the buffer and retransmits as soon as the suitable closest forwarding node is available. If many packets stored in the buffer and there is no room for storing a next packet then the packets dropping starts. For dropping the packets the FI FO (first in first out) algorithm is used.

5.3 Level of Trust:

Initially each packet received from the node is considered as valid data packet initiated by a legitimate node of the network. So value of trust level initially set to zero (0). After executing each constraint it on the packet and its source, the level of trust may either increased or decreased.

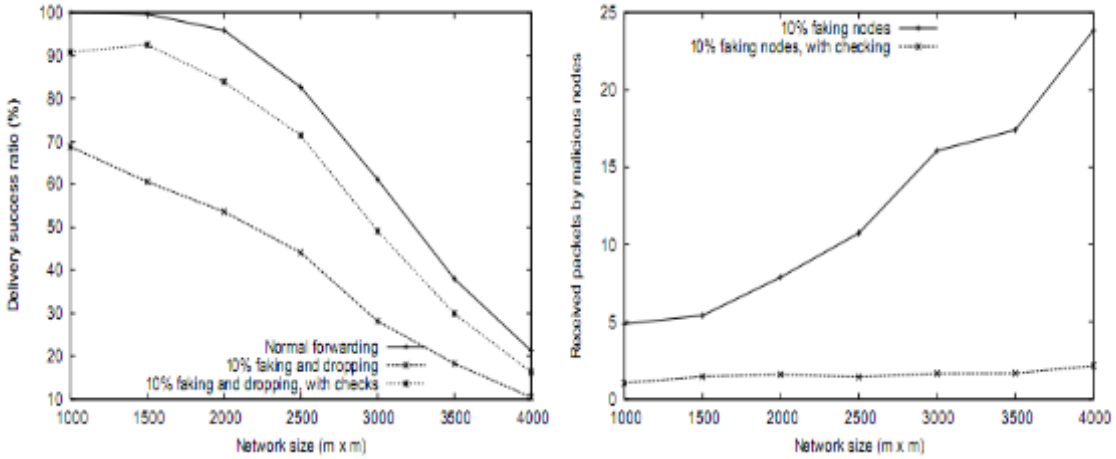


Figure 5.1: a) Result of false position and number of packets reached to destination
b) Number of packets received by problematic node

5.4 Transmission packets and rapid location change of Vehicles:

In the simulation we sent 100 different data packets (messages) from source node to destination node randomly in simulation time ranges from0---30 seconds.

Table: 5.1

Parameters List	Values
Transmission(Rmax)	250 meters
No of messages(packets) sent	100
Simulation per parameter set	15
Condition of City	
Number of nodes	100

Distance for nodes in square	1000---4000 meters
Number of Vehicles(density)	625 to 100
Maximum speed of Vehicles in meter per second	50
Break time in seconds	0.0
Change of location	Selected randomly
Time spent on each result in seconds	40
Highways / Motorways Conditions	
Number of Vehicles	Approximately 350
Each direction lines	2
Distance travelled on road in kilometers	12
Time spent on each result in seconds	120

5.5 Results Obtained:

To check that how effectively these constraints minimized the DoS (denial of Services) attacks in VANET (Vehicular ad hoc Wireless Network), can be indicated by the facts that how many packets reached to the problematic node or malicious node. The result obtained indicates that these constraints effectively minimized the DoS (Denial of Services attack) in the network.

6. Conclusion and future Work

6.1 Conclusion

In this work it has been tried to improve the level of trust on the neighboring nodes instead of using some specialized hardware or already installed network infrastructure. The main aim of introducing different constraints is to improve the reliability of the node which will receive the data packets or acts as packet forwarder. By these checks the trustworthiness of the location that a neighbored node claims can quickly be estimated and ultimately the possibilities for an attacker, using false location, are significantly decreased.

Also by introducing the injection rate limit constraint for different kinds of Vehicles, the possibility of fake and continuous message injection I the network has controlled and thus minimizing the possibility of jamming which is one of the major cause of DoS attack.

However more tight secure mechanisms are needed to deploy and implement the system in the real world. More constraints are required to improve the security level of the system and make it able for deployment in the real world scenario.

6.2 Future Work:

6.2.1 Possible Existing Problems:

Although the constraints proposed in this thesis minimized the DoS attacks to some extend but it has been analyzed that some drawbacks still exists in the system and thus need to be removed in the future work. These drawbacks are as under:

6.2.2 Faulty GPS(Global Positioning System):

As each Vehicles determine its current location and the location of those nodes with which the Vehicle communicates with the help of GPS(Global Positioning

System). If there is any sort of problem in GPS due to which it can not functions properly then Vehicle can not determine the accurate location of other Vehicles as well as its own. In that case the constraint proposed especially the Rmax and Vmax will be useless and a problematic Vehicle with false location can create different kinds of problems. Another limitation associated with GPS is that , it can not functions fully in the congested cities in the presence of high storey buildings, in jungles and in hilly areas.

6.2.3 Slow but gradual change in speed:

The maximum speed constraint i:e Vmaximum can easily be bypass by such a node which is malicious but it change its position slowly and gradually. Such a node would never cross the maximum speed limit in order to make Vmaximum constraint fool. In such a case the Vmaximum constraint will fail and will never detect such type of malicious activity. Thus additional constraint is required to detect such a node which slowly changes its location towards the destination and pretend a false location.

6.2.4 Limiting Signal Range:

In the solution phase of this work, we defined a maximum communication range 200-250 meters while it has been set by IEEE 802.11 for radio technology in wireless LAN as 300 meters. If we use the same mechanism in the congested areas, in the presence of high storey buildings where the signals will never penetrate and will never reach to its destination this limit will never reach to the limit defined in the IEEE 802.11. Thus it allow an attacker node which is 300 meters far to capture network traffic and creates problems for the sender node, if all other legitimate nodes available for forwarding are much closer to the sender. Just because of this reason the maximum range for radio signals has set as limited.

A better solution would be to provide a dynamic range where the node can set the range of the radio signals dynamically according to the surrounding circumstances.

7. Bibliography

1 B.Xio, B.Yu, C.Gao(Sept-2006),"Detection and localization of Sybil node in VANET", IEEE(Setp-2006).

2 C.Harsch, A.Festage, P.Papadimitratos (2007), "Secure Position based Routing protocol for VANET".

3 G. Calandriello , P. Papadimitratos , J.-P Hubaux and A. Lioy (2007)," Efficient and Robust Pseudonymous Authentication in VANET" ,IEEE-September- 2007.Aad, J-P.Hubaux (2005), "Security Aspects of Vehicular Communication"

4 M. Raya, P. Papadimitratos and J.-P Hubaux(April-2006) " Securing Vehicular Networks" IEEE April-2006..

5 M. Raya, P. Papadimitratos and J.-P Hubaux(October-2006) " Secure Vehicular Communication", IEEE October-2006

6 M. Raya, A. Aziz and J.-P Hubaux(Sept-2006) "Efficient Secure Aggregation In VANET", IEEE September- 2006.

7 M. Poturalski, (March-2006) "Verification of a VANET protocol", IEEE(March-2006)

8 M.A.Sharman, S-M.YOO(2004), "Black hole attack in Mobile ad hoc network", IEEE-2004.

9 S. Kurosawa, H. Nakyama, N.Kata(2006)," Detecting Black hole attack on AODV-Based in mobile ad hoc network by Dynamic learning", IEEE-2006

10 T. Leinmuller, C-Maihofer, E.schoch and F. Kargh (2006), "Improved security in geographic Ad hoc Routing through autonomous position varification"

11 CISCO. (1997)"Defining Strategies to Protect Against TCP SYN Denial of Service Attacks". September 17, 1996.
URL:http://cio.cisco.com/warp/public/707/4.html(4 Jan.2002)

12 CISCO,(1996)"Defining Strategies to Protect Against UDP Diagnostic Port DoS Attacks".
I. September 17, 1996. URL : http://cio.cisco.com/warp/public/707/3.html (4 Jan. 2002)

13 COOPER: Cooperative Network for intelligent Road Safety.

14 CIVIS: Cooperative Vehicle infrastructure System

15 www.ertico.com/en/activities/efficiency-environment/civis.htm

16 Dittrich, Dave(Feb-2000) "NANOG ISPSec Meeting/DDoS BoF",
I. IEEE 7 February, 2000.
II. URL:http://staff.washington.edu/dittrich/talks/nanog/ (4 Jan. 2002)

17 FleetNet: Internet on the Road.

18 www.et2.tu-harburg.de/fleetnet/english/vision.htm

19 Huegen, Craig A. (Feb-2000)"The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects". 8 February 2000.

20 URL:http://www.pentics.net/denial-of-service/white papers/smurf.cgi
I. (4 Jan. 2002)

21 Malaysian Computer Emergency Response Team. "MSA 029.072001:

I. MyCERT Special Alert - Code Red Worm". 20 July 2001. URL:
II. http://www.mycert.org.my/alerts/mycert_adv/MSA-029.072001.html (4 Jan. 2002)

22 Malaysian Computer Emergency Response Team. "MA-034.092001 :
I. NIMDA Worm". 19 September 2001. URL:
II. http://www.mycert.org.my/advisory/MA-034.092001.html (4 Jan. 2002)

23 Mandia, Kevin & Prosise, Chris. Incident Response : Investigating Computer Crime. Berkeley: Osborne/McGraw-Hill, 2001. 360-361.