Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.3, No.7, 2013

Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm

Rajpal Singh Khainwar
CSE. Deptt., RITS, Bhopal, India.
rajpalsingh1@gmail.com
Mr. Anurag Jain
CSE. Deptt., RITS, Bhopal, India.
ak.jain@gmail.com
Mr. Jagdish Prasad Tyagi
ECE. Deptt., MGCGV, Chitrakoot, India.
to.jptyagi@gmail.com

Abstract
In MANET, the more security is required in comparison to wired network. Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack. The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route with fewer. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. In this paper we specifically considering Wormhole attack. Instead of detecting suspicious routes as in previous methods, in this paper we implement a new method which detects malicious nodes and works without modification of protocol, using a hop-count and time delay analysis from the users point of view without any special environment assumptions. The proposed work is simulated using OPNET and results showing the advantages of proposed work.
Keywords: ad hoc network, hop-count analysis, network security, wormhole attack**.**

1 Introduction

A Mobile Ad-hoc Network (MANET) comprises nodes that are organized and maintained in a distributed manner without a fixed infrastructure. These nodes, such as wireless phones, have a limited transmission range. Hence, each node has the ability to communicate directly with another node and forward messages to neighbors until the messages arrive at the destination nodes i.e. the nodes act as both host and router at the same time, i.e., each node in the network can be independent. Since the transmission between two nodes has to rely on relay nodes, many routing protocols [1, 2, 3, 4] have been proposed for ad hoc networks. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Figure 1. The resulting route through the wormhole may have a better metric, i.e., a lower hop-count than normal routes. With this leverage, attackers using wormholes can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DoS (Denial of Service) attack. The entire routing system in MANET can even be brought down using the wormhole attack. Its severity and influence has been analyzed in [5].

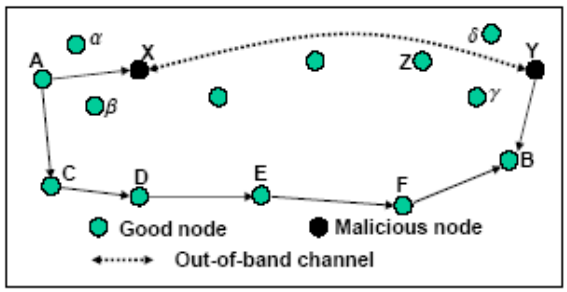

Fig 1.1 The wormhole attack in MANET

In wireless network many types of attacks can be initiated but most of them are relative easy to detect because of their property of dramatically altering the network statistics but one different type of attack we consider in this thesis. It is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand).

This paper is organized as follows. Section 2 presents related works regarding wormhole attacks. Section 3 presents proposed work. Simulation results and analysis are presented in Section 4. Finally, the conclusion is provided in Section 5.

2. Literature Survey

In this section, we review related works in the literature which discuss proposed wormhole attack defenses.

Packet Leash [6] is an approach in which some information is added to restrict the maximum transmission distance of packet. There are two types of packet leashes: geographic leash and temporal leash. In geographic leash, when a node A sends a packet to another node B, the node must include its location information and sending time into the packet. B can estimate the distance between them. The geographic leash computes an upper bound on the distance, whereas the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes' clocks is bounded by Δ, and this value should be known to all the nodes. By using metrics, each node checks the expiration time in the packet and determine whether or not wormhole attacks have occurred. If a packet receiving time exceed the expiration time, the packet is discarded.

Unlike Packet Leash, Capkun et al. [7] presented SECTOR, which does not require any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). Node A estimates the distance to another node B in its transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash is.

Shalini Jain et al. [8] presented a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, demonstrate that scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase.

In order to avoid the problem of using special hardware, a Round Trip Time (RTT) mechanism [9] is proposed by Jane Zhen and Sampalli. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving Time from a node B. A will calculate the RTT between A and all its neighbors. Because the RTT between two fake neighbors is higher than between two real neighbors, node A can identify both the fake and real neighbors. In this mechanism, each node calculates the RTT between itself and all its neighbors. This mechanism does not require any special hardware and it is easy to implement; however it cannot detect exposed attacks because fake neighbors are created in exposed attacks.

Debdutta Barman Roy et al. [10] presented a cluster based counter-measure for the wormhole attack; Routing security in ad hoc networks is often equated with strong and feasible node authentication and lightweight cryptography. Unfortunately, the wormhole attack can hardly be defeated by crypto graphical measures, as wormhole attackers do not create separate packets. They simply replay packets already existing on the network, which pass the cryptographic checks. Existing works on wormhole detection have often focused on detection using specialized hardware, such as directional antennas, etc. alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. In this a cluster based counter-measure for the wormhole attack that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET.

Khalil et al. [11] introduces LITEWORP in which they used the notion of guard node. The guard node can detect the wormhole if one of its neighbors is behaving maliciously. The guard node is a common neighbor of two nodes to detect a legitimate link between them. In a sparse network, however, it is not always possible to find a guard node for a particular link.

Sun Choi et al. [12] presented an effective method called Wormhole Attack Prevention (WAP) without using specialized hardware. In WAP All nodes monitor its neighbor's behavior when they send RREQ messages to the destination by using a special list called Neighbor List. When a source node receives some RREP messages, it can detect a route under wormhole attack among the routes. Once wormhole node is detected, source node records them in the Wormhole Node List. Even though malicious nodes have been excluded from routing in the past, the nodes have a chance of attack once more. Therefore, we store the information of wormhole nodes at the source node to prevent them taking part in routing again.

However, most of these mechanisms require some special assumptions and supporting hardware, and some of them are based on specific protocols.

3. Proposed Work

In this method we specifically consider Wormhole attack which does not require exploiting any nodes in the network and interfere with the route establishment process. Instead of detecting suspicious routes as in

previous methods, We implement a new method which detects the attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions. The proposed work is simulated using OPNET and results showing the advantages of proposed work. The steps of modeling in FSM (Finite State Machine) of Proposed Algorithm are as follows:

Step1. Randomly Generate a Number in between 0 to maximum number of nodes.
Step2. Make the Node with same number as transmitter node.
Step3. Generate the Route from selected transmitting node to any destination node with specified average route length.
Step4. Send packet According to selected destination and start timer to count hops and delay.
Step5. Repeat the process and store routes and their hops and delay.
Step6. Now if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker.
Step7. Now check the delay of all previous routes which involve any on node of the suspicious route. Now the node not encounter previously should be malicious let there are N such nodes.
Step8. In N == 1 then it is the attacker else wait for future sequences which shows deviation and involve only one of N nodes.
Step9. These nodes are black listed by the nodes hence they are not involved in future routes.
Step10. Whole process (from step1 to step9) is repeated until we didn't get the specified goal (goal can be
1. To get complete list of malicious nodes.
2. To run for specified time.
3. To run for specific number of packets etc.

4. Implementation and Results

Validation of the proposed algorithm is performed by simulating it on network simulation software OPNET 14.0. For the evaluation of practical feasibility & effectiveness of the proposed algorithm we generated many scenarios for analysis of the system under all practically possible conditions. Some of the major analysis parameters for which scenarios designed are:

(i) How the algorithm works with High (50) Nodes density with varying number of attackers.
(ii) Effect of algorithm under different traffic conditions.
(iii) Effect of algorithm for different probability distribution for node packet generation & inter arrival time

4.1 Simulation Environment and Parameters:

The effectiveness of our protocol to detect wormhole attacks is evaluated in this section using extensive simulations. We have performed the simulation of the proposed scheme in Opnet Network Modeler 14.0 to prove practical efficiency of the method. The radio model corresponds to the 802.11 Wave LAN, operating at a maximum air-link rate of 11 Mbps. CBR traffic pattern is used.

4.1.1 Parameters

No. of Nodes	50
No. of Malicious Nodes	6
Data Rate	11 Mbps.
Area	10 square Km.
Routing Protocol	AODV
Traffic Model	CBR
MAC	IEEE 802.11
Mobility	Random
Packet inter arrival time	1sec. constant
Packet size	1024 bits

4.1.2 RF Transmitter Properties

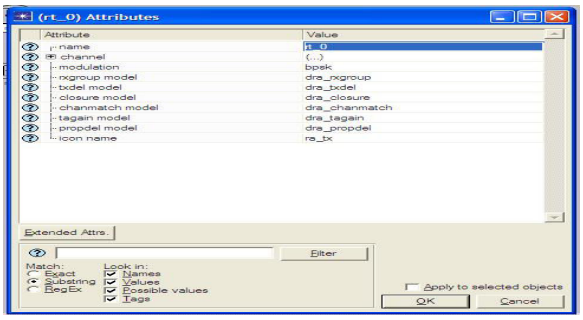

Fig 4.1

4.1.3 RF Receiver Properties

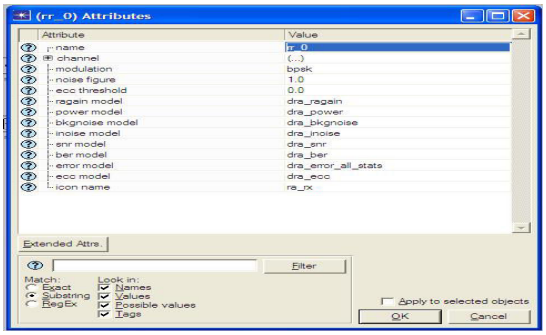

Fig 4.2

4.2 Simulation Results

The simulation results from Opnet Network Modeler 14.0 with respect to the Average Hop count per route and Average delay per route in different scenario.

4.2.1 Scenario 1:- 50 Nodes distribution without wormhole attack:

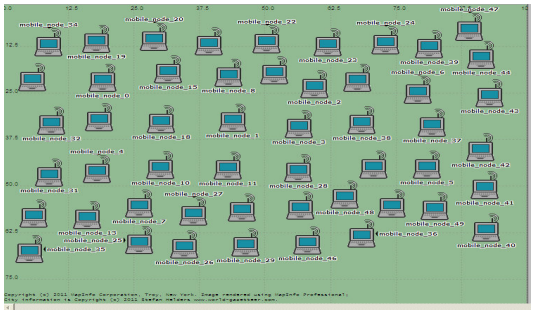

Fig 4.3

Initial distribution of the nodes which is almost uniform this scenario is for high node density system with no wormhole attack.

4.2.1.1 Average Hop count per route in scenario 1 without wormhole attack

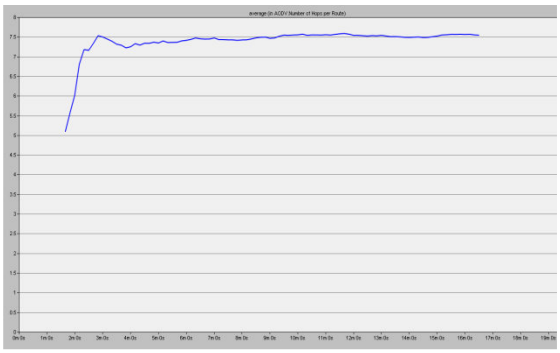

Fig 4.4

Average Hop count per route show's that under high node density conditions created scenario having average route length of 7.5 & will be used as reference for attack indicator.

4.2.1.2 Average delays per route in scenario 4 without wormhole attack

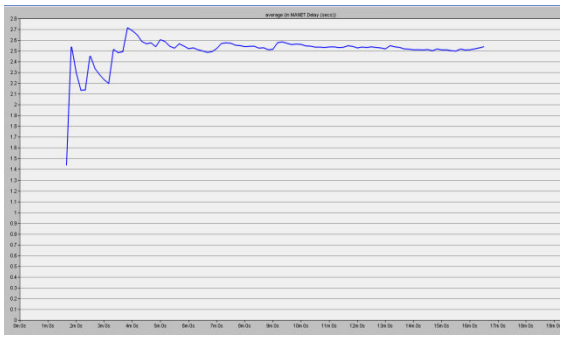

Fig 4.5

Average delay per route show's that under normal conditions created scenario having average delay per route2.5 & will be used as reference for attack indicator.

4.2.2 Scenario 2:- 50 Nodes distribution with wormhole attack

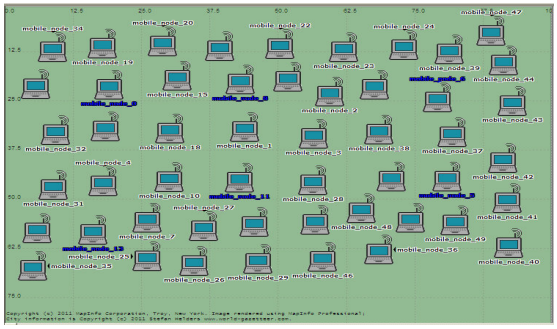

Fig 4.6

Initial distribution of the nodes which is almost uniform this scenario is for high node density system with wormhole attack. The scenario having a attacking tunnel between highlighted nodes.

4.2.2.1 Average Hop count per route in scenario 2 with wormhole attack

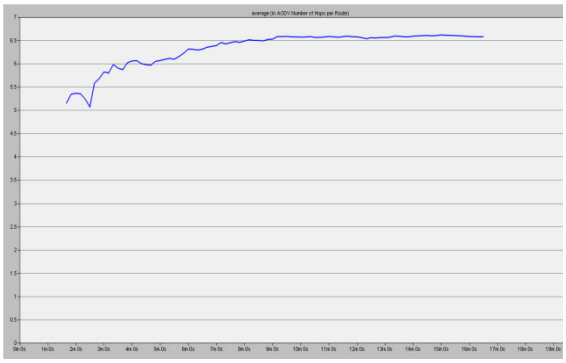

Fig 4.7

With no Prevention to attack, the graph shows decrease in average hop count. In Present scenario Average hop count per route decrease from 7.5 to 6.5

4.2.2.2 Average delays per route in scenario 2 with wormhole attack

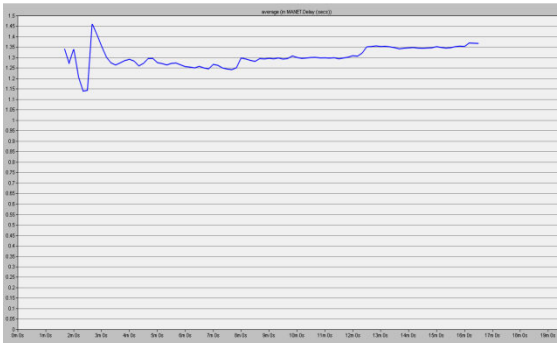

Fig 4.8

Average delay per route in scenario 2 shows Significant in delay because of involvement of attacker.

4.2.3 Scenario 3:- 50 Nodes distribution with wormhole attack and applied proposed Algorithm

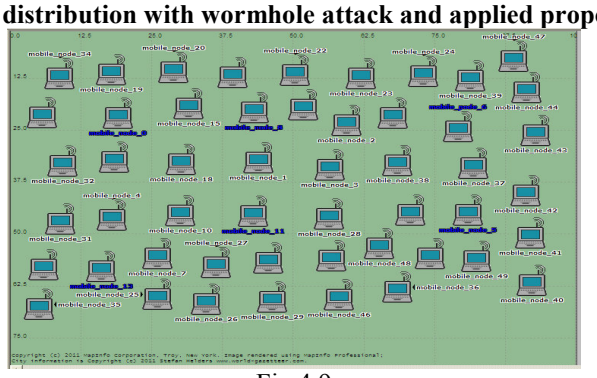

Fig 4.9

Initial distribution of the nodes which is almost uniform this scenario is for high node density system with wormhole attack. The scenario having an attacking tunnel between highlighted nodes, and applied proposed algorithm of them.

4.2.3.1 Average Hop count per route in scenario 3 with wormhole attack and applied proposed Algorithm

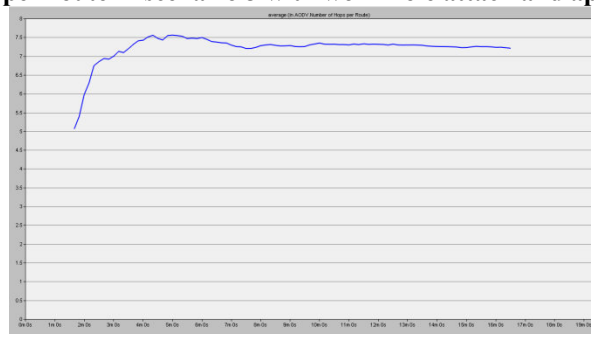

Fig 4.9

Average Hop count per route in scenario 6 increase in average hop count indicates that now the nodes avoiding attacker's path with very effectively.

4.2.3.2 Average delays per route in scenario 6 with wormhole attack and applied proposed algorithm

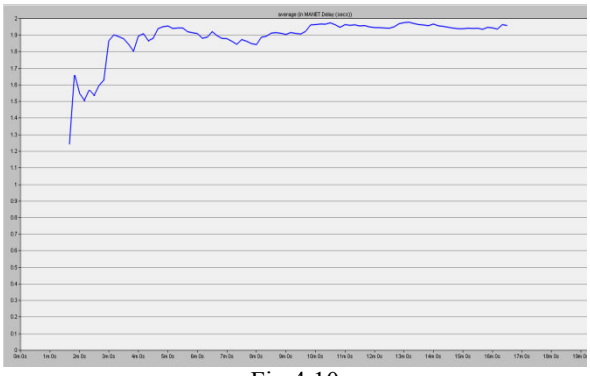

Fig 4.10

Average delays per route in scenario 3 the delay is again setting to original evaluating as in without attack scenario.

4.2.4 Average Hop count per route comparison in 50 nodes

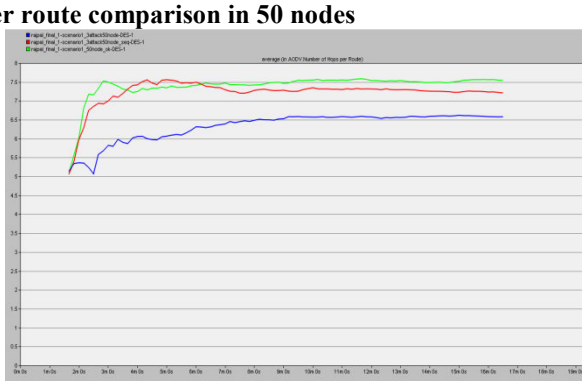

Fig 4.11

Attack reduces the average hop count by 13% (shown in blue) from normal condition (shown in green) which shows the selection of attaching node in route, the proposed algorithm significantly regains the hop counts by avoiding the attacker (shown in red**).**

4.2.5 Average delays per route comparison in 50 nodes

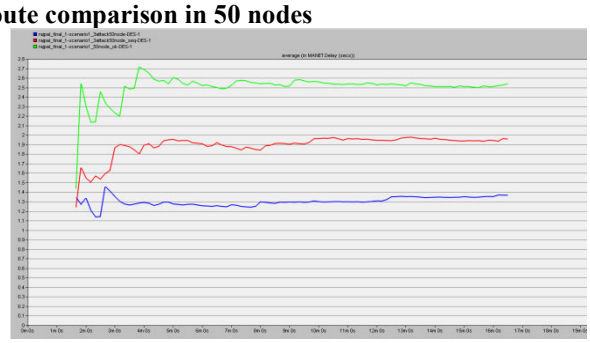

Fig 4.12

Attack reduces the average delay by 48% (shown in blue) from normal condition (shown in green) which shows the shorting of route by attacking route, the proposed algorithm have much better delay which presents the elimination of attacker (shown in red).

5. Conclusion

Our method provides good performance for detecting wormhole attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users, without any special environment assumptions. When the nodes found malicious behavior then these nodes are black listed by the source node hence they are not involved in future routes. Our method provides good performance for high node density system compare to average and low density system.

REFERENCES

[1] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. RFC 3561, The Internet Engineering Task Force, Network Working Group, Jul 2003. http://www.ietf.org/rfc/rfc3561.txt.

[2] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors,Mobile Computing, volume 353, pages 153–181. Kluwer Academic Publishers, 1996.

[3] D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. RFC 4728, The Internet Engineering Task Force, Network Working Group, Feb 2007. http://www.ietf.org/rfc/rfc4728.txt.

[4] R. V. Boppana and S. P. Konduru. An adaptive distance vector routing algorithm for mobile, ad hoc networks. In IEEE Computer and communications Societies (INFOCOM 2001), pages 1753–1762, 2001.

[5] Khabbazian, M.; Mercier, H.; Bhargava, V.K. Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks. IEEE Trans. Wireless Commun. 2009, 8, 736–745.

[6] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. IEEE INFOCOM, Mar 2003.

[7] S. Capkun, L. Butty´an, and J.-P. Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pages 21–32, Oct 2003.

[8] Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" in International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201, pp.78-86.
[9] J. Zhen and S. Srinivas. Preventing replay attacks for ecure routing in ad hoc networks. In ADHOC-NOW, LNCS 2865, pages 140–150, 2003.
[10] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki " A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks" in International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009, 44-52.
[11] I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. International Conference on Dependable Systems and Networks, pp. 612–621, 2005.
[12] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, pp. 343-348.
[13]. Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. pp. 2- 17.
[14]. C. Siva Ram Murthy and B.S. Manoj. [2004] " Ad Hoc Wireless Networks, Architecture and Protocols", 2004 Pearson Education, pp. 321-386, 473-526.