http://dx.doi.org/10.21172/ijiet.151.03

A Conjectural based Framework to Detect & defend/Classify Selfish Nodes and Malicious Nodes in Manets Using AODV

Geetha V[1], Dr.Hariprasad S A[2]
[1]*Geetha V, Assistant Professor,Information Science & Engg, RVCE(Affiliated to VTU),Bengaluru India*
[2]*Dr.Hariprasad S A, Director, Jain University, Bengaluru,India*

Abstract: A Mobile Ad-hoc Network (MANET) is such an autonomous system operating in decentralized and distributed manner where mobile nodes connect spontaneously without a fixed infrastructure. The nodes in the routing process tend to misbehave by either being selfish or malicious.In present day world the researchers are addressing this misbehaviour of nodes using Dynamic source routing protocol and it is observed by the survey that the success ratio of attaining QoS parameters are not satisfactory. Further the success ratio for attaining better QoS parameters can be improvised by using other efficient Manet Frameworks.

In this paper, we address this issue with a Conjectural Frameworkwhich integrates detection of selfish and malicious nodes based on direct and indirect approach. Ad-hoc On-demand Distance Vector (AODV) routing protocolis extended and adopts an extensive deep packet scrutiny (EDPS) technique to detect suspicious activities from the mobile nodes before they start dropping data packets.

The basic and common limitation when compared with the existing frameworks are that there are no framework existing which incorporates the direct and indirect reputation based approach to detect and defend both the Malicious and Selfish nodes using AODV protocol. And there is no such framework which incorporates the punishment strategy and second chance mechanism for the badly reputed nodes. The Success ratio of the same is shown in the results.

Experimental results prove that the proposed reputation model enhance the quality of service metrics.The performance of proposed scheme is evaluated against AODV, SHRCM and PCMA, CORE, CONFIDANT with NS-2 simulator.The results show that proposed scheme achieves remarkable improvement in network life time, network throughput,average packet delay,packet delivery ratio,overhead and reliability with routing overhead and average end-to-end delay as compared to existing schemes.

Keywords: Mobile Ad-hoc Network, Ad-hoc On-demand Distance Vector, extensive deep packet scrutiny, , Vickrey, Clarke, and Groves model.

I. INTRODUCTION

Our reputation based framework is proposed for distributed system where each and every nodes maintains a reputation table which holds reputation information of all the neighboring nodes with whom it is communicating or nodes who are of interest. As the scenario which we are considering for experimental purpose is a network with high mobility, it is preferred at every node to maintain reputation for as many nodes as possible. The selection of distributed type reputation model ensures that the requirement is fulfilled.

The basic and common limitation is that there is no framework existing which incorporates the direct and indirect reputation based approach to detect and defend both the Malicious and Selfish nodes using AODV protocol. And there is no such framework which incorporates the punishment strategy and second chance mechanism for the badly reputed nodes.

The prime purpose of the proposed research work is to evolve up with an efficient technique that assists in developing the framework for reputation based approach in handling security issues in MANETs.

II. RELATED WORKS

Michardi and Molva [1] have proposed a collaborative reputation framework, which utilizes watch-dog as the detection component. Authors have utilized three reputation approaches viz., subjective reputation, indirect reputation and functional reputation for detecting selfish nodes. Authors also formulated a mechanism for detecting misbehaving nodes based on threshold level of packets dropped by a mobile node. CORE is developed on DSR routing protocol and uses indirect reputation approach. Does not detect selfish node behavior.

Further, Buchegger and Boudec [2], have proposed a novel reputation approach based on four entities namely trust manager, path manager, monitor and the reputation system which estimates the reputation level of each and every mobile node present in the ad hoc network through the first and second hand information. This approach is a distributed approach which maintains alarm table, trust table and friend list for detecting selfish nodes through the coordination of trust manager and path manager. This mechanism also isolates the selfish nodes at the faster rate

based on the component called monitor that continuously monitors the deviation of an individual node from its normal behavior and uses DSR protocol for routing and direct reputation based aproach. Does not detect malicious nodes.

In addition, Farad and Askwith [3] proposed a Packet Conservation Monitoring Algorithm (PCMA) that aids indetecting the malicious nodes in the ad hoc scenario. This monitoring algorithm mainly targets on the detection of specific type of malicious nodes from the routing path and thus enables reliable dissemination of data by increasing the overall performance of the network in terms of packet delivery ratio, throughput, total overhead and control overhead. Does not use reputation based approach and detects only selfish nodes and does not detect malicious nodes but uses AODV as a routing protocol.

Yet another, novel method for mitigating selfish through second hand reputation mechanism based on split half reliability coefficient was proposed by Sengathir and Manoharan[4].This mechanism estimates the nodes' behaviour with regard to two perspectives viz, packet delivery rate of a mobile node and packet forwarding ability of a mobile node. The split half reliability coefficient is derived based on Karl Pearson correlation coefficient and spearman brown formula that interprets the change in the level of nodes' behaviour from its normal routing activity Does not use reputation based approach and detects only selfish nodes and does not detect malicious nodes but uses AODV as a routing protocol

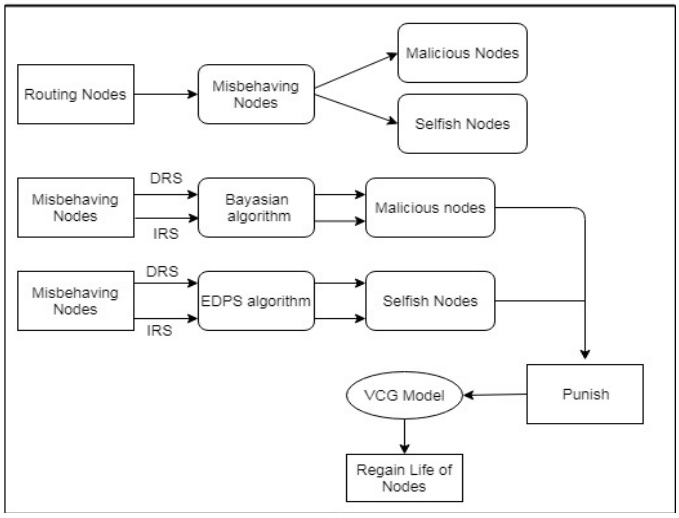
From the survey it was found that performances of routing protocol depend on the scenario in which the location of the nodes, speed of the nodes, number of connections of nodes and traffic in between nodes are varied, are compared interms of throughput, packet delivery ratio and end-to-end delay. AODV and DSR protocols outperformed each other in different scenarios. Most often DSR protocol was preferred in small network and less mobility while AODV performed better when node density and mobility is high. From the survey it is also observed that all the existing algorithms makes use of DSR protocol but not AODV protocol. Since AODV is also more vulnerable to the blackhole attack a need for the framework comprising AODV for reputation based approach in handling security issues in MANETs can be noted.

Further a Extensive deep packet scrutiny algorithm is considered and incorporated in the proposed framework to detect and defend both selfish nodes and malicious nodes using direct and indirect reputation based approach. And the proposed framework proves its novelty by punishing the misbehaving nodes and inculcates second chance mechanism for regaining the life for badly reputed nodes. So the proposed framework incorporates all the limitations of the existing work and efficiency of the framework is analysed using simulation and results proves that the proposed framework is better in attaining the Qos Parameters such as Packet delivery ratio, Throughput, Network overhead, reliability etc..

III. DESIGN OF THE REPUTATION BASED FRAMEWORK

Extended from the Ad-hoc On-demand Distance Vector (AODV) routing protocol, we propose a reputation-based scheme which adopts an extensive deep packet scrutiny (EDPS) technique to detect suspicious activities from the mobile nodes before they start dropping data packets. Further, For the purpose of selfish and malicious nodes classification, we construct supervised learning technique relied on Deep Neural Networks (DNN). Finally, to repair selfish nodes to cooperate and encode the packets, the Vickrey, Clarke, and Groves (VCG) model is used.

The performance of proposed scheme is evaluated against AODV, SHRCM and PCMA with NS-2 simulator..



3.1 Vickrey, Clarke, and Groves (VCG) model

Here, we define VGC modelusing standard mechanism design notation. We treat our problem as a game where mobile nodes are the players. Each node holds a private information θ_i about its preferences (θ_i is known as the type of player i). The type θ_i is drawn from each player's available type set $\Theta_i = \{Malicious, Selfish\}$, it describes how each player values all possible outcomes. Moreover, we define S_i as the available set of strategies for player i . In our model, we are using direct revelation mechanism in which $\Theta_i = S_i$.

$$u_i(\theta_i, o(\theta_i, \theta_{-j}) = p_i - v_i(\theta_i, o(\theta_i, \theta_{-i})) \quad (5)$$

Where,

θ_{-i} is the type of all nodes in a network region.

v_i is the valuation of player i to the output $o \in O$, knowing that O is the set of possible outcomes. In our case, v_i is the cost of analysis C_i that will be revealed by i after selecting its type θ_i .

$p_i \in \Re$ is the payment given by the mechanism to a selected node. Payment is given in the form of reputation.

To achieve the desired goal, credits are computed using VCG mechanism where truth-telling is proved to be dominant.

$$p_i = R_i = \sum_{j \in -n_i} v_j(\theta_j, o(\theta_i, \theta_{-i})) \quad (6)$$

Where R_i is the reputation and denotes, according to the standard notation in mechanism design, the best payment excluding n_i .

The punishment scheme uses credit as an incentive to stimulate selfish nodes to cooperate. Selfish nodes are motivated to relay routing packets because it is beneficial for nodes for two reasons: (1) they can improve their reputation, so they can relay their packets with low payment (2) nodes dropping routing packets are never involved in forwarding routes, and therefore, they cannot earn any credits. Some selfish nodes may selectively forward data packets in order to earn credits while preserving their resource. However, dropping packets cause degradation in the node reputation value, so these nodes need to pay a high payment for each packet sent which depletes their credits rapidly. For nodes situated in peripheral positions, we have to using periodical credit increase method. Thus, although peripheral nodes cannot improve their credits, they have the opportunity to relay routing packets, so they can improve their reputation and they can relay their packets with less payment.

For the purpose of second hand reuse of punished selfish nodes we make T_{RI} (Time for reintegration) proportional to the number of times in which node S_{i+1} is punished as selfish. For example, if it is the first punishment of the node S_{i+1}, node S_{i+1} is reintegrated within the network after T_{RI} . If it is its k times isolation, node S_{i+1} is reintegrated within the network after $k * T_{RI}$. A node is regarded as selfish if its credit account is equal to zero. It can become a cooperative node by improving its credit account by relaying packets for other nodes. Cooperative nodes refuse to relay all packets initiated by selfish nodes for their punishment.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

Here we implemented a model based verification of our reasoned outcomes in both homogeneous and heterogeneous environment. The simulation is performed on sensing of data models. The simulation and analytical results are associated through variable node density, transmission range, sensing range and availability of node. In the model, nodes are organized regarding with an identical transmission in an adjusted system domain. The packet transfers into the system domain commencing on an arbitrarily selecting a point on the system margin. NS-2 simulation is executed, and every data transmission for both homogeneous and heterogeneous environment of active guard and sleeping state is given in following figures. The numerical outcomes are estimated using some QoS parameters. For consecutive simulation runs, the nodes are identically reorganized in the system area. For existing algorithm we have to compare our proposed REDPS with SHRCM (Split Half Reliability Coefficient based Mathematical Model), PCMA (Packet Conservation Monitoring Algorithm) and AODV.

Table 3: Simulation parameters and its value

Parameter	Value
Total number of nodes	100
Distance among adjacent nodes	100 m
Deployment area	50m×2500m
Total number of relay nodes	98
Source node	1
Sink node	1
Packet size Initial energy	1024 bits 1J
Packet sending rate	1 packet/sec

We consider the simulation experiments using NS-2 with 100 nodes consistently dispersed. Every single node has the same frequency B = 1 Mbit/s, and firmware character energy consumption χ_{elec} and energy dissipation during transmission λ_{amp} is set as 10 × 10−9 J/bit and 130 × 10−12 J/bit/m2, correspondingly. Additional simulation parameters are given in Table 1.

The parameters like network life time, throughput, average packet delay, packet delivery ratio, overhead and reliability are improved as previously noted. The parameter analysis of proposed scheme compared with existing schemes can be seen in Table 4.

Table 4 Parameter analysis versus number of nodes

Methods	No of Nodes	Network Life Time (Rounds)	Throughput (Mbps)	Average Packet Delay (Ms)	Packet Delivery Ratio (%)	Overhead (%)	Reliability (%)
AODV	20	14	65	160	69	16	13.1
	40	31	62	164	64	18	39.3
	60	45	57	184	59	19.25	81.7
	80	59	53	190	53	20.4	85.6
	100	71	49	212	50	21.25	87
PCMA	20	19	80	148	81	13.2	15.3
	40	34	75	154	74	15.25	42.4
	60	49	68	158	69	16.4	82.3
	80	63	64	165	61	17.6	86.2
	100	75	57	167	58	19.65	87.7
SHRCM	20	25	82	142	81	12	16.5
	40	43	79	144	76	13.6	45.6
	60	54	75	145	71	15.2	83.4
	80	69	69	155	67	16.2	87.5
	100	84	57	170	64	16.8	89.4
REDPS	20	34	87	136	88	10.85	17.4
	40	52	80	138	83	12	44.9
	60	74	76	140	81	12.8	84.6
	80	86	72	147	78.5	15.2	89
	100	94	69	154	74	16.65	91.7

T-Test

A t-test is used to compare the mean scores obtained by two groups on a single variable. The critical ratio test or t-test is used for two sample difference of means. Here it was applied to determine the differences between means of two scores obtained from the one group based on the two variables. It is very useful when the population variance is not known and when the sample size is small.

The T-test value is calculated for our proposed system REDPS and other existing systems like SHRCM, PCMA, and AODV.

4.1 Network life time:

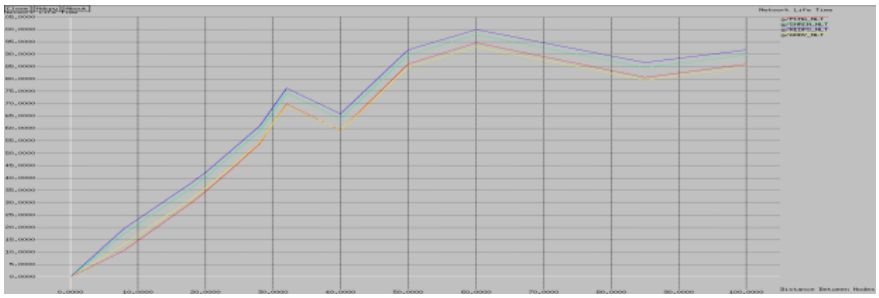


Fig 3:Network lifetime analysis

Network lifetime for the number of nodes is measured to give the proposed work's efficiency. From figure 3, we can show, while increasing the simulation time, network lifetime is decreased. Since, compared to the previous methods, proposed work efficiency is high. In case of life time of mobile nodes are not changed due to the energy consumption network life time is slightly decreased but it is better when comparing to the existing work.
The T-test value of network lifetime analysis for the proposed REDPS is compared with the existing techniques such as SHRCM,PCMA, and AODV. Specifically, in case of network lifetime analysis our proposed method is 3.86% higher than the SHRCM, 5.04% more than the PCMA, and 25.15% better than the AODV technique.

4.2 Throughput:

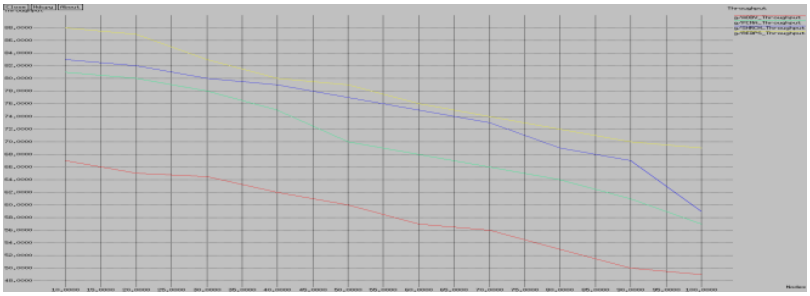


Fig 4: Throughput analysis

Throughput should be high for the efficient transmission and it is high associating with the existing methods. While taking the proposed work, throughput is high for the minimum number of nodes and while reaching at maximum node density, it is decreasing and after some period throughput is again improved. Throughput for the current work is nearly 90%.
The T-test value of throughput for the proposed REDPS is compared with the existing techniques such as SHRCM,PCMA, and AODV. Specifically, in case of throughput value our proposed method is 22.22% higher than the SHCM, 12.12% more than the PCMA, and 41.37% greater than the AODV technique.

4.3 Average packet delay:

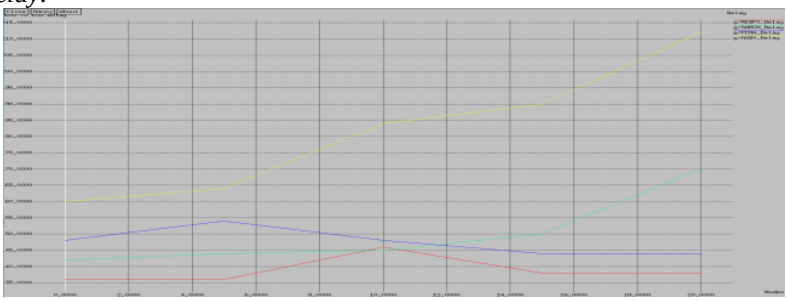


Fig 5: Average delay analysis

Packet delay is calculated since the portion of entire delays inside the whole transmission once associated to the measure of data well offer to the recipient target nodes all over the complete recursive run. In figure 4, delay for the

proposed work is very low (i.e. nearly 0.04%). For the number of nodes, delay will be increased but it is lesser than 0.1%.
The T-test value of average packet delay for the proposed REDPS is compared with the existing techniques such as SHRCM,PCMA, and AODV. The average packet delay of our proposed method is 26.64% higher than the SHCM, 29.96% more than the PCMA, and 31.09% greater than the AODV technique.

4.4 Packet delivery ratio (PDR):

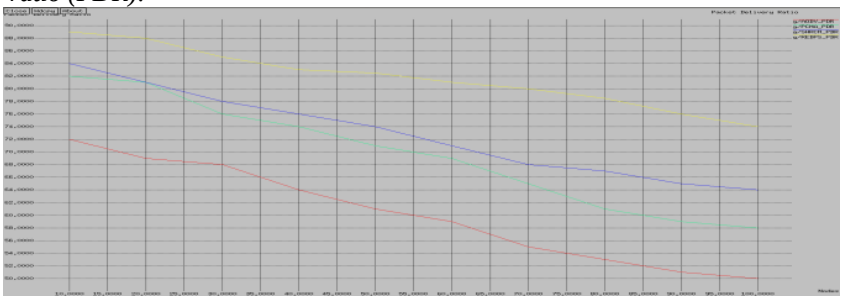


Fig 6: Packet delivery ratio analysis

For an efficient transmission, packet delivery ratio should be high. If the packet delivery ratio is maximum means we can get all information at the receiver without any loss. Here the delivery ratio is high which is high at minimum number of nodes.
The Packet Delivery Ratio of our proposed method is compared with the existing system such as SHRCM, PCMA, and AODV. The PDR value of proposed technique is 16.21% higher than the SHRCM technique, 1.32% higher than the PCMA technique, and 24.85% more than that of AODV technique.

4.5 Overhead analysis:

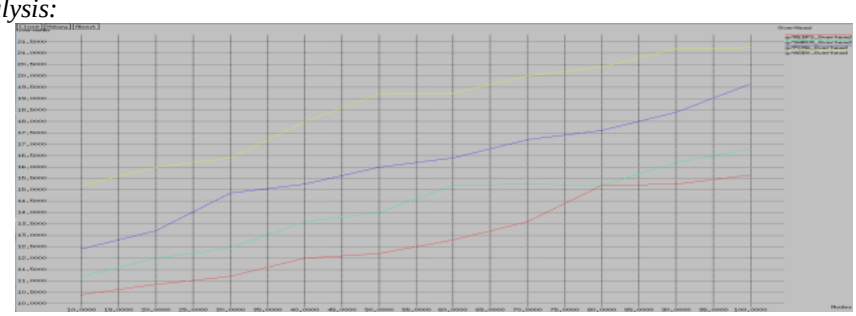


Fig 7: Overhead analysis

The overhead value of our proposed system REDPS is compared with other existing systems like SHRCM, PCMA, and AODV. The overhead analysis of REDPS technique is 11.36% more than the SHCM, 8.98% higher than the PCMA, and also 8.98% more than the AODV technique.

4.6 Reliability analysis:

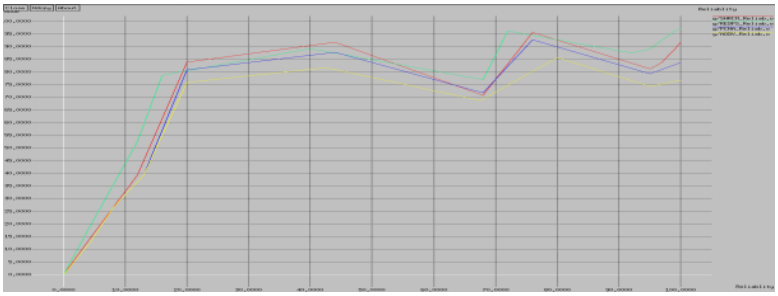


Fig 8: Reliability analysis

The reliability analysis of our proposed system REDPS is compared with other existing systems like SHRCM, PCMA, and AODV. The overhead analysis of REDPS technique is 45.77% more than the SHCM, 5.83% higher than the PCMA, and also 31.92% more than the AODV technique.
Based on the above parametric matrices like network life time, throughput, average packet delay, packet delivery ratio, overhead and reliability are improved compared to other existing schemes. It denotes our proposed reputation based scheme provides better quality of service (QoS) and security against vulnerabilities.

V. CONCLUSION

Mobile ad hoc networks have attracted much interest in the research community due to their potential applications. However, the inherent characteristics of such networks make them vulnerable to a wide variety of attacks.Unlike other existing reputation-based schemes, we address this issue by introducing a novel reputation-based model which integrates attack pattern discovery and classification mechanism. Although, the proposed reputation model has been incorporated with AODV protocol, any reactive protocol can be modified for this purpose.The classification of selfish and malicious node is done by DNN and detected selfish nodes are islocated and punished by VCG meachnism.The performance of proposed scheme is evaluated against AODV, SHRCM and PCMA with NS-2 simulator.The results show that proposed scheme achieves remarkable improvement in network life time, network throughput,average packet delay,packet delivery ratio,overhead and reliability with routing overhead and average end-to-end delay as compared to existing schemes.

VI. REFERENCES

[1] Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proc., 6th IFIP Conf. on Security, Communications and Multimedia, Protoroz, Solvenia, vol. 228, no. 1; 2002. p. 107–21.
[2] Buchegger S, Boudec J-Y. Performance Analysis of the CONFIDANT protocol: Cooperation of Nodes – Fairness in Distributed Ad-hoc Networks. In: Proc., 3rd ACM International Symposium on Mobile ad hoc Networking and Computing (MobiHoc ’02), New York, USA, Vol. 1, No. 1; 2002 p. 226–36.
[3] Fahad Tarag, Askwith Robert. A node misbehaviour detection mechanism for mobile ad hoc networks. In: Proc., Seventh Annual Post Graduate Symposium on the convergence of Telecommunications, Networking and Broadcasting (PGNet), vol. 1, no. 1; 2006. p. 78–84.
[4] Sengathir J, Manoharan R. A split half reliability coefficient based mathematical model for mitigating selfish in MANETs. In: Proc., 3rd IEEE International Advance Computing Conference, Ghaziabad, India, vol. 1, no. 1; 2013. p. 267–72.
[5] Taneja, Sunil, and Ashwani Kush, "A survey of routing protocols in mobile ad hoc networks", International Journal of innovation, Management and technology, Vol. 1, No. 3, pp. 279, 2010.
[6] Ade, S. A., and P. A. Tijare, "Performance comparison of AODV, DSDV, OLSR and DSR routing protocols in mobile ad hoc networks", International journal of information technology and knowledge management, Vol. 2, No. 2, pp. 545-548, 2010.
[7] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi, "Manet: vulnerabilities, challenges, attacks, application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, No. 2011, pp. 32-37, 2011.
[8] Mamatha, G. S., and Dr SC Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS-A Survey", International Journal of Computer Applications, Vol. 9, No. 9, pp. 12-17, 2010.
[9] Gerla, Mario, and Leonard Kleinrock, "Vehicular networks and the future of the mobile internet", Computer Networks, Vol. 55, No. 2, pp. 457-469, 2011.
[10] Khokhar, Rashid Hafeez, Md Asri Ngadi, and Satria Mandala, "A review of current routing attacks in mobile ad hoc networks", International Journal of Computer Science and Security, Vol. 2, No. 3, pp. 18-29, 2008.