IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 7, July 2016

ESDIT: An Approach for Improving Performance in MANET by Detecting and Isolating Selfish Nodes

G. Sri Kanya[1], P. Ramya[2]

M.Tech Student, E.C.E, Gudlavalleru Engineering College, Gudlavalleru, India [1]

Assistant Professor, E.C.E, Gudlavalleru Engineering College, Gudlavalleru, India [2]

Abstract: Mobile Ad hoc Network (MANET) is a dynamic self-organized network which comprises of wireless mobile nodes. Ad hoc networks can be merged or can be partitioned into separate networks, without relying on a fixed infrastructure to manage the operation. The performance of MANET diminishes significantly because of misbehaviour of nodes due to selfish reasons. A selfish node refuses to share its resources with neighbouring nodes and uses for its own purpose. So this may lead to packet loss in MANET. To improve the performance of MANET it is important to detect and isolate the selfish nodes. In this paper, ESDIT (Efficient Selfish node Detection and Isolation Technique) is proposed to efficiently detect and isolate selfish nodes in MANET. The proposed technique has been carried out to analyze the selfish nodes detection on essential function such as network routing. The simulation study demonstrates that the proposed ESDIT enhances the packet delivery ratio and throughput.

Keywords: MANET, ad hoc networks, self-organized, selfish node, ESDIT.

I. INTRODUCTION

Mobile ad hoc network (MANET) is a dynamic network system which comprises of a number of movable nodes that communicate by using wireless medium. The phenomenon of network dissection is a crucial problem in MANET that arises because of the unlimited movement of mobile nodes in the network. In MANET [1] data accessibility is to be examined attentively. In MANET to transmit the data packets each mobile node in the network requires the cooperation of other mobile nodes. In between consecutive transmissions the nodes are assumed to wait for a predefined interval of time.

The deflection of a mobile node from the actual routing and forwarding mechanism is mentioned as the node misbehaviour. In MANET to transmit the data packets successfully to the destination node it is mandatory for a source node to broadcast data packets to the intermediate nodes. Some nodes in the network may refuse to forward the data packets that are not related to it, to save their minimal resources leading to selfish behaviour. A selfish node may purposely delay and drop the packets to utilize its minimal resources only for its own purpose. The selfish behaviour of the nodes in the network may impact the performance of the network. The intent of the selfish node is to save its resources such as processing time, memory and battery life for future use. Fig. 1 shows a sample MANET.

The selfish node features are as follows:

- Do not participate in routing
- Do not reply or transmit HELLO messages
- Postpone route request and reply packets
- Drop data packets

Fig 1 Mobile Ad Hoc Network

The rest of the paper is organized as follows: Section II gives the overview of the related work. Section III describes the proposed method for detecting and isolating selfish nodes in MANET. The performance analysis is discussed in section IV. Finally, the conclusions are summarized in section V.

DOI 10.17148/IJARCCE.2016.57137

II. RELATED WORK

The existing solutions for detecting and handling the node misbehaviour in MANET are discussed in this section. Hernandez et al. [2] implemented a fast analytical model using a collaborative watchdog approach to evaluate the detection of selfish node in MANET. For detecting one selfish node they evaluated the overhead and the detection time of collaborative watchdog approach. Jawhar et al. [3] proposed a more reliable routing protocol to improve the reliability and security of communication in MANET and sensor networks. The improved reliability and security were achieved in the network by maintenance of the reliability factor by the nodes. Rodriguez and Gozalvez [4] suggested different reputation based protocols to deal with selfishness prevention in MANETs. These protocols were used to observe correct relaying of data packets and to compile the information about potential selfish nodes in the network. Hernandez et al. [5] recommended a collaborative watchdog mechanism to improve detection of selfish nodes in MANET. They implemented an analytical model to evaluate the cost of the collaborative approach and the detection time of selfish node.

Padiya et al. [6] proposed innovative techniques namely acknowledgement based technique, reputation-based technique and credit-based technique in order to detect selfish nodes in MANET. Roy and Chaki [7] proposed mobile agents based new IDS (Intrusion Detection System). The main objective of this approach was to focus on the limitations of IDS system by taking the benefits of mobile agent system. Koshti and Kamoji [8] discussed two techniques, namely credit-based technique and reputation-based technique. The 2ack scheme was used to detect and attenuate the effect of nodes misbehaviour in MANET. Yoo et al. [9] suggested a credit payment scheme to attain fairness in packet forwarding. In this scheme nodes require credits to transmit their packets which can be earned by transmitting the packets of other nodes. Ramya et al. [10] proposed an improved energy efficient and certificate revocation technique for MANETs. Zhong et al. proposed Sprite [11], a simple, cheat proof, credit based system for MANETs. Sprite uses credit to provide incentives for mobile nodes to cooperate and report actions honestly. A CCS(Credit Clearance Service) is introduced to determine the charge and credit to each node involved in the transmission of a message. Qunwei Zheng et al. [12] proposed a secure data transmission scheme that takes advantage of node mobility, the scheme is based on the observation that due to mobility, messages sent at different times are routed through different intermediate nodes.

III.PROPOSED METHOD

The main aim of this approach is to detect and isolate selfish nodes in MANET using ESDIT technique. The proposed method contains a robust mechanism for the detection of node misbehaviour. The information about the detected selfish nodes can be used by the neighbouring nodes and they may use the information to keep selfish nodes away either from data aggregation, data forwarding, or any other cooperative function. The flow chart of ESDIT technique is shown in Fig. 2. The initial step is to create a network consisting of number of mobile nodes with indicated position. Route is discovered between the source and destination node. The success and failure rates of neighbouring nodes are collected to calculate the assurance value. Selfish nodes are detected based on the assurance value. The detected selfish nodes are isolated keeping them away from network operations. The data packets are transferred to non-selfish nodes. Finally the performance of the network is evaluated.

A. Route Discovery

In route discovery the initial step is to create number of mobile nodes with designated position. To discover the route between nodes, the source node initially transmits a RREQ (Route REQuest) message; this message may be received by all the nodes that are within the transmission range of the initiating node. The destination when receives the RREQ message it will reply with a RREP (Route REPly) message. The route discovery will be successful, when the initiating node receives a RREP message with a list containing a sequence of network hops.

B. Selfish Node Behaviour

In MANET some nodes may refuse to participate in routing and packet forwarding to save their resources leading to selfish behaviour. A selfish node does not perform the process related to packet forwarding for data packets which are not related to it. The selfish node utilizes its limited resources only for its own purpose because of the energy and storage constraints for each node in MANET. It aims to save its resources to the maximum, so this type of misbehaving node discards all incoming packets except those that are destined to it.

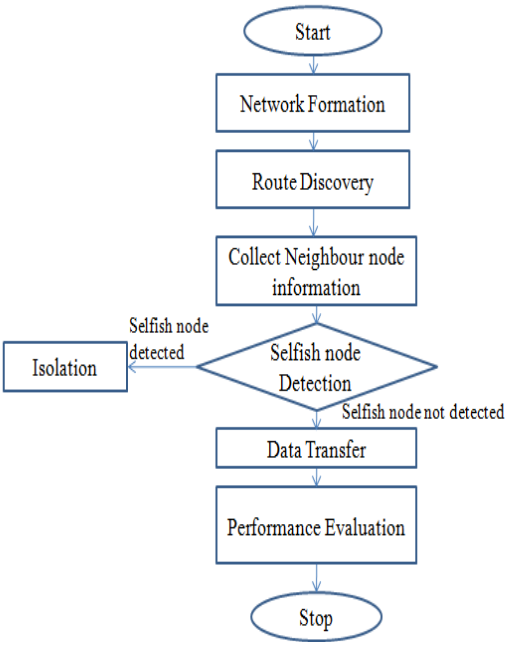

Fig 2 Flow chart of ESDIT technique

DOI 10.17148/IJARCCE.2016.57137

C. Efficient Selfish Node Detection and Isolation Technique

In MANET, nodes may communicate directly or they make use of intermediate nodes. Route is discovered between the source and destination node using RREQ and RREP messages. The neighbouring nodes information is collected to calculate the assurance value. The assurance value is calculated based on the success and failure rates of route request, reply and data transmission.

$$R_{req} = \frac{R_{rsr} - R_{rfr}}{R_{rsr} + R_{rfr}} \qquad (1)$$

$$R_{res} = \frac{R_{psr} - R_{pfr}}{R_{psr} + R_{pfr}} \qquad (2)$$

$$R_{data} = \frac{R_{dsr} - R_{dfr}}{R_{dsr} + R_{dfr}} \qquad (3)$$

R_{req}, R_{res} and R_{data} represent the node request rate, node response rate and data transmission rate calculated as shown in equations (1), (2) and (3) respectively.R_{rsr} represents the route request success rate, evaluated based on the number of nodes that have successfully received RREQ messages from the source node. R_{rfr} represents the route request failure rate, evaluated based on the number of nodes that have not successfully received RREQ messages from the source node. R_{psr} is defined as the route reply success rate, evaluated based on the successful RREP messages received by the source. R_{pfr} is defined as the route reply failure rate, evaluated based on the number of nodes that have not sent the RREP messages. R_{dsr} represents the data success rate, evaluated based on successful transmission of data. R_{dfr} represents the data failure rate, evaluated based on the data that have not reached the destination successfully. Based on the assurance value, the selfish nodes are detected. Once selfish nodes are detected, they are added to block list and are isolated from the network. Data will be transferred to non-selfish nodes.

IV. PERFORMANCE ANALYSIS

The ESDIT has been implemented using NS2.34 (Network Simulator version 2.34) and the performance of the proposed ESDIT is compared with the existing watchdog mechanism. The performance of the network is evaluated using four different metrics: packet delivery ratio, throughput, end-to-end delay and energy consumed. Table 1 shows the simulation parameters.

TABLE I SIMULATION PARAMETERS

Simulation Parameter	Value
Simulator	NS2(Version 2.34)
Propagation model	Two Ray Ground
Antenna type	Omni Antenna
Channel type	Wireless channel
Simulation area	500m×500m
Number of mobile nodes	50
Simulation time	10s
Traffic type	Constant Bit Rate(CBR)

A. Packet Delivery Ratio (PDR)

PDR is described as ratio between the number of data packets received by the destination node and number of data packets transmitted by the source node as shown in equation (4). Greater the value of packet delivery ratio better will be the performance of the protocol. Fig. 3 and Fig. 4 shows the comparison of PDR graph between the watchdog and ESDIT technique. Compared to watchdog the number of packets delivered is more for ESDIT.

$$\text{Packet Delivery Ratio} = \frac{\sum Number\ \ of\ packets\ \ received}{\sum Number\ \ of\ packets\ \ sent} \qquad (4)$$

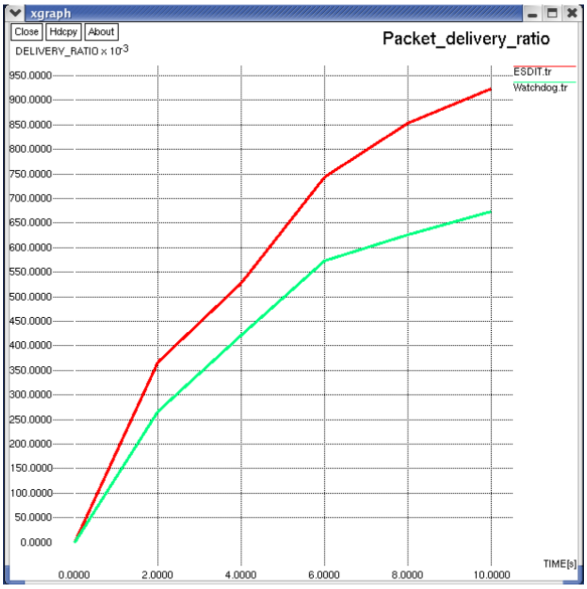

Fig. 3. PDR – ESDIT vs. watchdog

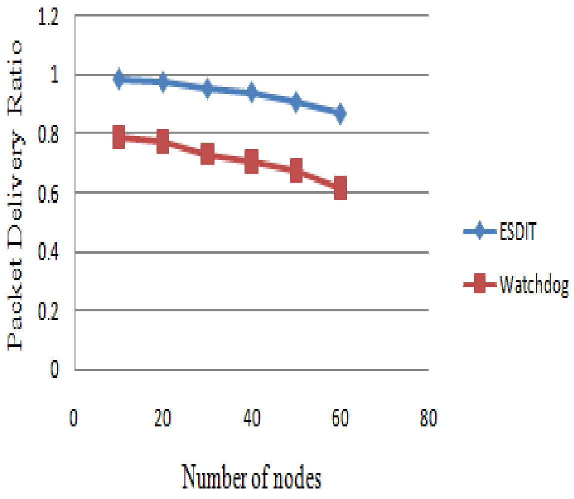

Fig. 4. PDR for both ESDIT and watchdog w.r.t. number of nodes

DOI 10.17148/IJARCCE.2016.57137

B. Throughput

Throughput is the number of data packets successfully received by receiver with in the data transmission time as shown in equation (5). In any network throughput is the average rate of data packets delivered successfully from source node to destination node. Throughput is measured in bits/bytes per second. Higher throughput is the most essential factor in any network.

Fig. 5 and Fig. 6 shows the comparison of throughput graph between the watchdog and ESDIT technique. The number of packets received by destination node within the data transmission time is more for ESDIT when compared with watchdog.

$$\text{Throughput}=\frac{number\ \ of\ packets\ \ delivered\ \ *packet\ \ size}{total\ \ duration\ \ of\ simulation} \quad (5)$$

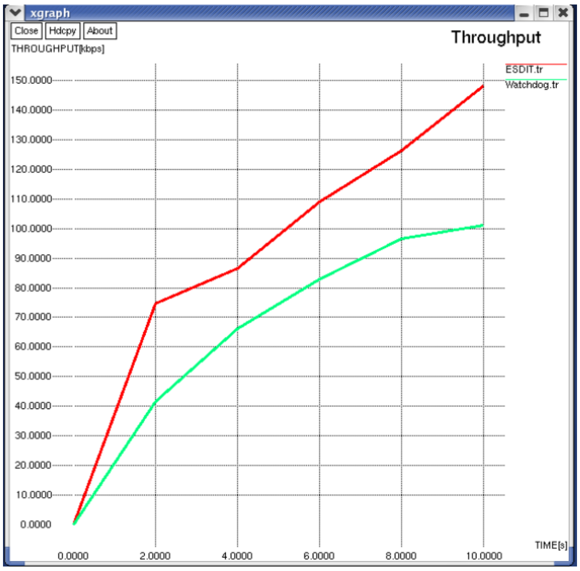

Fig. 5. Throughput– ESDIT vs. watchdog

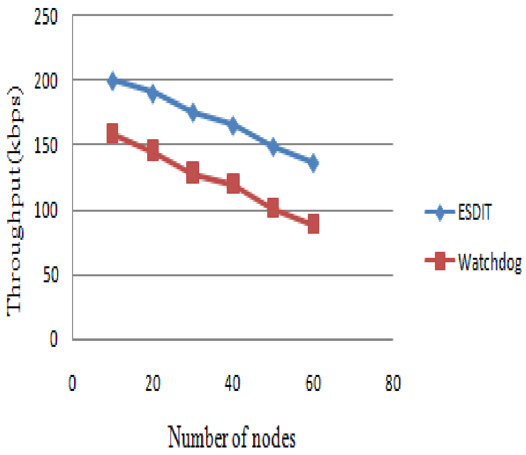

Fig. 6. Throughput for both ESDIT and watchdog w.r.t. number of nodes

C. End-to-end Delay

It can be defined as the average amount of time taken by the data packets to transmit from source node to destination node across MANET. End-to-end delay includes all the possible delays taken by the router to seek path in network consumption, retransmission delay, propagation delay and processing delay. End-to-end delay for the data packet dp sent by the node n, as a source node and received by destination node successfully is as shown in equation (6)

$$End\ to\ end\ delay_{ndp}=starttime_{ndp}-endtime_{ndp} \quad (6)$$

Where $starttime_{ndp}$ is the time at which the node n starts sending data packet dp, $endtime_{ndp}$ is the time at which the destination receives the data packet successfully sent by node n. Fig. 7 and Fig. 8 shows the comparison of end-to-end delay graph between the watchdog and ESDIT technique.

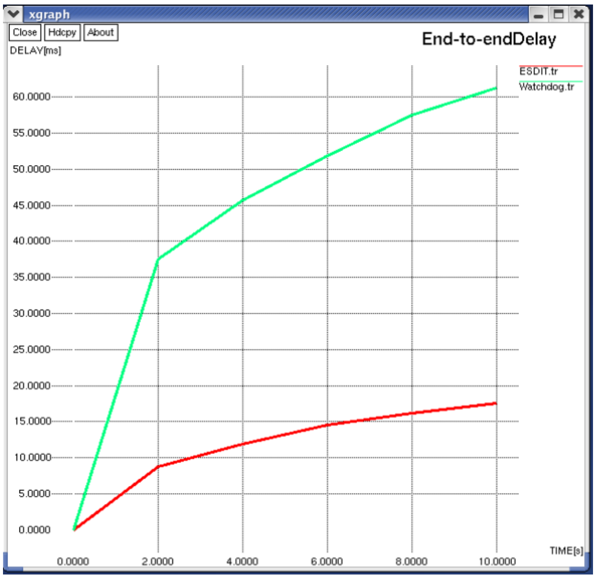

Fig. 7. End-to-end Delay– ESDIT vs. watchdog

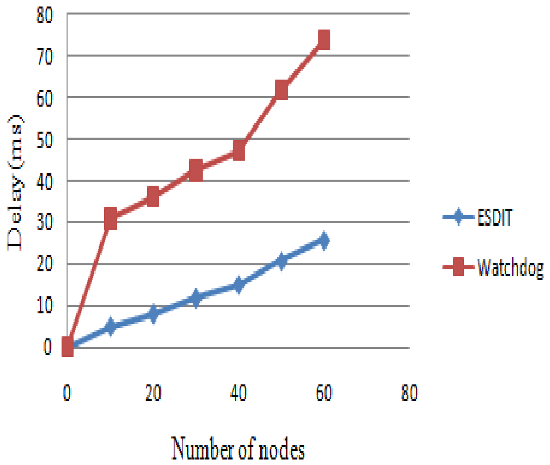

Fig. 8. End-to-end Delay for both ESDIT and watchdog w.r.t. number of nodes

D. Energy Consumed

In MANET four possible states of energy consumption are transmit, receive, idle and sleep state. In transmit and receive states the nodes transmit and receive packets

DOI 10.17148/IJARCCE.2016.57137

respectively. In idle state the nodes may either transmit or receive the packets, while in sleep state the node neither transmits nor receives the packets until it is woken up.

It is defined as the amount of energy consumed by all the nodes in the network during the transmission of packets. It is measured in Joules. Fig. 9 and Fig. 10 shows the comparison of average energy consumed graph between the watchdog and ESDIT technique. The average energy consumed by the mobile nodes in the network is low for ESDIT when compared with watchdog.

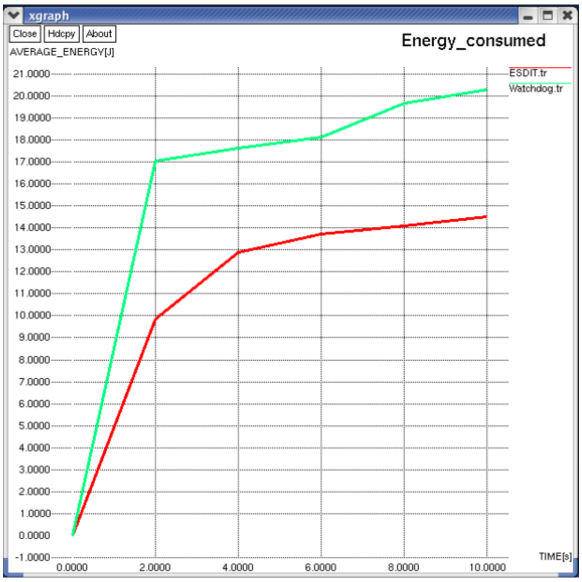

Fig. 9. Energy consumed– ESDIT vs. watchdog

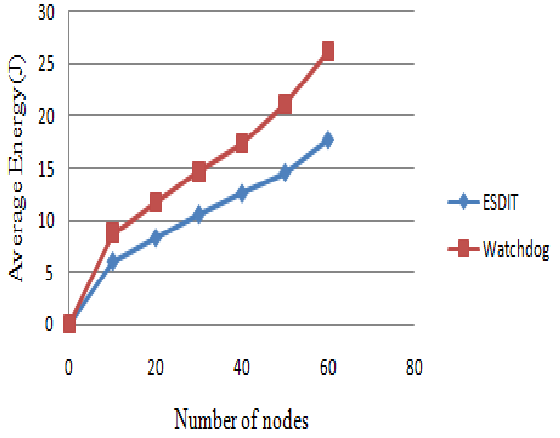

Fig. 10. Energy consumed for both ESDIT and watchdog w.r.t. number of nodes

From the above results it is observed that the proposed ESDIT technique is effective and improves the performance of MANET compared to watchdog mechanism.

V. CONCLUSION

In MANET some nodes may refuse to participate in routing and packet forwarding to save their resources leading to selfish behaviour. Selfish node purposely delays and drops the packets to utilize its minimal resources only for its own purpose. Existence of selfish nodes in MANET degrades its performance. In this paper, ESDIT is proposed to detect and isolate selfish nodes in MANET. It enhances the performance metrics such as packet delivery ratio and throughput. Compared to the traditional watchdog mechanism the proposed ESDIT technique performs significantly better and improves the performance of MANET.

REFERENCES

[1] J. H. Choi, K. S. Shim, S. Lee and K. L. Wu, "Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network," in IEEE Transactions on Mobile Computing, vol. 11, no. 2, pp. 278-291, Feb. 2012.

[2] E. Hernández-Orallo, M.S. Olmos, J.C. Cano, C. Calafate and P. Manzoni, "A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs," Wireless Personal Communications, vol. 74,no. 3, pp. 1099–1116, Feb. 2014.

[3] I. Jawhar, Z. Trabelsi and J. Al-Jaroodi, "Towards more reliable and secure source routing in mobile ad hoc and sensor networks," Telecommunication Systems, vol. 55,no. 1, pp. 81–91, Jan. 2014.

[4] A. Rodriguez-Mayol and J. Gozalvez, "Reputation based selfishness prevention techniques for mobile ad-hoc networks," Telecommunication Systems, vol. 57, no. 2, pp. 181–195, Oct. 2014.

[5] E. Hernandez-Orallo, M. D. Serrat, J. C. Cano, C. T. Calafate and P. Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," in IEEE Communications Letters, vol. 16, no. 5, pp. 642-645, May 2012.

[6] S. Padiya, R. Pandit and S. Patel, "Survey of innovated techniques to detect selfish nodes in MANET," International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), vol. 3, no. 1, pp. 221-230, Mar. 2013.

[7] D.B. Roy, R. Chaki "MADSN: mobile agent based detection of selfish node in MANET," International Journal of Wireless & Mobile Networks (IJWMN), vol. 3, no. 4, pp. 225-235, Aug. 2011.

[8] D. Koshti, S. Kamoji, "Comparative study of techniques used for detection of selfish nodes in mobile ad hoc networks," International Journal of Soft Computing and Engineering (IJSCE), vol. 1, no. 4, pp. 190-194, Sep. 2011.

[9] Y. Yoo, S. Ahn, and D. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in IEEE International Conference on Communications , vol. 5, pp. 3005–3009, May 2005.

[10] P.Ramya, S.Bhavani, V.Priyadarshini, "An Improved Energy Efficient and Certificate Revocation Technique for Mobile Ad Hoc Networks", IEEE sponsored 4th International Conference on Communications, Signal Processing, Computing and Information Technologies (ICCSPCIT-2015), MRCET, December 18-19, 2015.

[11] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat Proof, Credit based System for Mobile Ad Hoc Networks," in Proc. of IEEE Infocom, vol. 3, no., pp. 1987-1997, Apr. 2003.

[12] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat Proof, Credit based System for Mobile Ad Hoc Networks," in Proc. of IEEE Infocom, vol. 3, no., pp. 1987-1997, Apr. 2003.