International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 09 | Sep 2021 www.irjet.net p-ISSN: 2395-0072

Black Hole Attack Detection and Prevention Method in VANET by Using E-DSR Routing Method

Ms. Neha Rai[1], Mr. Rajneesh Pachouri[2], Mr. Anurag Jain[3]

[1]*M.Tech Research Scholar Department of Computer Science Engineering AIST, Sagar*
[2]*Assistant Professor, Department of Computer Science Engineering AIST, Sagar*
[3]*Assistant Professor, Department of Computer Science Engineering AIST, Sagar*

Abstract - *Next-generation communication networks are widely known as ad-hoc networks, widely classified as mobile nodes based on ad-hoc mobile networks (MANET) and automotive networks based on the ad-hoc network (VANET). VANET aims to maintain safety for motorists by initiating independent communication with nearby vehicles. The need for secure communication is a very important part of the network due to the presence of unwanted attackers. The SDSR indicates that the package is collapsing but only due to the presence of invaders. If the intrusion is found quickly enough, the attacker can be identified and removed from the network before a destructive act or data is compromised. In addition, the proposed SDSR acts as a defense, acting to prevent intrusion. The proposed system facilitates the collection of information about intrusion strategies that can be used to strengthen the entry point. These networks are heavily affected by various attacks such as Warm Hole attacks, denial of service attacks and Black Hole Attack attacks. This paper is a novel attempt to explore and investigate the security aspects of router agreements in VANET, the implementation of the AODV (Ad hoc On Demand) protocol to detect and deal with a particular category of network attacks, known as Black Hole Attacks. The effectiveness of the proposed security system is better because at the end of the receiver it identifies the falling packets setting the drop limit and also indicates the presence of attackers in the network which shows the attackers' effect and affects the network performance of the network. The proposed performance of the SDSR is measured by performance metrics and the result shows performance improvement.*

Key Words: DSR, AODV, Blackhole, BAODV, SAODV, SDSR

1. INTRODUCTION

Vehicular advert hoc networks (VANETs) are a subgroup of cell advert hoc networks (MANETs) with the distinguishing belongings that the nodes are automobiles like cars, trucks, buses and motorcycles. This means that node motion is limited through elements like street course, encompassing visitors and visitors' regulations. Because of the limited node motion it's miles a viable assumption that the VANET could be supported through a few constant infrastructure that assists with a few offerings and might offer get admission to to desk bound networks. The constant infrastructure could be deployed at crucial places like slip roads, carrier stations, risky intersections or locations famous for dangerous climate situations.

1.1 Uses of VANET

According to the DSRC, there are over 100endorsedprograms of VANETs. These programs are of categories, protection and non-protection associated. Moreover, they may be labeled into OBU-to-OBU or OBU-to-RSU programs. Here we listing number ofthoseprograms:

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

a. Co-operative Collision Warning:

Co-operative collision caution is an OBU-to-OBU protection software, that is, in case of any abrupt alternate in velocity or riding direction, the automobile is taken into consideration strange and pronounces a caution message to warn all the following automobiles of the probably danger. This software calls forangreen broadcasting set of rules with a totally small latency.

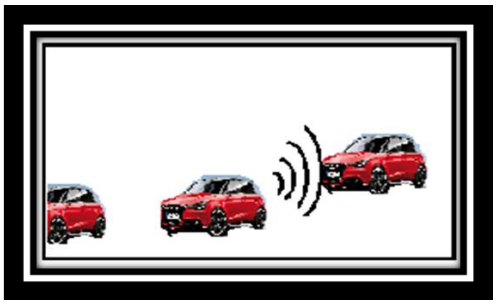


Figure 1 Cooperative Collision Warning

b. .Lane Change Warning: Lane-alternate caution is an OBU-to-OBU protection utility, this is, a car motive force can warn different automobiles of his purpose to alternate the visiting lane and to e book an empty room in the upcoming lane. Again, this utility relies upon on broadcasting

c. Intersection Collision Warning: Intersection collision caution is an OBU-to-RSU protection utility. At intersections, a centralized node warns coming near automobiles of viable injuries and assists them figuring out an appropriate coming near speed. This utility makes use of simplest broadcast messages.

1.2 Vehicle Componentizing Vanet

The additives of a VANET enabled Vehicle consists of laptop managed gadgets and radio transceivers for

message trade. The protocol that has been standardized for conversation in VANET is DSRC, which has a conversation variety of three hundred mts to at least one km. The roadside base station presents data to the motive force all through his adventure in order that he can discover a excellent direction to his destination. The data is periodically exchanged.

2. LITERATURE SURVEY

a. Feng Zhang et.al [1] presents a traffic information aggregation and propagation scheme, which is suitable for the city environment and based on Vehicle Ad hoc Network (VANET) to improve the traffic condition. Roadside units (RSUs) can collect, create and distribute traffic messages, using vehicle-to-vehicle communication and vehicles mutual cooperation. The traffic messages can help drivers to choose a better route and prepare against the traffic events. It's useful to avoid traffic jam and reduce the occurrence of traffic accidents. But in this paper author not show the effect of attack by that the congestion is occur because to identifies attacker is a difficult issue that one is the main cause of congestion.

b. HalabiHasbullah et.al [2] Vehicular Ad-hoc Network (VANET) is taking more attention in automotive industry due to the safety concern of human lives on roads. Security is one of the safety traits in VANET, network availability must be obtained at all times since availability of the network is vitally needed when a node sends any life critical information to other nodes. However, it can be predictable that security attacks are likely to be increase in the coming future due to more and more wireless applications being developed and deployed onto the well-known expose nature of the wireless medium. In this respect, the network availability is exposed to many types of attacks. In this paper, Distributed Denial of Service (DDOS) attack on network availability is presented and its cruelty level in VANET environment is complicated. A model to secure the VANET from the DDOS attacks has been developed and some possible solutions to overcome the attacks have been discussed.

c. Sarah Madi, Hend Al-Qamzi et.al [3] integrates mobile connectivity protocols to expedite data transfer between vehicles as well as between roadside equipment and available traffic in network. In VANET, Wireless device sends information to nearby vehicles, and messages can be transmit from one vehicle to another vehicle. Therefore, using VANET can increase safety and traffic optimization. Similar to other technology, in VANET there are some important and noticeable issues. One of the most important of them is Security. In this paper, I try to discuss security issues as one of the most important problems in Vehicular Ad hoc network.

d. Jakub Jakubiak and Yevgeni Koucheryavy,al [4] design a crosslayer control system where the objective is to not improve the efficiency of the MAC but to improve the vehicle tracking accuracy. The authors consider a lossy shared channel where increased message frequency can increase the channel congestion and effectively cause a loss in accuracy of other vehicles' positions. The proposed algorithm is a method to adapt the periodicity of transmission to attain the optimal accuracy.

e. R. G. Engoulou, M. Bellaïche, S. Pierre [6] The black hole attack is one of the security attacks that occur in MANETs which can occur in VANETs as well. A black hole is formed when nodes refuse to participate in the network or when an established node drops out. In this type of attacks, all network traffics are redirected to a specific node, which does not exist at all that cause those data to be lost [6]. There are two proposed possible solutions for this problem in MANETs. The protocol finds more than one route to the destination.

3. Proposed Methodology

A VANET is highly dynamic in nature it may subject to internal and external adversaries which raise important technical challenges in terms of reliability and secure routing. Compared to the way of constructing roads, attacker driving pattern is a less sustainable and more costly way to alleviate traffic in network and enhances the possibility of routing misbehavior.

The malicious behavior in network is caused by the presence of Blackhole attacker. Without security guarantee, some badly-behaved or malicious vehicles make vulnerable the system by providing low quality services or even put the user vehicles in dangerous situations. Therefore, how to identify those badly-behaved or malicious vehicles has become a fundamental requirement in securing VANET. Malicious user vehicles may behave well and badly alternatively.

The property of attacker to generate the fake information in network and drop all the traffic packets in network. The attacker vehicles are enhances the overhead in network because packets are heavily losses in network. The retransmission of packets are also enhances the delay in network but after all due Blackhole presence it is not possible to secure vehicles communication and not deliver traffic status properly. The proposed SDSR Allow secure delivery of data packets in multi-hop fashion by detecting and preventing malicious vehicles.

Proposed Attack Identification And Removal Scheme

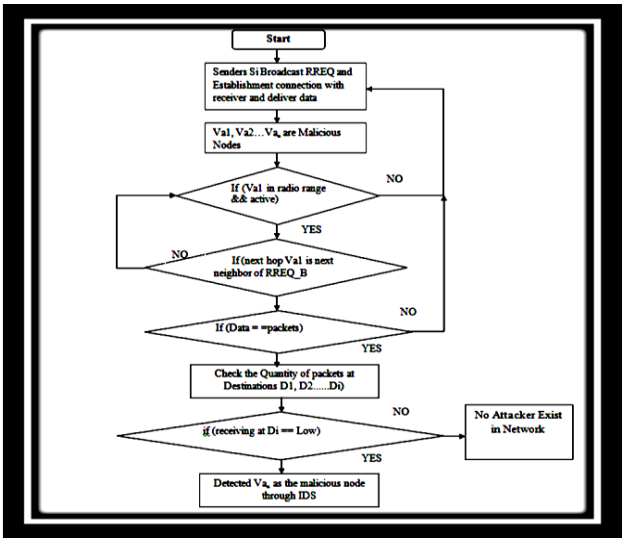
The proposed security scheme against Blackhole attack in VANET. Here the Blackhole attacker is create the 'gaps of information delivery' in between vehicles by that the vehicles speed are slowed and the infection is affected the performance of normal vehicles. The proposed scheme is applied with V to RSU communication for maintaining the security and forwarded the attacker vehicle information to all rest RSU and their surrounding vehicles. The proposed prevention scheme is block the attacker malicious activities and provides secure communication in VANET. The following steps to identify the malicious vehicles in network:-

1) The sender vehicles are sending the traffic status information packets to destination vehicles for giving traffic status information.

2) The numbers of sending vehicles are sending the traffic status to destination vehicles and the *attacker or malicious node presence is drop traffic information*. This is the behavior of attacker.
3) The whole research is divided in to three different scenarios.
    i) To evaluate performance of only AODV protocol
    ii) Evaluate Existing protocol performance of SAODV.
    iii) Evaluate performance in presence of Validate Data Delivery Security Scheme with DSR.
4) Count the data receiving at the destination end in each scenario.
5) The counting of traffic status packets in case of attacker is minimum or negligible at destination end.
6) The presence of attacker is confirmed but *which node is attacker.*
    i) Check the receiving and forwarding of each node.
    ii) If receiving is *true* and forwarding is *false* is found in routing table record then the attacker is found.
    iii) Count the number of packets received by attacker but not forwarded.
    iv) Otherwise node is normal.

FLOW CHART OF ATTACKER DETECTION

The flow chart of proposed Security scheme is represents the steps to identify the malicious behavior of attacker in VANET. The detection is required to identify which nodes are dropping the packets continuously in network.



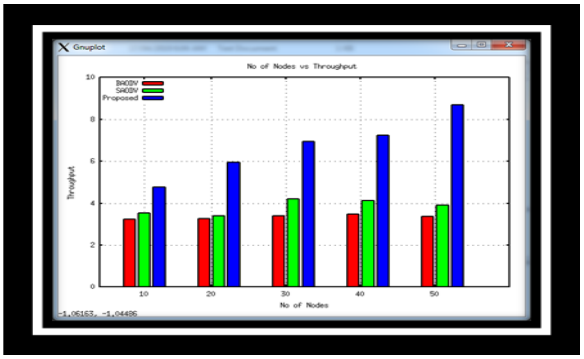
4. RESULT ANALYSIS

Simulation Parameters

The simulation must be carried out on the premise of Simulation parameters which might be proven in desk 1. The quantity of nodes is taken under consideration as cell detector nodes. All nodes has random mobility velocity to transport in community. The simulator model is hired for simulation is NS-2.31[16]. The very last parameters of Network parameters are indexed in Table 1.

Table 1 Simulation Parameters

NS-2.31	
Number of nodes	10, 20, 30, 40, 50
Attacker	Blackhole
Propagation	Two-Ray Ground
Antenna	Omi-directional
Dimension of simulated area	800×800
Routing Protocol	AODV
Performance Evaluated	BAODV, SAODV, SDSR
Simulation time (seconds)	100
Transmission Range (meters)	550
Transport Layer	TCP,UDP



Results Analysis

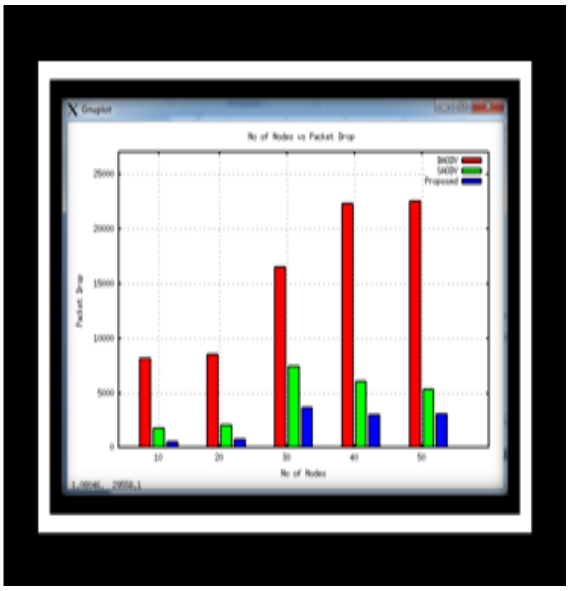
The overall performance of proposed protection scheme with DSR routing protocol is measured with preceding SAODV and Blackhole AODV(BAODV). The range of nodes eventualities is identical in all modules. The overall performance of proposed protection scheme is displaying the higher overall performance.

Throughput Performance Analysis

Throughput Performance Analysis In Vehicular networks, throughput or community throughput is the a hit message transport over a verbal exchange channel as much as vacation spot car.

Packet Drop Performance Analysis

The range of visitors repute packets are drop in community due to attacker misbehavior. The routing protocol lifestyles



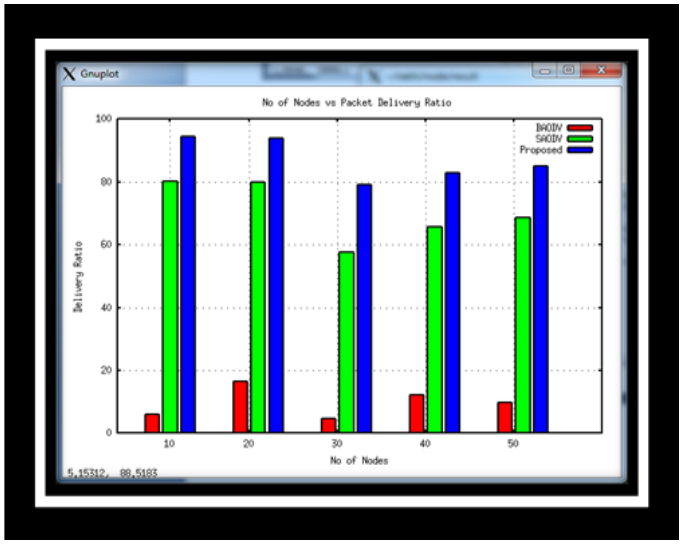
are likewise essential in VANET and the motors are constantly sends and obtain visitors information in community for higher riding facility on roads. In this graph simplest information drop in presence of BAODV, SAODV and SDSR is evaluated.

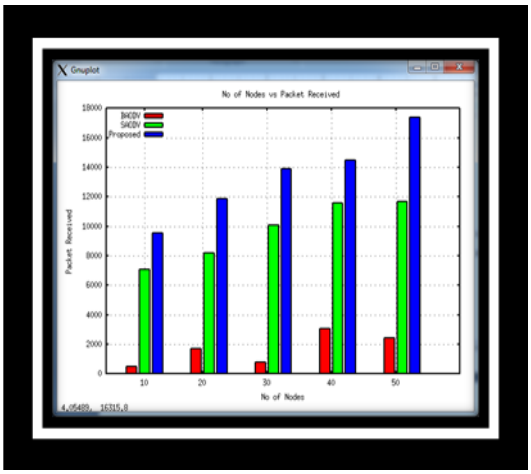
PDR Performance Analysis

The proper communication is necessary in network but it is very important in real time traffic system. The vehicles wrong information is misguides the trailing vehicles and because of that the road traffic is In VANET only short information (about traffic status and something un-happened on roads like accidents) are deliver to nearby vehicles. In this graph the PDR performance of BAODV, SAODV proposed SDSR communication is assessed and observe that the proposed scheme is really effective to identify the Black-hole assailant presence. The PDR performance as compare to SAODV is better and provides 97% successful delivery at destination. The attacker performance in network not more than 18% because most of the data are dropped in network e.g. is also the enhance NRL (Normal Routing Load) and end to end delay (NRL and end to end delay always minimum better). The attacker existence is absolutely blocked by proposed security for providing secure communication between vehicles.

Packet Receiving Performance Analysis

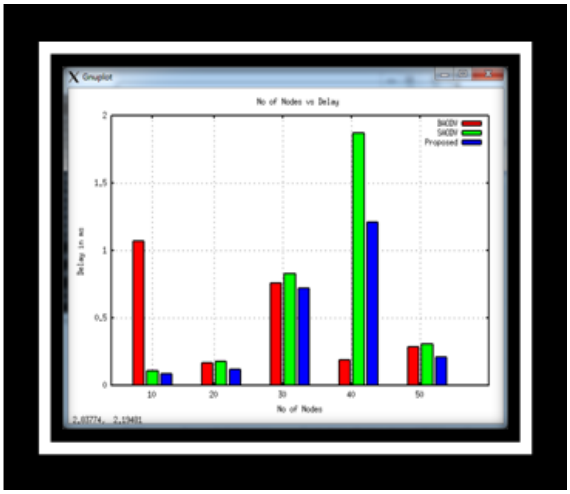
The verbal exchange is VANET whole the request of sender motors and keeps the visitors in roads. In this graph BAODV information receiving is negligible as evaluate to SADV and SDSR. meaning black hollow assault case information loss is most and if we observe proposed SDSR with information receiving is excessive, that indicates in all node density eventualities.





Delay Performance Analysis

The put off purpose in street visitors is motors in street is greater and the visitors repute records is nor introduced to motors properly. The follower motors are constantly sends the visitors request for acknowledges the visitors repute. The motors are power on that direction in line with the visitors records of starting motors. Traffic records is likewise damaging if it will likely be supply in community e.g. carry out misbehave because of presence of via way of means of Blackhole attacker (BAODV). In this graph the put off overall performance is measured and found that the put off overall performance of BAODV is usually excessive in all node density eventualities. The put off enhancement is greater in additionally SAODV however minimal in proposed SDSR scheme. The proposed protection scheme in opposition to Black-hole attacker is stable the community overall performance and offering the request packets transport as same to everyday VANET overall performance.



5. CONCLUSIONS

The malicious vehicle/s presence is definitely degrades the performance of In presence of black- hole attacker packets drooping is enhanced and receiving and sending is reduced too much as comparison to normal communication. In this research the proposed SDSR security scheme is detect and prevent the network from single as well as multiple black - hole attack in VANET. The proposed approach is decided that the packet dropping is counting more than certain threshold then the attacker may be present in network.The number of vehicles is cross the road and terminals like RSU units. The RSU unit is observe the traffic status information sending by the vehicles in limited range to identified the further traffic status from leading vehicles. The RSU monitoring is detecting the attacker presence and after that prevents it. In this paper a range of facet of VANET like its environment, standards and network architecture has been converse. In VANET for receiving and generating traffic request routing is perform an important part which used for more prominent and expedient communication. The security in VANET is improves the throughput and PDR. The improvement in packets receiving is also enhance the performance by reducing delay and overhead .While attack creates a more harsh condition, it is necessary to investigate the effect of attack on routing protocols which makes more protected vehicular environment. The proposed SDSR is reduces the packets dropping and due to attacker presence the dropping is completely cover-up and removes attacker infection from network.

The attacker presence in VANET is very effective to find out it by applying the location identification system or Global Positioning System (GPS) to identify the malicious vehicle actual or current location. The location based scheme is also improves the more performance in term of delay and overhead.

REFERENCES

1. Feng Zhang; Jianjun Hao; Shan Li "Traffic information aggregation and propagation scheme for vanet in city environment". 2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT) 26-28 Oct. 2010.
2. Sumra, Irshad Ahmed, Iftikhar Ahmad, HalabiHasbullah, and J-L. bin Ab Manan. "Classes of Attacks in VANET." IEEE Saudi International Electronics, Communications and Photonics Conference (SIECPC), 2011, pp. 1-5, 2011.
3. Sarah Madi, Hend Al-Qamzi, "A Survey on Realistic Mobility Models for Vehicular Ad Hoc Networks (VANETs)", IEEE 10th IEEE International Conference On Networking, Sensing And Control (ICNSC), 2013.
4. Jakub Jakubiak and Yevgeni Koucheryavy, "State of the Art and Research Challengies for VANETs", Proceedings of the 5th annual IEEE CCNC, pp.912-916, 2008.\
5. Mengjiong Qian, Yong Li, DepengJin, Lieguang Zeng", Characterizing the Connectivity of Large Scale Vehicular Ad-Hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC): Networks, 2013.
6. R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET Security Surveys," Computer Communication, Vol. 44, pp. 1–13, May 2014.
7. Anas Abu Taleb, "VANET Routing Protocols and Architectures: An Overview", Journal of Computer Science, 2018.
8. Duduku, V., V.A. Chekima, F. Wong and J.A. Dargham, "A Survey on Routing Protocols in Vehicular Ad Hoc Networks", International Journal Innovative Research of Computer Communication Engineering, pp.12071-12079, 2015.
9. Jair Jose Ferronato, Marco Antonio, SandiniTrentin, "Analysis of Routing Protocols OLSR, AODV and ZRP in Real Urban Vehicular Scenario with Density Variation", IEEE Latin America Transactions Volume: 15 , Issue: 9, pp.1727 - 1734, 2017.
10. A.P. Jadhao, Dr.D.N.Chaudhari, "Security Aware Routing Scheme In Vehicular Adhoc Network", IEEE Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), 2018.
11. Kumud Dixit Priya Pathak Sandeep Gupta, "A New Technique for Trust Computation and Routing in VANET", IEEE, 2016.
12. TrupilLimbasiya, Debasis Das, "Secure Message Transmission Algorithm for Vehicle to Vehicle (V2V) Communication", IEEE, 2016.
13. KhaoulaJeffane, and Khalil Ibrahimi, "Detection and Identification of Attacks in Vehicular Ad-Hoc Network", IEEE, 2016.

14. Mengjiong Qian, Yong Li, DepengJin, Lieguang Zeng, "Characterizing the Connectivity of Large Scale Vehicular Ad-Hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, 2013.
15. Sourav Kumar Bhoi, Eabitra Mohan Khilar, "A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services", International conference on Communication and Signal Processing, April 3-5, 2013.
16. Samir A. Elsagheer Mohamed A. Nasr Gufran Ahmad Ansari "PRECISE POSITIONING SYSTEMS FOR VEHICULAR AD-HOC NETWORKS" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 2, April 2012
17. Lingyun Zhu; Chen Chen; Xin Wang; Azman Osman Lim "SMSS: Symmetric-Masquerade Security Scheme for VANETs" 2011 Tenth International Symposium on Autonomous Decentralized Systems. 23-27 March 2011. **ISBN:**978-1-61284-213-4
18. D.Manivannana Shafika, Showkat Monia, Sherali Zeadallyb "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)" Vehicular Communications Volume 25, October 2020, 100247.
19. Mostofa Kamal Nasir,1 Rafidah Md Noor, M. A. Kalam, and B. M. Masum Reduction of Fuel Consumption and Exhaust Pollutant Using Intelligent Transport Systems Received 18 February 2014; Accepted 3 April 2014; Published 17 June 2014.
20. Alefiya Hussain, John Heidemann Christos Papadopoulos "A Framework for Classifying Denial of Service Attacks" July 2003ACM SIGCOMM Computer Communication Review 33(4) Date: 25 Feb 2003, Updated: 25 June 2003.