國立交通大學

資訊科學與工程研究所

碩士論文

在無線隨意式網路中可抵抗蟲洞攻擊
之路由協定

An auto-resilient routing protocol against
wormhole attacks in Mobile Ad-hoc network

研 究 生：王偉民

指導教授：蔡文能　教授

中華民國九十八年五月

在無線隨意式網路中可抵抗蟲洞攻擊之路由協定

An auto-resilient routing protocol against wormhole attacks in mobile Ad-hoc network

研究生：王偉民　　Student：Wei-Ming Wang

指導教授：蔡文能　　Advisor：Wen-Nung Tsai

國立交通大學
資訊科學與工程研究所
碩士論文

A Thesis
Submitted to Institute of Computer Science and Engineering
College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master

In

Computer Science
May 2009
Hsinchu, Taiwan, Republic of China

中華民國九十八年五月

在無線隨意式網路中可抵抗蟲洞攻擊之路由協定

研究生： 王偉民　　　　　　　　　　　　指導教授：蔡文能教授

國立交通大學

資訊科學與工程學系碩士班

摘要

無線隨意式網路是一種在節點間可自我組態的網路並且在網路內的節點皆可自由移動以及擁有路由的能力。然而，這些無線隨意式網路的特性無形中也增加了蟲洞攻擊發生的危險性。近幾來來，關於如何在無線隨意式網路中防範蟲洞攻擊一直是熱門的研究議題。然而之前所提的方法，大部分將重點擺在如何根據蟲洞的行為來設計解決的方法，然而在我們的研究中認為從根本的路由協議中找出其路由弱點並且加以克服解決將可以有較好的防制效果。我們將在本論文研究在無線隨意式網路中路由協議的弱點並且進一步提出健壯的路由協議來避免攻擊。

An auto-resilient routing protocol against wormhole attacks in mobile Ad-hoc network

Student: Wei-Ming Wang **Advisor: Wen-Nung Tsai**

Department of Computer Science and Information Engineering
National Chiao-Tung University

Abstract

The Mobile Ad-hoc networks (MANETs) are self-configuring network and each node in MANETs is free to move and has the ability to route packets. However, these characteristics will give rise to Wormhole attack which will increase the influences of network attacks. In recent years, the methods how to avoid wormhole attacks have become attractive research issues. However, many previous works focus on observing the behavior of wormhole node to solve the attack issues. We thought against wormhole attack utilizing the routing characteristics of MANETs will has the better resulting of avoiding attacks. We researched the routing protocol of MANETs, present the wormhole attacks using the weakness of routing protocols and we will propose a robust routing protocol to solve the wormhole attacks.

誌謝

本論文能夠順利完成，首先要感謝蔡文能老師這兩年來的指導，不論在研究議題以及論文內容都給了很多寶貴的建議。再來要感謝宗易學長一路上熱心的幫忙以及協助指導。另外，還有實驗室的同學彥寧、昱華和安勝，陪我度過這兩年愉快的研究所時光。最後要感謝家人還有女朋友鈺穎的一路上的鼓勵和支持，讓我可以如期完成論文和碩士學位。

Contents

List of Figure

Chapter 1 Introduction

In recent years, the MANET (mobile ad hoc network) technology has become a mature technology and also it has been more and more popular. The MANET is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. In comparison with traditional network environment that depends on some infrastructure, mobile ad hoc network can communication each other without infrastructure.

However, some characteristics of mobile ad hoc network will increase their vulnerability to attacks. Wireless links are inherently vulnerable to eavesdropping and message injection, as well as jamming attacks. In these security issues, security routing in MANET is an especially hard task to accomplish securely, robustly and efficiently. The MANET is constrained in memory, computing power, and battery power in mobile devices. These restrictions will result that routing protocol of MANET should be faced a tradeoff between security and resource consumption.

In this theme, we conduct a study for the wormhole attack and we proposed a routing protocol against wormhole attack in AODV, our method will be effective to prevent wormhole attacks and it is very suitable for MANET environment due to it does not require too much computing or any special hardware.

1.1 Research Motivation and Goals

In our research, we introduce the wormhole attack which has formed a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. Also, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack. In this theme, we design an effect approach to against wormhole attacks and this approach can not only detect the wormhole attack but also auto resilient from wormhole attack. Many of the existing methods have requirements of time synchronization, GPS receiver, etc. However, our proposed protocol does not require special hardware and only need few computing resources.

1.2 Thesis Organization

The rest of this thesis is organized as follows: In Chapter 2, we discuss the background about Wireless Security issues and the routing protocol of Wireless Ad-hoc Network. In chapter

3, we discuss the related works and compare their advantages and disadvantages. In Chapter 4, we present our Auto-resilient Routing against Wormhole Attacks in Ad Hoc Networks. In Chapter 5, we discuss our evaluation methods and the results. Finally, we conclude this thesis in Chapter 6.

Chapter 2　Background

In the section, we will discuss three topics about mobile Ad-Hoc networks include routing protocol of MANETs, related security issues of MANETs and wormhole attacks. Unlike traditional wired network or infrastructure-based wireless network, each node in mobile Ad-Hoc network has routing capabilities; the prototype of mobile Ad-Hoc network composes when a collection of mobile nodes link together and create a network by agreeing to route messages for each other. There is no shared infrastructure in an Ad-Hoc network such as centralized routers or defined administrative policy.

However, these feathers of ad hoc network routing protocol bring new security problems. Unlike traditional wire network or infrastructure-based wireless network, each node in Ad-Hoc network has routing capabilities and can be regarded as independent; it means each node in the Ad-Hoc networks can arbitrarily attack other nodes by changing the routing rules. We will introduction these security issues in section 2.2 and Wormhole Attack, the most intractable security attack of MANET, in section 2.3.

2.1 Routing Protocols in mobile Ad-Hoc Networks

A mobile Ad-Hoc network is a collection of mobile nodes that are dynamically and arbitrarily located in such a method that the interconnections between nodes are capable of changing on a continual basis. In order to facilitate communication within the network, a routing protocol is used to discover the path between nodes. An Ad-Hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. The primary goal of such an ad hoc network routing protocol is exact and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption.

In Ad-Hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

Classification of routing protocols in MANET’s can be done in many ways, but most of these are done depending on routing strategy and network structure [13][14]. According to the routing strategy the routing protocols can be categorized as Table-driven and source initiated.

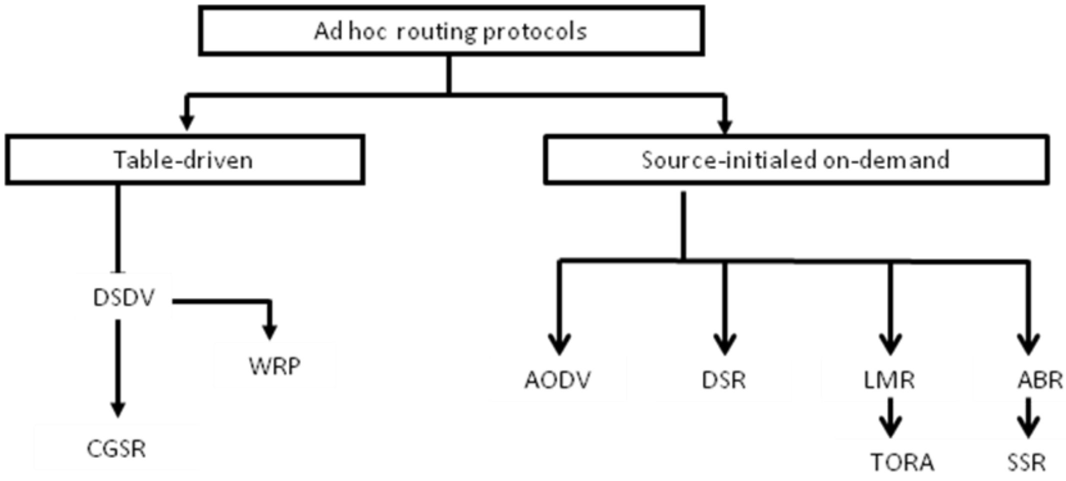


Figure 2-1 Classification of routing protocols in MANET

2.1.1 Table-Driven Routing Protocols

These protocols have the same characteristics that they maintain the routing information before it is required. For this characterize, the protocols also called as proactive protocols. Every node in the network maintains routing information to other node in the network. Routes information is usually kept in the routing tables and is periodically updated when the network topology changes. Many of these routing protocols come from the link-state routing. There are some differences between the protocols in this group depending on the routing information and the routing table. These protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to more consumption of bandwidth.

2.1.2 Reactive Routing Protocols

These protocols have the main characteristic that they don't maintain routing information or routing activity in advance when the network in initial step. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network.

2.1.3 Hybrid Routing Protocols

This type of protocols couples the benefit of proactive and of reactive routing like HSLS (Hazy Sighted Link State routing protocol) [15], ZRP (Zone Routing Protocol) [16], etc. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are

1. Benefit should rely on number of nodes in network.
2. The Reaction speed of demand depends on traffic volume.

2.2 Security Issues in Mobile Ad-Hoc Networks

In recent years MANETs (mobile ad hoc networks) have received great attention due to their capabilities of self-configuration and self-maintenance. While security issues have become a primary interest in order to provide safe communication. Mobile Ad-Hoc networks were proposed to support dynamic scenarios and situations where no wired network infrastructure exists. In fact most Ad-Hoc routing protocols are collaborative by nature and rely on implicit trust among the participating nodes to route packets through without any security or information integrity guarantees. However, this is not always suitable especially when information security and integrity is an important issue of the application

Although security issues have been an active research topic for a long time in wired networks and there are a lot of research results. However, unlike the wired networks the unique characteristics of MANETs present a new set of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology.

2.2.1 The Vulnerable Characteristic of Mobile Ad-Hoc Networks

In general, the wireless MANET is especially defenseless due to its fundamental property of open medium, dynamic topology, and absence of central authorities, distributed cooperation, and constrained capability. In this section, we briefly list the following vulnerable characteristics about MANET.

First, use of wireless links causes an Ad-Hoc network vulnerable to security attacks include passive eavesdropping and active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation.

Secondly, nodes, roaming in an unfriendly environment with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by inside nodes.

Thirdly, an Ad-Hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP nodes in an ad hoc network may dynamically become affiliated with administrative domains.

Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

2.2.2 Routing Security in MANETs

Routing protocols in MANETs are very different than traditional network, it has the advantage of free configuration and high flexible. However, the features of routing protocols in MANETs also causes many security attacks be launched by finding the loophole in routing protocols in MANETs. Here we list the a few common attacks by utilizing the leak of routing protocols of MANETs.

Black hole: In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. We provide a detailed description herein.

Denial of service: The DoS attack results when the network bandwidth is hijacked by a malicious node. It has many forms: the classic way is to flood any centralized resource so that the network no longer operates correctly or crashes. For instance, a route request is generated whenever a node has to send data to a particular destination. A malicious node might generate frequent unnecessary route requests to make the network resources unavailable to other nodes.

Routing table overflow: The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.

Information disclosure: The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route.

2.3 Wormhole Attacks in Mobile Ad-Hoc Networks

Wormhole attack is a particularly severe control attack depends on the routing functionality of wireless networks. It has been introduced in the context of Ad-Hoc networks. During the attack, a malicious node captures packets from one location in the network, and “tunnels” them to another malicious node at a distant point, which replays them locally. In fact, the wormhole attack is considered particularly insidious since it can be launched without having access to any cryptographic keys or compromising any legitimate node in the network.

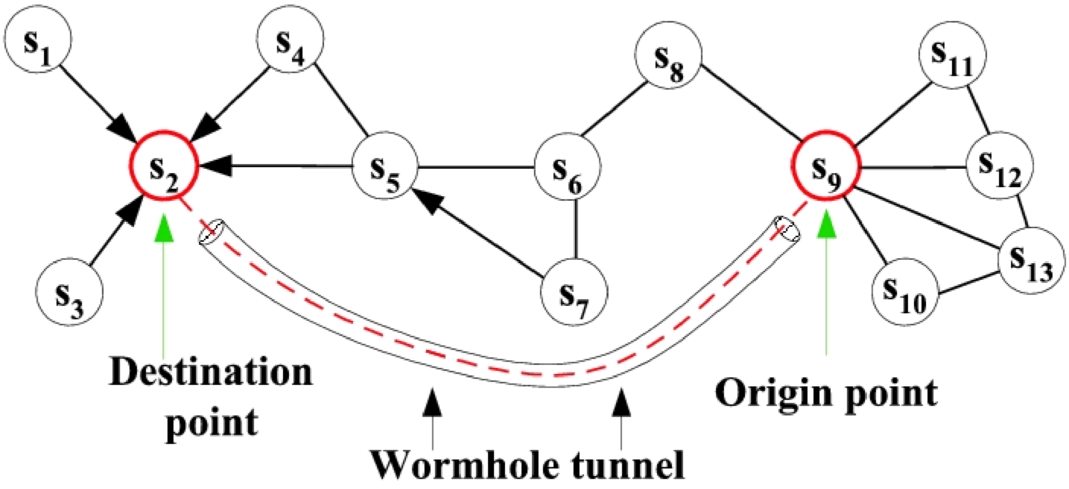


Figure 2-2 Wormhole attack

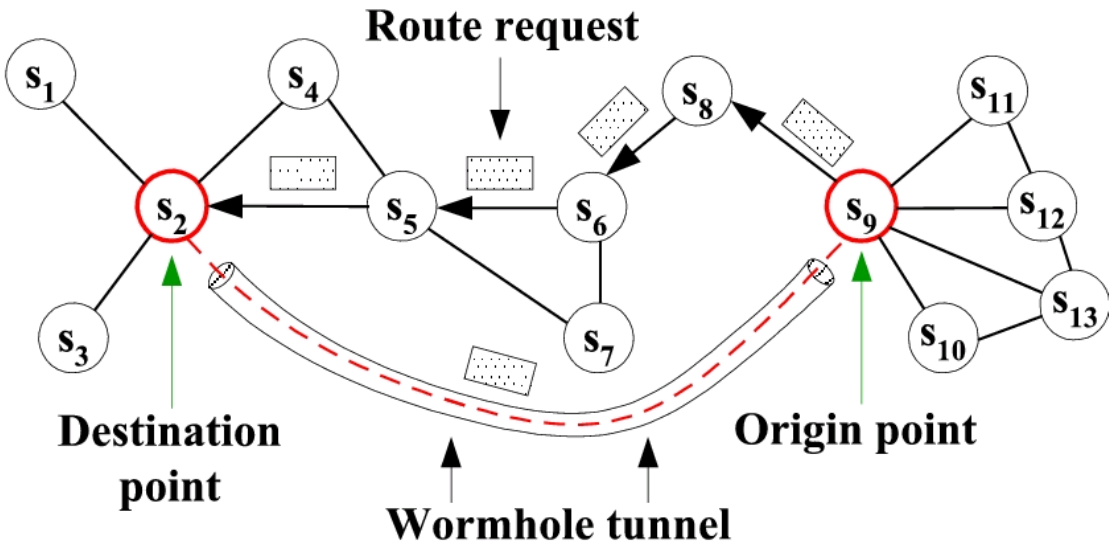


Figure 2-3 Wormhole attack against Routing

2.3.1 Wormhole Attack

Wormhole attacks happen when one wormhole node eavesdrops and records packets at one location, and then tunnels the eavesdropped packets to a certain faraway collusive wormhole node. After receiving the tunneled packets, the faraway collusive wormhole node replays these packets (Figure 2-2). The tunnel between collusive wormhole nodes can be established in various ways, such as direct wire connection, high power transmission, and out-of-band hidden channel.

In a wormhole attack, an attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network. Figure 2-2 shows a basic wormhole attack. The attacker replays packets received by X at node Y, and vice versa. If it would normally take several hops for a packet to traverse from a location near X to a location near Y, packets transmitted near X traveling through the wormhole will arrive at Y before packets traveling through multiple hops in the network. The attacker can make A and B believe they are neighbors by forwarding routing messages, and then selectively drop data messages to disrupt communications between A and B.

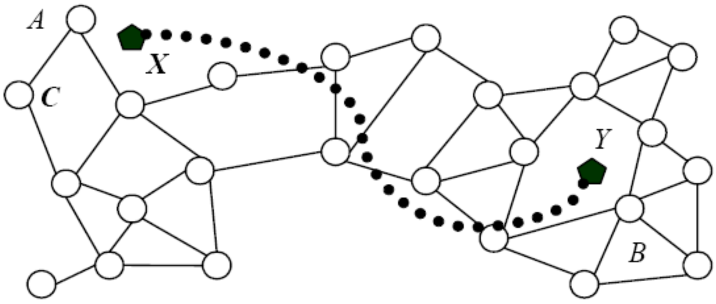


Figure 2-4 Illustration of wormhole attack

For most routing protocols, the attack has impact on nodes beyond the wormhole endpoints' neighborhoods also. Node *A* will advertise a one-hop path to *B* so that *C* will direct packets towards *B* through *A*. For example, in on-demand routing protocols (DSR and AODV) or secure on-demand routing protocols (SEAD, Ariadne, SRP), the wormhole attack can be mounted by tunneling ROUTE REQUEST messages directly to nodes near the destination node. Since the ROUTE REQUEST message is tunneled through high quality channel, it arrives earlier than other requests. According to the protocol, other ROUTE REQUEST messages received for the same route discovery will be discarded. This attack thus prevents any other routes from being discovered, and the wormhole will have full control of the route. The attacker can discard all messages to create a denial-of-service attack, or more subtly, selectively discard certain messages to alter the function of the network. An attacker with a suitable wormhole can easily create a sinkhole that attracts (but does not forward) packets to many destinations. An intelligent attacker may be able to selectively forward messages to enable other attacks.

To show how much damage a single wormhole can cause to routing, we simulated randomly distributing nodes in a rectangular region and used the shortest path algorithm to find the best route between any node pairs. If a wormhole is formed, some far away nodes will appear to be neighbors and some node pairs will be able to find a “shorter” path through the wormhole. Hence the route between them is disrupted by the wormhole. In simulation experiments, a single wormhole with two randomly placed endpoints disrupts over 5% of all network routes. A more intelligent attacker may be able to place wormhole endpoints at particular locations. Strategically placed wormhole endpoints can disrupt nearly all communications to or from a certain node and all other nodes in the network. In sensor network applications, where most communications are directed from sensor nodes to a common base station, wormhole attacks can be particularly devastating. If the base station is at the corner of the network, a wormhole with one endpoint near the base station and the other endpoint one hop away will be able to attract nearly all traffic from sensor nodes to the base station. If the base station is at the center of the network, a single wormhole will be able to attract traffic from a quadrant of the network. Figure 2 shows the effectiveness of a wormhole in disrupting communications from sensor nodes to a base station. One endpoint of the wormhole is within one hop of the base station; the position of the second endpoint varies along the x axis. When the base station is in a corner of the network, a wormhole with the second endpoint near the base station can effectively disrupt all network communications. If the second endpoint is placed in the opposite corner, approximately half of the nodes in the network will send messages for the base station to the wormhole.

2.3.2 The effects of Wormhole Attacks

Wormhole attacks have very different features from other attacks: an adversary does not have to breach the cryptography nor compromise any nodes for launching wormhole attacks, because the adversary nodes need not decapsulate any frames or packets during attacks. What an adversary needs to do is to setup collusive wormhole nodes in wireless networks, to capture radio signals and to build tunnels between the collusive nodes. Then the wormhole nodes can eavesdrop, capture and tunnel radio signals or steal private information that flows via collusive wormhole nodes, although they have no identities or cryptography keys required in the network. Additionally, since wormhole nodes replay signals at a place and can attract network traffic, wormhole attacks are a combination of replay attacks, black hole attacks or grey holes attacks.

Hence, it is much more difficult to detect and prevent wormhole attacks. In fact, if the wormhole nodes conduct no mal-behaviors in the network or are configured by network administrators, wormhole tunnel may be a very pleasing feature. They may provide alternate and faster routes, and even reduce the use of wireless bandwidth and save energy of mobile nodes. But quite often the wormhole nodes may be laid down by malicious adversaries.

Wormhole attacks affect a network most significantly while nodes are establishing route to another node. Wormhole attacks can make particular nodes in a network generate improper routing tables for themselves. For example, if a wormhole attack is launched on a periodic routing protocol, such as optimized link state routing protocol (OLSR), the collusive wormhole nodes can let a regular node trust some other nodes are its neighbor nodes. In figure 1.2, node S broadcast a *Hello* message periodically. If no wormhole nodes exist, only node A and B learn that S is their neighbor nodes; however, if wormhole attacks exist, M_1 can tunnel the *Hello* message to M_2, and M_2 replays the Hello message. As a result, node W, X, Y and Z also believe that S is their neighbor nodes

Besides periodic routing protocol, wormhole attacks can also cause great disruption on on-deman routing protocol, such as DSR [9] and AODV [10]. Firstly, we suppose no wormhole attacks happen in figure 1.3. We assume that S is attempting to establish a new route to W. S can establish a good route to W by sending a route request (RREQ) through node A, C, D and W respectively, thus S knows a route of S

-> A -> C -> D -> W. On the other hand, we assume that wormhole attacks exist, nodes.

It is worth noting that in the network, although both M_1 and M_2 physically exist, they virtually vanish. M_1 and M_2 have no network identities but are repeaters in; i.e., none of the good nodes in the network is able to aware of the existence of M_1 and M_2.

This is the major reason why wormhole attacks are difficult to deal with. As it is not able to easily find out wormhole nodes in a network, a specific mechanism to prevent and detect wormhole attacks is necessary.

Chapter 3 Related Work

In this chapter, several research works related to wormhole attacks will be introduced. These research works address the detecting mechanisms and prevention methods of Wormhole Attack in mobile Ad-Hoc networks. For these methods defend against wormhole attack, it can be classified into distance or time limiting detection approaches, false geometry or topology detection approaches, and neighbor nodes monitoring approaches. We will discuss the theoretic these three types of detecting approaches below. Moreover, we analyze and compare of these methods.

3.1 Wormhole Attacks Prevention

Dahill[8],Papadimitratos[9] and Hu[6] have separately introduced detail about Wormhole attacks in wireless networks. Initial proposals to avoid wormhole attacks propose using secure methods of bits over the wireless channel that can be recognize only by authorized nodes. This only defends against outside of network attackers who do not own cryptographic keys. Recently, researches are devoted to the study of prevention of inside attackers, it cannot be cannot be prevented by cryptographic mechanisms alone

3.1.1 Distance or Time Limiting Detection Approaches

The concept behind this approaches are intuitive, it restricts the distance or the period that packets can traverse between nodes in network. When node in network receives packets, it will check the transmission range of nodes or the transmission time. If a packet traverses more than a default value, this packet is perhaps being affected by malicious attacks or goes through the wormhole tunnel. Hu, L. and Evans et al [6] proposed a general mechanism related to this concept called “Packet Leashes”. It add the information to the packets, this information is designed to restrict the packet’s maximum allowed transmission distance, we called the packets are “Packet Leashes”. Two types of packet leashes were presented: Geographic Leashes and Temporal Leashes. The first leashes, each node has to know its precise location and all nodes have to know another node’s location information. Before sending a packet, each node adds the information of its current location and time in the packet. When the receive node receives the packet, it checks the packet by computing the distance to the sending node or the transmission time of the traverse path. The receiving node can use this computing result to decide whether the packet was transmitted through wormhole nodes. In Temporal Leashes, all nodes require very tight time synchronization. Before sending a packet, each node attaches its current time to the packet. When receiving the packet, the receiving node compares the temporal leash of the packet to its time, and computes the distance to the sending node by assuming the propagation speed is equal to the light speed. As a result, it can determine if the packet traveled an overlong distance caused by wormhole attacks. The drawbacks of Packet Leashes are that all nodes in network need accurate time and close time synchronism; and Geographic Leashes require extra hardware such as GPS or location service to let each node obtain its precise location.

This method is the earliest proposed method to defend against wormhole attack. The idea of this mechanism is very simple and ordinary. However, this method requires time synchronization or accurate location information on each node to calculate the distance between nodes.

3.1.2 Topology detection Approaches

These methods use geometric or topology information to detect wormhole attacks. If the analyzed results of the collected information violate the predefine situation, wormhole attacks may occur in the network. These methods do not require time synchronization, but need more complicated processes and message exchanges to observe and collect the information of packets. Lazos et al. [5] proposed a topology detection approach using cryptographic mechanism called local broadcast keys (LBK). It based on keys only known within each real neighbor nodes to prevent wormhole attacks. LBK does not need any time synchronization, but require a few additional network nodes, the guard nodes, which know their location and own broader transmission range than the regular nodes. While establishing LBKs, all guard nodes broadcast their fractional keys and location information to the network; and then regular nodes collect every fractional key they received. If two regular nodes share more than a threshold number of fractional keys, they use these keys to generate a pair-wise key. Finally, every node generates an LBK and unicast it to the nodes which it shares with same pair-wise key. After establishing the LBKs, each node can only communicate with their real nodes. In addition, Lazos et al. also provide a simple mechanism, called closet guard algorithm (CGA), which adopts the observation that a regular node should not receive fractional keys from guard nodes that are at a distance of more than two times of the transmission range of guard nodes, to distinguish which guards are infected by wormhole attacks.

3.1.3 Graph Theoretic and Geometric Approaches

In Geometric approaches, the nodes have to send their neighbor list to their neighbors. The neighbors are guards to each other and monitor the transmission of their neighbors. Like[26], LITEWWORP is geometric method proposed by Khalil et al. In the LITEWORP, each node can be server as a guard node, they define a malicious counter. When some unreasonable actions of node are detected, the malicious counter increases. Once the malicious counter on a particular neighbor is higher than a threshold, the neighbor revoke the node from its neighbor list and trigger an isolation algorithm to isolate the node which is thought as malicious. In their analysis, if the coverage of neighbors is not wide enough or too many/less neighbors aggregate in a region, the performances both go down. The neighbors of a node have to be kept in about 9~25 nodes, the system may work well above 90% detection rate. However, the false alarm rates of LITEWORK are between 10% and 28% when the neighbors number is about 17~29. As the result, we think only when the neighbors of a node around 9 to 17, the scheme do work. And hence the nodes in LITEWORP have to monitor the communication s of all neighbors, the energy consumption also be a problem.

3.1.4 Other Mechanisms and Protocols

Some Wormhole Attacks detection methods use the extra hardware or physical property to detect attacks. In [6], Hu and Evans utilize directional antennas to prevent wormhole links. Unlike our method, every node of the network is equipped with directional antennas and all antennas should have the same orientation. Different directions called zones are sequentially numbered and every node includes the transmitting zone at each message. A receiver hearing information at a zone A verifies that the sender transmitted the message at the correct zone B, where A, B are opposite zones. Based on information provided by neighbors that assist the wormhole detection by acting as verifiers, every node discovers its neighbors. As pointed out by the authors of [6], a valid verifier must exist in order for the wormhole to be detected, since not all neighbors can act as verifiers. Finally, as noted by the authors of [6], this method can only prevent single wormholes and does not secure the network against multiple wormhole links [6].

3.2 Comparison of Main Mechanisms

We will discuss the main difference and conceptions of the mechanism mentioned above. Look at Table 1, here we list the main ideas of the mechanisms, the original routing protocols they based on or the improved, and their special assumptions, hardware or special nodes needed in the mechanisms. Finally, we compare their computational and control overheads.

First, Distance or Time Limiting Detection Approaches use the packets transmission distance to judge a node. This way can detect the Wormhole attacks effectively due to transmission distance cannot forge except that malicious nodes have capacity of moving the node's location rapidly. However, this solution needs accurate location information or precise clock synchronization. And this way assumes the nodes are not movable, this drawback greatly decreases the practicality. In topology detection approaches, all transmissions between node pairs have to be encrypted by local broadcast key of the sending end and decrypted at the receiving end. As a result the time delay in each node is extended a lot. Finally, the Statistical analysis methods use a central authority (CA) or coordinate node to monitor the Ad-hoc networks. If the central node can collect and analysis the network information, it will aware the behavior of Wormhole attacks as soon. But, practically, most ad-hoc network routing protocols are tend to non-central authority. So, this statistical solution requires particular routing protocols or specific hardware to implement.

Protocol	**Description**	**Drawback**
Hu and al. 2003	Use of packet leaches With geographical and temporal information	requires synchronized clocks and GPS equipped devices
L. Hu and al. 2004	Use the direction of the antenna Of the neighbors	use of directional antenna
R. Maheshwari and al. 2007	Search for forbidden structure caused by the wormhole	Difficulty to compute a parameter to determine forbidden structure

Table 1 Comparison of Main Mechanisms

Chapter 4 The Proposed Protocol: AR-AODV Routing Protocol

AR-AODV protocol presents Auto Resilient AODV routing protocol. In this Chapter, we introduced the AR-AODV protocol include design conception and the future. In Section 4.1, we first describe our observation about the Wormhole Attacks using AODV routing protocol; and later we proposed our design protocol against Wormhole Attacks. Also, we described particularity how to implement our AR-AODV routing Protocol in final.

4.1 Observation of Wormhole Attacks on AODV

We proposed a routing protocol for preventing the Wormhole Attack on Ad-hoc Network, called AR-AODV (Auto resilient Ad hoc On-Demand Distance Vector Routing). This Protocol is based on AODV (Ad hoc On-Demand Distance Vector Routing) protocol. The original AODV routing protocol cannot prevent from wormhole attack. Our Protocol, AR-AODV, uses the node hop numbers difference to detect the Wormhole Attack.

At first, we explain how Wormhole Attack take place on AODV routing protocol, and discuss our observation about the characteristic of the network it was be infected by Wormhole Attack.

a. How Wormhole Attack take place on AODV

The major mission for malicious node intended to execute Wormhole Attack is how to get many chances to achieve the maximum packages on network. As soon as malicious node can obtain more and more packages, the Wormhole attack’s destruction will be more serious. On Ad-hoc network, routing cost is an important concern. So if any router can decrease the routing cost, it will get many chances to achieve the packages. For this reason, Wormhole attacks will try all the means to decrease the routing cost. Next, we will introduce how Wormhole attacks decrease the routing cost on AODV.

<table>
<tr><td>Type</td><td>D</td><td>G</td><td>Reserved</td><td>Hop count</td></tr>
<tr><td colspan="5">Broadcast ID</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Destination sequence number</td></tr>
<tr><td colspan="5">Originator IP address</td></tr>
<tr><td colspan="5">Originator sequence number</td></tr>
</table>

Protocol such as AODV discover and decide routing path by comparing the *hop counts* in the **RREQ** package. Hop Count is the number of hops from the Originator IP Address to the node handling the request. A typical Wormhole attack occurred on AODV is possible by modification of the hop count field in route discovery messages RREQ. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, malicious nodes can increase the chances they are included on a newly created route by resetting the hop count field of the RREQ to zero.

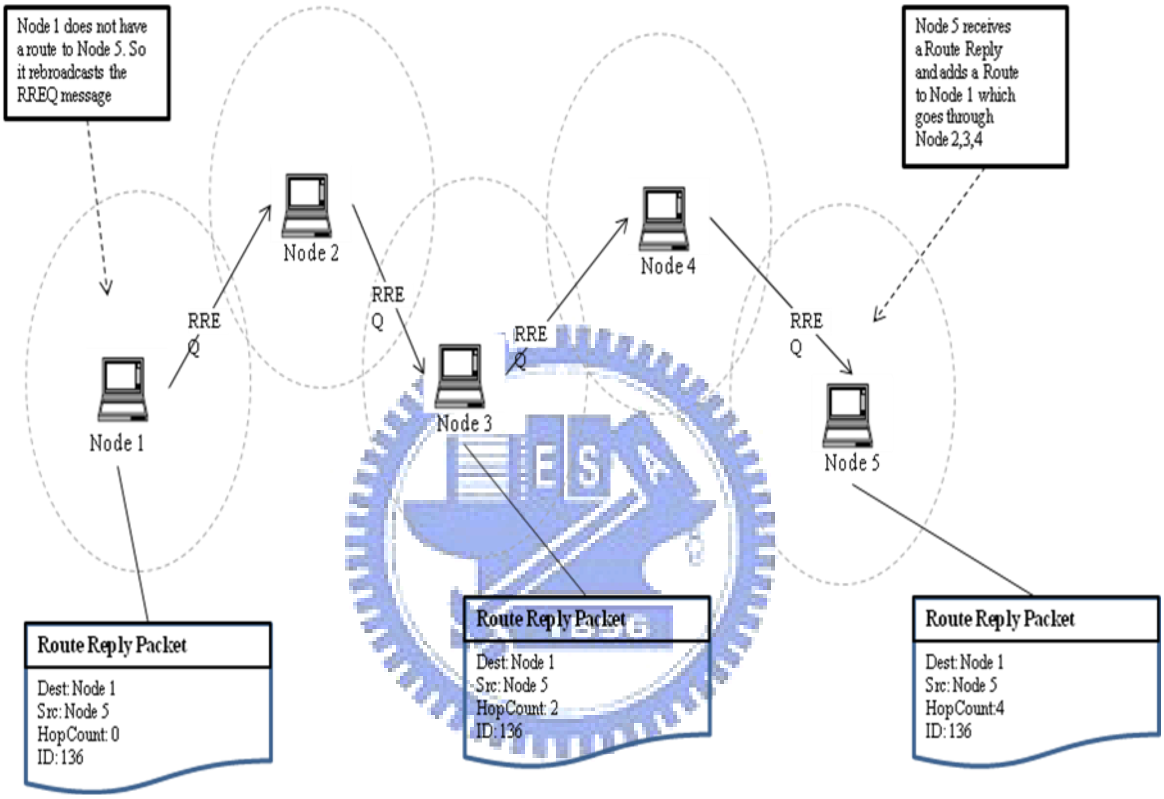


Figure 4-1 Routing request

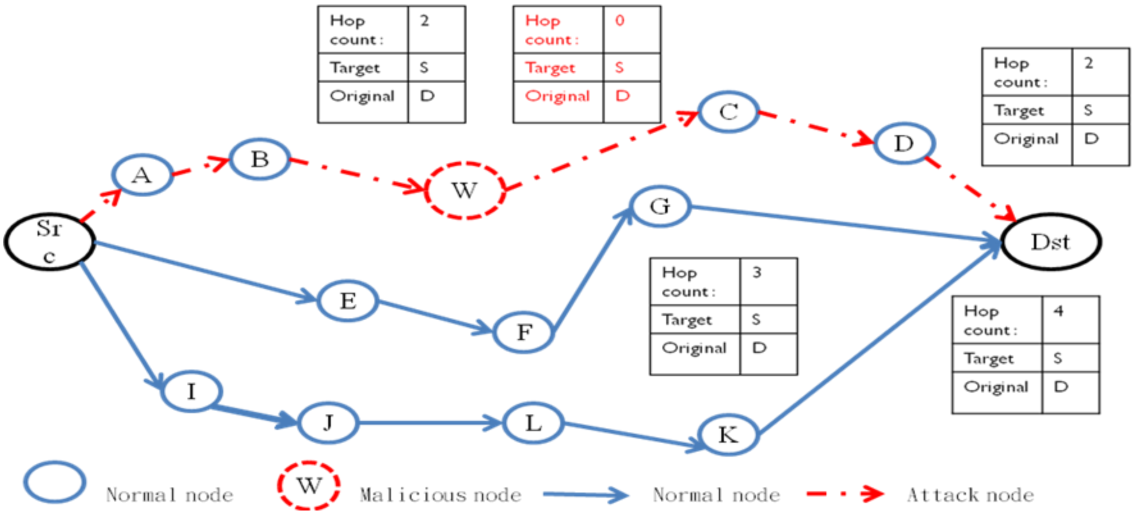


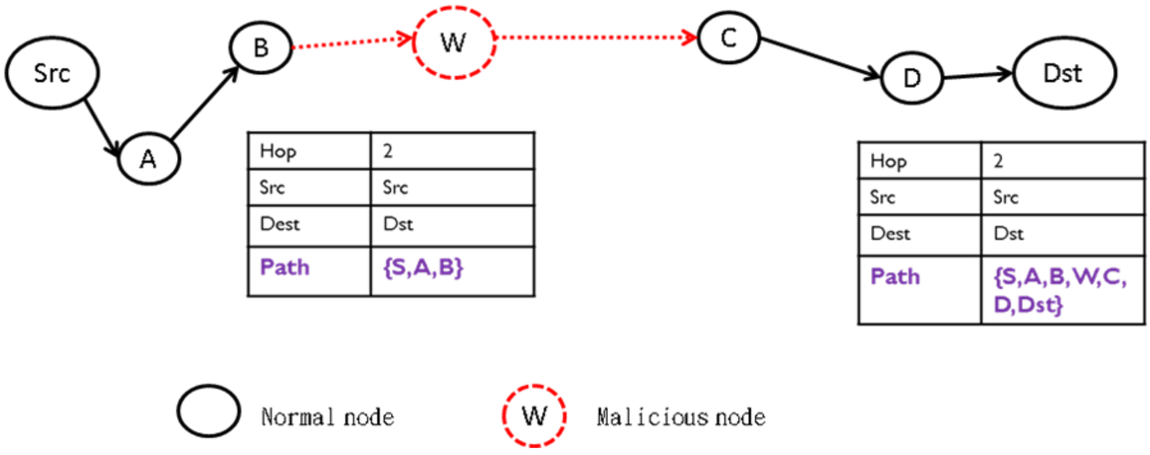
Figure 4-2 wormhole attack on AODV

b. our observation about the characteristic of Wormhole attack

Based on the above described, we observation the changes in packets. There is a difference about the hop count between before packets through the wormhole node and after packets through the wormhole node. According to the clues, we monitor the hop count of packets immediately. Therefore, when one hop counts of RREQ with the dramatic changes, we can take appropriate measures to prevent attack in time. However, it is not enough to guard against such wormhole attacks. The measure of monitoring hop count can only determine whether the wormhole attacks exist. This method cannot be found to the specific locations of wormhole node. Our goal is not only discover attacks but also auto resilient the network barriers, so we must do more to meet our requirements. Reviewing the packets message of AODV, we think there are not enough clues to identify specific wormhole node. For this reason, we have added one column to the RREQ packet. This column is recorded the path history from source node to destination node. After adding this path column to track the path and collecting the monitor of hop counts, we can determine whether Wormhole Attacks has occurred, and more importantly, this method can identify the wormhole node specifically.

4.2 The Proposed Protocol: AR-AODV

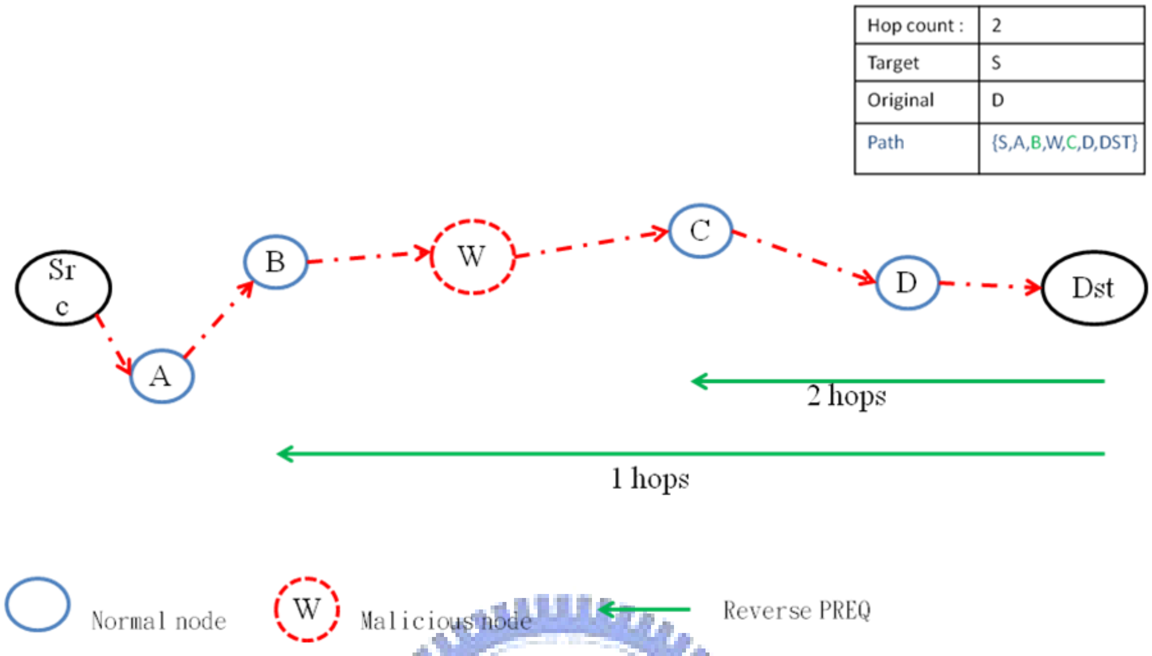
In this section, we will bring up our ideas to solve the security problem as mentioned above. In our proposed protocols, we can detect the malicious node altering the RREQ's hop counts.



Hop	2
Src	Src
Dest	Dst
Path	{S,A,B}

Hop	2
Src	Src
Dest	Dst
Path	{S,A,B,W,C,D,Dst}

Figure 4-3 Path Record



Hop count :	2
Target	S
Original	D
Path	{S,A,B,W,C,D,DST}

Figure 4-4 Reverse RREQ

4.2.1 Design Conception

First, our AR-AODV protocol will add one column into the RREQ package. The original RREQ packages on AODV protocol do not contain the any information about the routing path history. The fewer packet size perhaps can increase routing efficiency and speed up the duration of data transmission. However, we find if the packages do not contain the routing information, it will become a huge security loophole on Ad-hoc network. For this reason, we slightly modify the Route Request (RREQ) Message, like the (Table 2 Traceable RREQ).

Type	D	G	Reserved	Hop count
Broadcast ID				
Destination IP address				
Destination sequence number				
Originator IP address				
Originator sequence number				
Routing history				

Table 2 Traceable RREQ

Second, our AR-AODC protocol will add a new routing packet type: Reverse RREQ. Comparing with the RREQ packets sent from source node, Reverse RREQ packets are sent from destination node, and traced back along the RREQ's path to find the malicious node. Reverse RREQ are like RREQ, when destination nodes send reverse RREQ package, the node should assign a goal. After assigning the goal, Reverse RREQ package will go along the old path to count the routing cost. And we find, we can detect malicious node if we send continuously two reverse RREQ packets that target nodes are different and malicious node is between two target nodes.(Figure 4-5 Illustration of route establishment)

4.2.2 Route Establishment

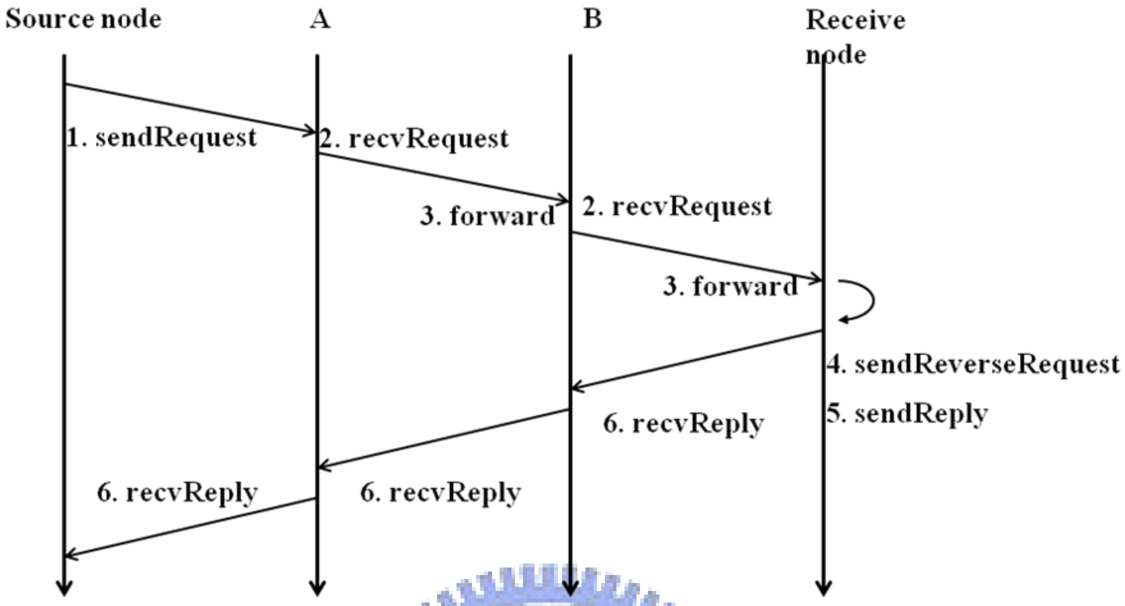


Figure 4-5 Illustration of route establishment

1. Send Request

When one node needs to send a message to another node that is not its Neighbor it broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message and a Sequence Number which serves as a unique ID.

2. Receive request

When Node 1's Neighbors receive the RREQ message they have two choices; if they know a route to the destination or if they are the destination they can send a Route Reply (RREP) message back to Node 1, otherwise they will rebroadcast (forward) the RREQ to their set of

Neighbors. The message keeps getting rebroadcast until its lifespan is up.

3. Forward

When one node receives a RREQ message and it does not know how to route to the destination, it will forward this RREQ message to neighbors.

4. Send Reverse Request

When destination node receive the RREQ message, it should check the RREQ whether the routing path contain Wormhole nodes.

5. Send Reply

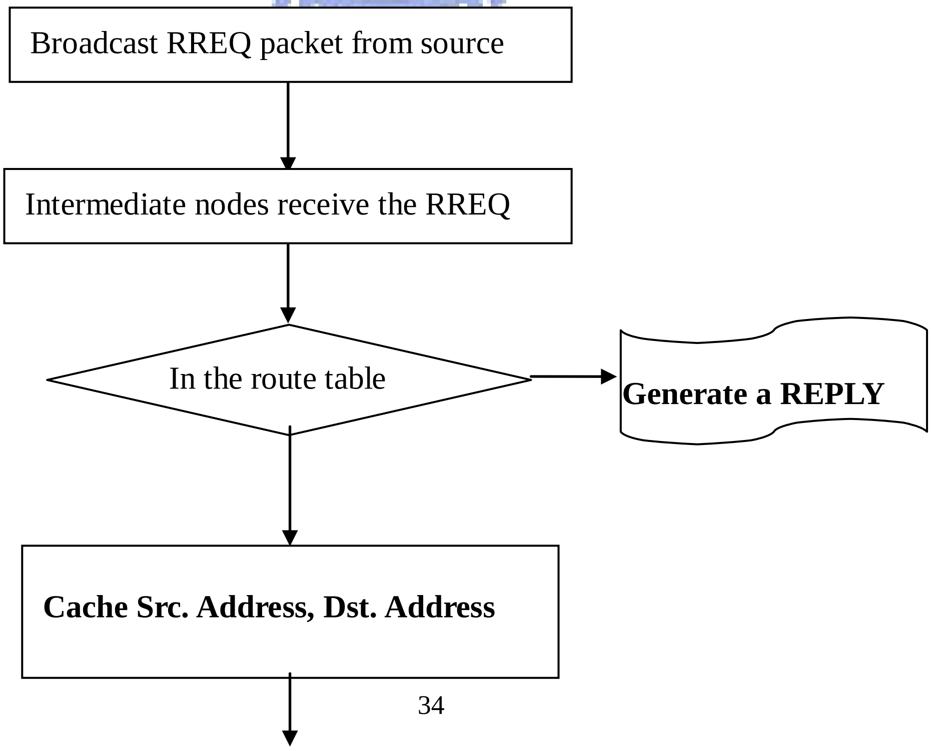
If setp.4 has checked and the routing path does not contain wormhole nodes, then destination node will send out a RREP message to source node from the request routing path.

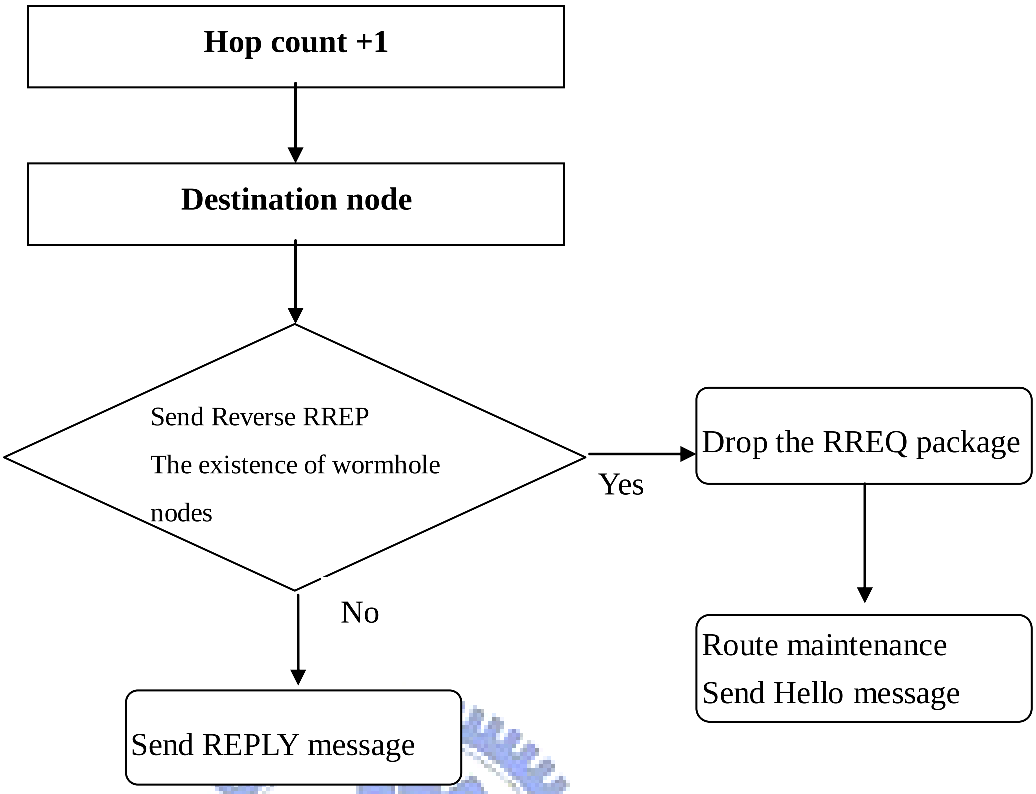
6. Receive Reply

When source node receives the RREP message, in our methods, it means that the path is safe.

4.2.3 Route Maintenance

When wormhole nodes have been detected, the next most important thing is how to disable the wormhole nodes. Actually, it is not as simple as wired network which can easily find the physical location of any nodes or just disable the attack node from the router. In Wireless Ad-Hoc network, node can easily change its location and we cannot disable one node from a specific router because each node is a router include attack node. Since we cannot disable one node in Ad-Hoc network directly, we adopt an indirect approach to achieve the purpose of the prohibition of attack node. Reviewing the AODV routing protocol, it define a HELLO message to maintain the network. We used this HELLO message to disable the Wormhole attack node. HELLO message can be communicate with directly are considered to be neighbors. In our methods, we add one column to record the list of wormhole attack nodes. When nodes in the network receive the HELLO message, it will check the list of wormhole attack nodes and add the list to the routing table. Our mechanism is when a node receives RREQ from neighbors, it should query the routing table to judge whether the neighbor can be trusted. If the neighbor's id is in the list of wormhole attack nodes, the AR-AODV will automatically add a weighted value to the hop count number of RREQ message. The effect of doing so is to reduce the chance of the routing path include wormhole node be selected.


Broadcast RREQ packet from source
Intermediate nodes receive the RREQ
In the route table
Generate a REPLY
Cache Src. Address, Dst. Address


Hop count +1
Destination node
Send Reverse RREP
The existence of wormhole
nodes
Yes
Drop the RREQ package
No
Route maintenance
Send Hello message
Send REPLY message

Chapter 5 Simulation and Results

In this Chapter, we will evaluation our AR-AODV protocol through simulations. The first section will explain out simulation environment, include the simulation tool ns-2[7]. The second section, we will show three scenarios of simulations to evaluation the AR-AODV including its performance, the rate of detecting Wormhole Attacks. Finally we will show the simulation results.

5.1 Simulation Environment

In our simulation, we use the NS-2 as the simulation tool. NS -2 is a discrete event simulator targeted at networking research. Ns-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. Also, we chose NAM as our network animation tool. Nam is a TCL / TK based animation tool for viewing network simulation traces and real world packet traces. It is mainly intended as a companion animator to the ns simulator.

The simulator automatically deploys nodes with assigned amount in random and the transmission range of simulator are a fixed value of 0.25m. In order to simulate the more realistic situation, we evaluate two types of Ad-hoc network model. One is smaller network used usually in room or classroom; the other one is larger network used in indoor buildings. The smaller network we define the length and width of 10 meters with 50 nodes; the larger network model we define the length and width are 50 meters with 1000 nodes.

CPU	**Intel(R) Core(TM2) Duo CPU T7250 2.00.GH**
Memory	**4 GB**
OS	**Microsoft Windows XP**
NIC	**Inter(R) PRO/1000 Ethernet**
Hard Disk	**SCSI 250G**

Table 3 Experimental environment

Simulation parameter	value
Radio-propagation model	Propagation/TwoRayGround
MAC type	802.11
Routing protocol	AODV/AR-AODV
Time of simulation end	300.0s
Antenna model	OmniAntenna

Table 4 Simulation parameter

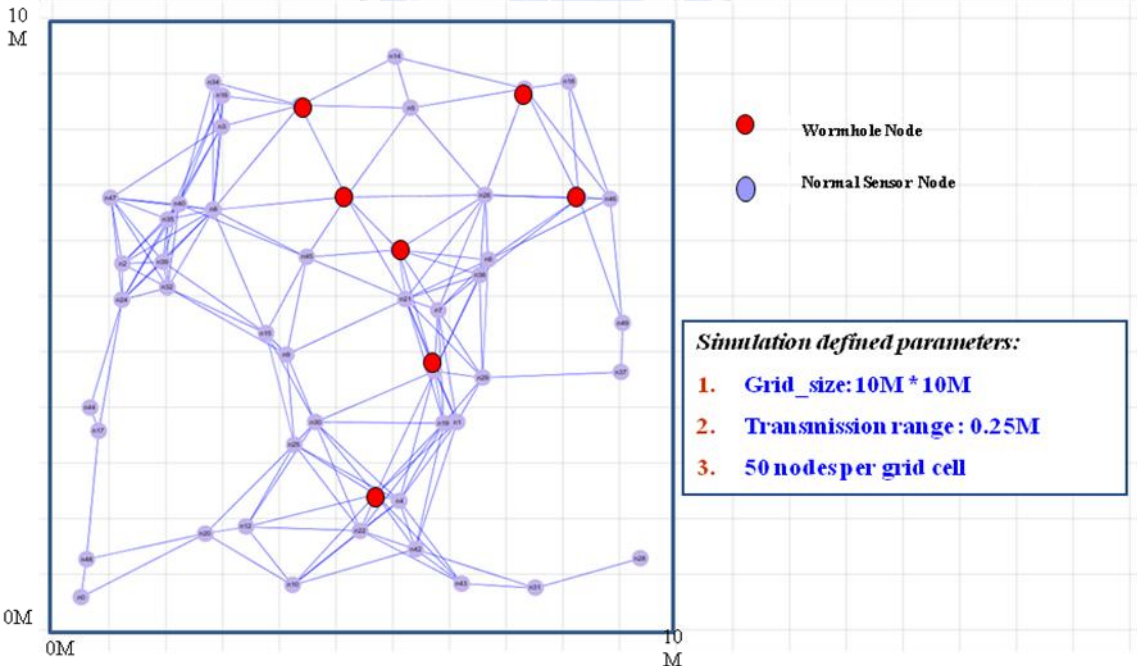

10
M
0M
0M
10
M
Wormhole Node
Normal Sensor Node
Simulation defined parameters:
1. Grid_size: 10M * 10M
2. Transmission range : 0.25M
3. 50 nodes per grid cell

Figure 5-1 simple grid (10M*10M, 50 nodes)

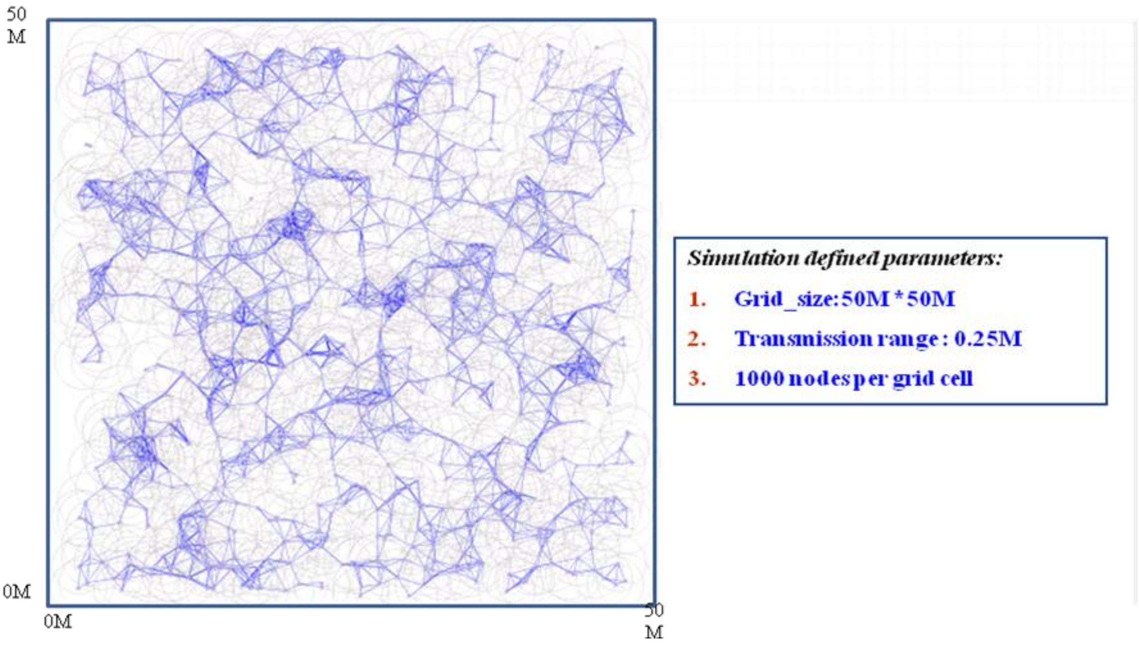

50 M
0M
0M
50 M
Simulation defined parameters:
1. Grid_size:50M*50M
2. Transmission range: 0.25M
3. 1000 nodes per grid cell

Figure 5-2 large grid (50M*50M, 1000 nodes)

5.2 Simulation and Results

In this section, we show the simulation results of AR-AODV protocol and the analysis of simulation outcome. In our simulation scenarios, we focus on two parts: detection rate and overhead. We will use charts to show it.

5.2.1 The impact of wormhole attack

The main purpose of this experiment is to measure the detection rate of routing protocols. We define a measurement criterion: Wormhole attack impact rate. It means the probability of data packets through the wormhole attack node. The higher of this impact rate of routing protocol, the more dangerous about this network. In our experiment, we measure this value in three cases. The first case that T is 0 means the original AODV routing protocol. This case will have a high impact rate due to AODV routing protocol does not have defense mechanism to wormhole attack. In other two cases, they all use the AR-AODV routing protocol. But these two cases are not the same as the timing of the use of detecting methods. When T is”average path length”, it will check the RREQ packets just when hop count number less than average path length. However, when T is ”the longest path length”, it will check the RREQ packets all the time.

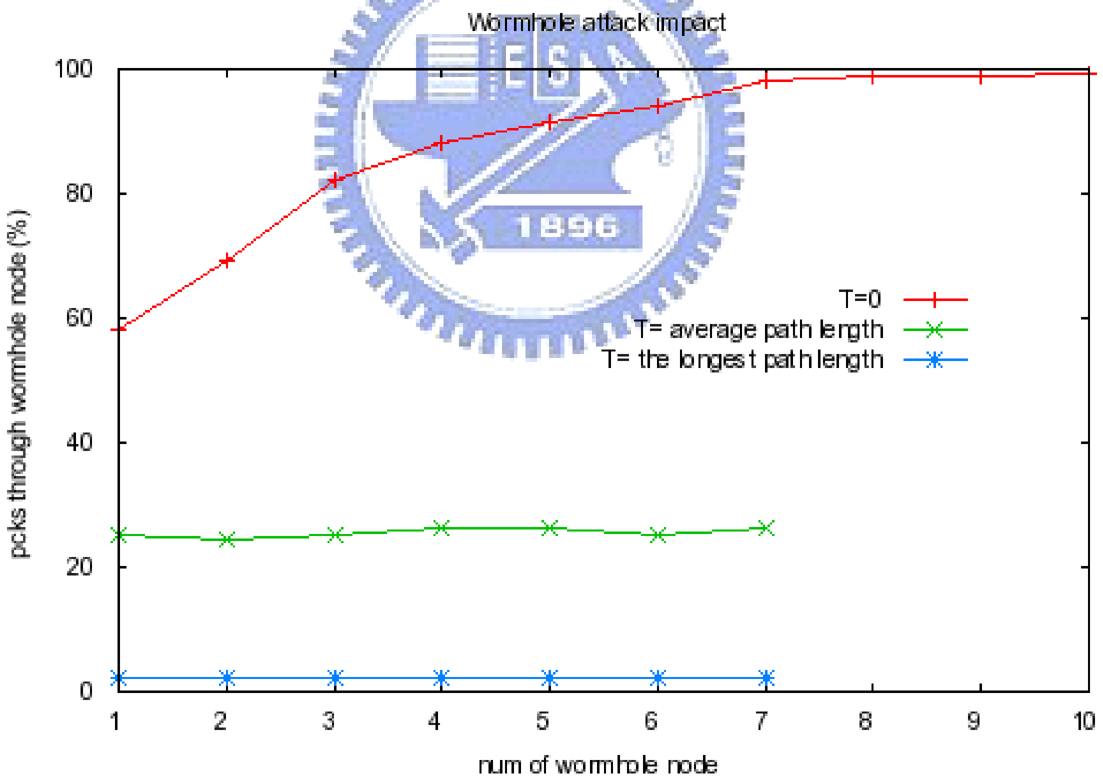


Figure 5-3 impact rate (simple grid)

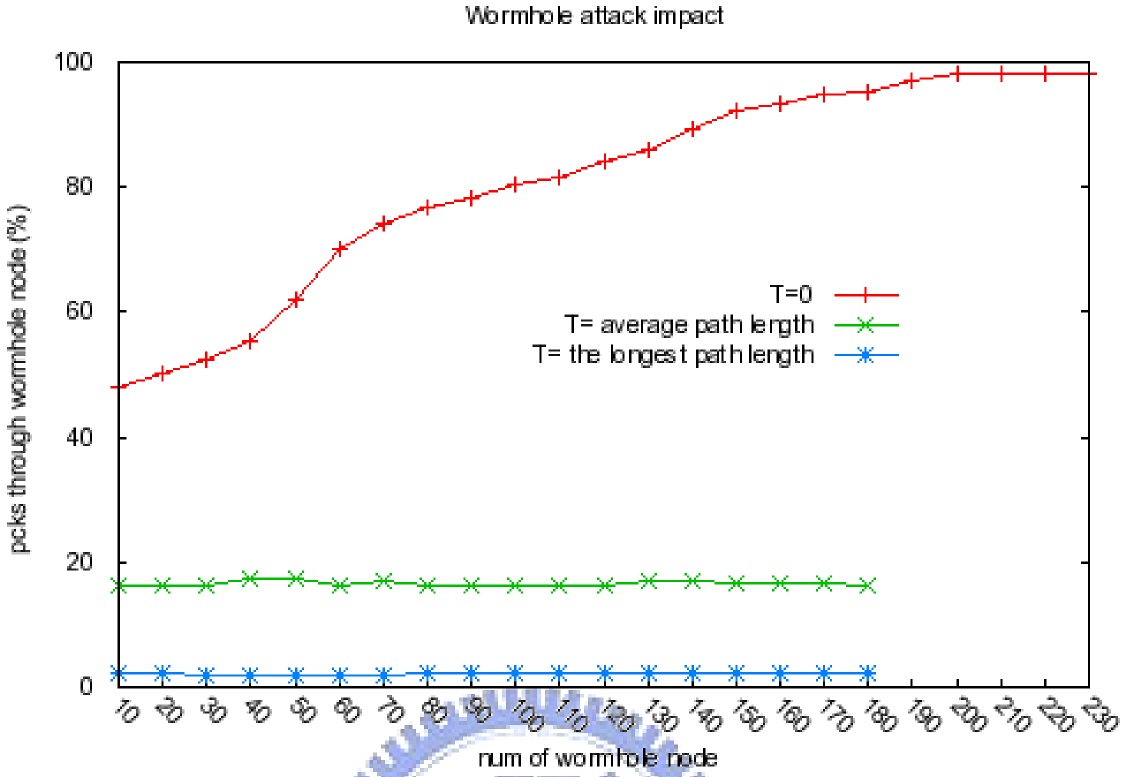


Figure 5-4 impact rate (large grid)

5.2.2 Overhead of AR-AODV

The main purpose of this experiment is to assess the overhead of AR-AODV. In 5.2.1 section, the simulation results show that AR-AODV can suppress the wormhole attacks. However, we evaluate a routing protocol also should consider the overhead of the methods. If the overhead of new approach are much heaver than original protocol, it is not a high-perfomance method.

In first part, we show the overhead about the latency of RREQ packets. The latency means the speed of finding a routing path form source node to destination node. If the value of latency is too large, then the efficacy of the entire network will be very low. From the simulation results, the original routing protocol AODV has the smallest delay. The latency of AR-AODV routing protocol are more than twice as high as AODV. However, the latency will gradually become smaller with the time. This is due to that AR-AODV should send Reverse RREQ packets at first time if the routing table has no cache data, but next time the AR-AODV can query the routing table data, it will reduce the delay time. The latency will reduce to just higher than the latency of AODV a little. Extra latency is because AR-AODV should do some routing maintaining actions.

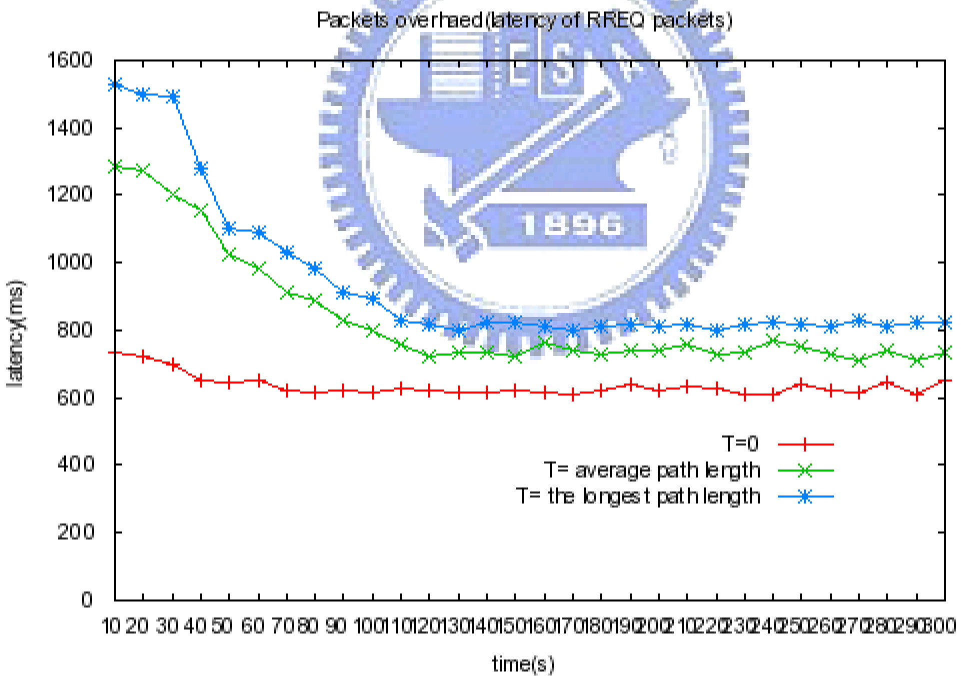


Figure 5-5 latency of RREQ packets (simple grid)

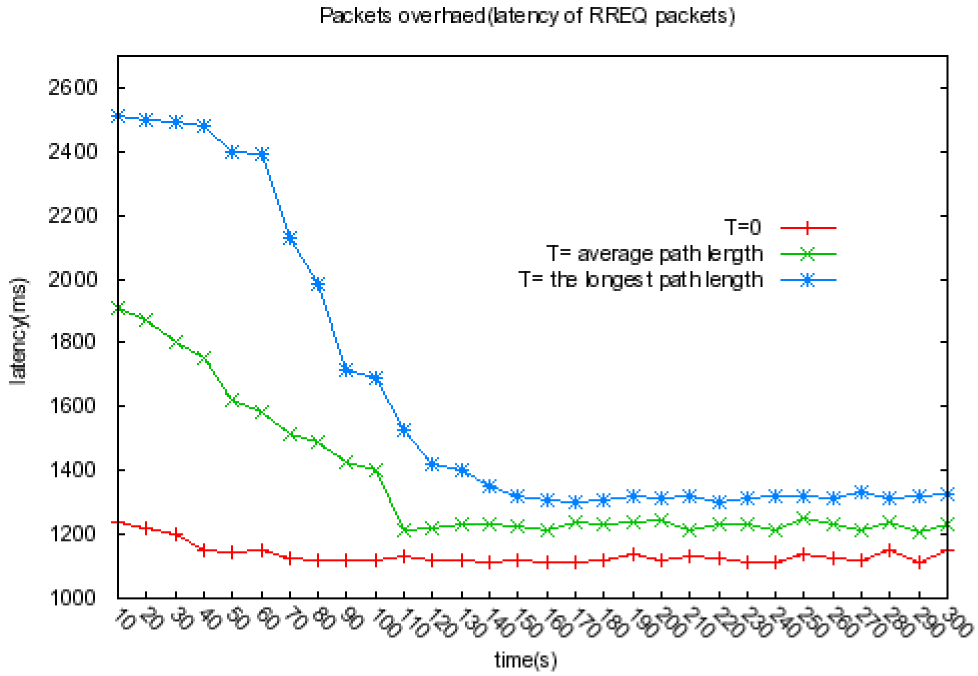


Figure 5-6 latency of RREQ packets (large grid)

In second part, we show the number of RREQ packets in network. When AODV routing protocol is in the initial stage, it should send the RREQ packets to discover network topology. Our AR-AODV routing protocol also uses the initial stage to detect the wormhole attack. The purpose of this experiment is to compare the overhead of number of RREQ packets. The lower number of RREQ packets will be able to mitigate the load of network. From the simulation results, the original routing protocol AODV has the smaller number of RREQ packets in the beginning, it is three times less than AR-AODV. However, the number of RREQ packets will reduce gradually after a period time. This is due to the RREQ packets did not really sent out to the network after the network initial stage. If the routing table has cached the routing data, the RREQ packets will never be sent out. Another reason about the our protocol has smallest number of packets at final is because some nodes have be disabled, it also will reduce the number of RREQ packets.

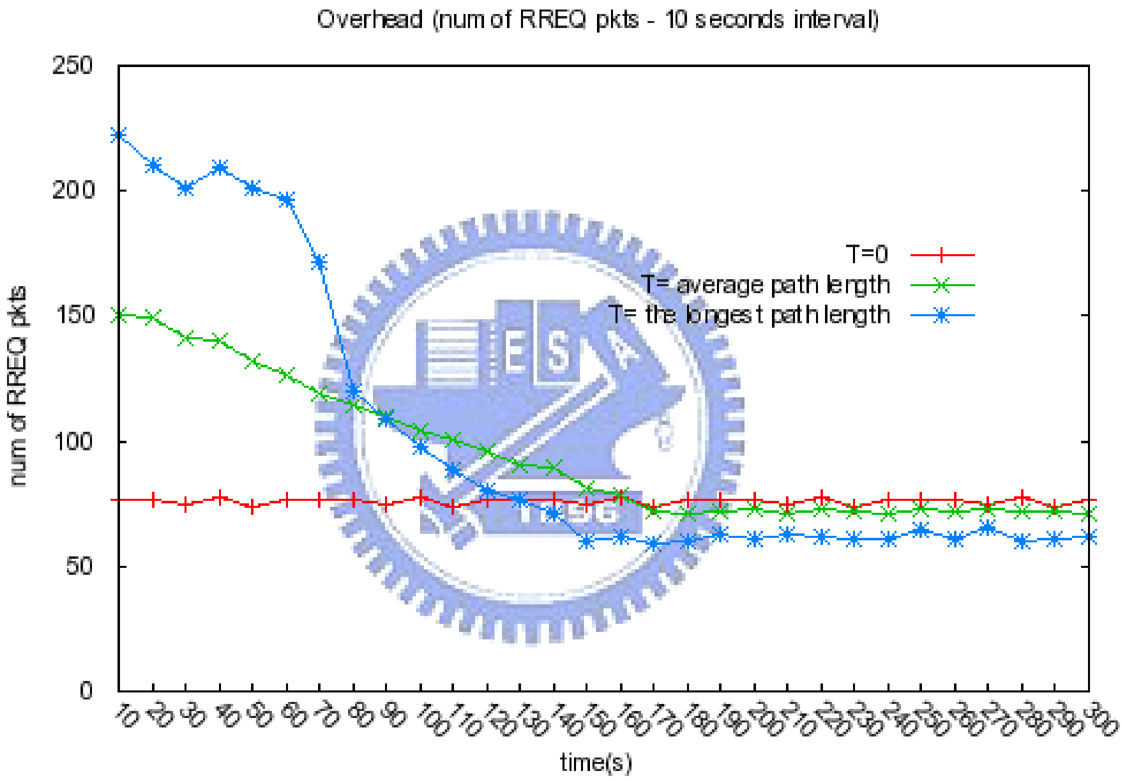


Figure 5-7 num of RREQ pkts (simple grid)

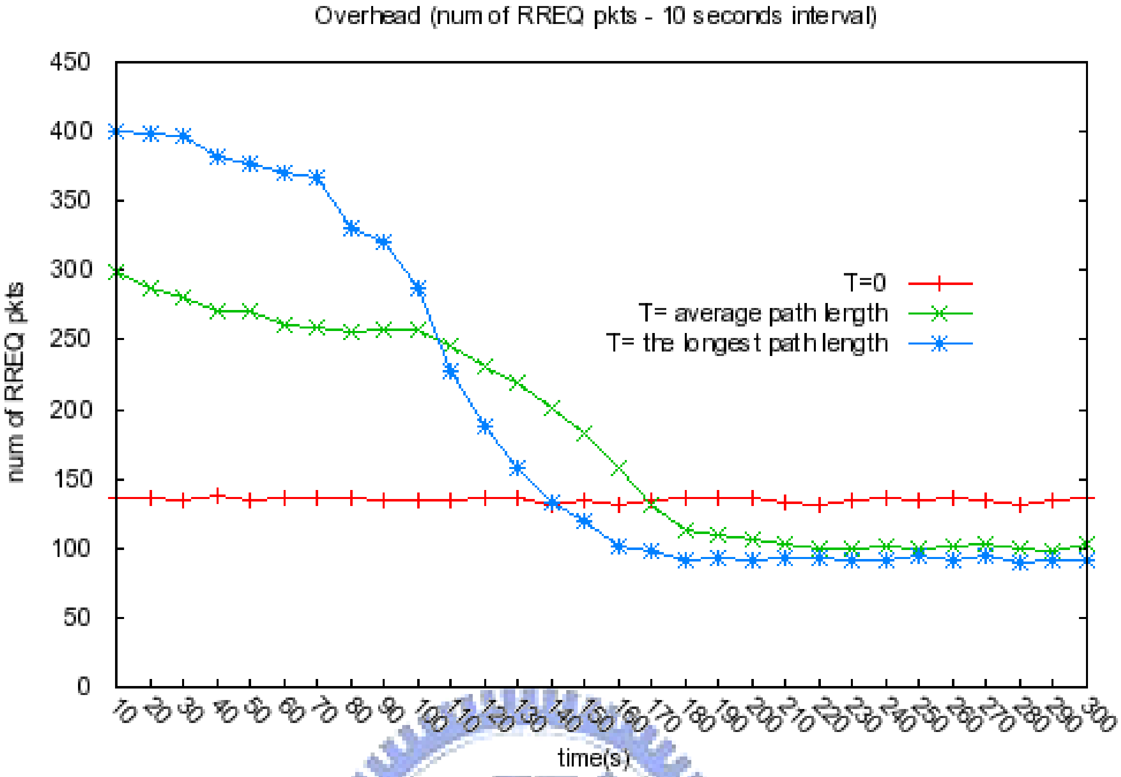


Figure 5-8 num of RREQ pkts (large grid)

Chapter 6 Conclusion and Future Work

6.1 Conclusions

In this thesis, we studied the effect of the wormhole attack in mobile Ad-Hoc networks (MANETS) and analyze the security issues of MANETs. We proposed a new on-demand routing protocol, Auto-Resilient **A**d hoc **O**n-Demand **D**istance **V**ector Routing (AR-AODV), to against wormhole attacks on mobile Ad-Hoc networks (MANETs) and recover the network. AR-AODV utilizes Reverse RREQ packets to detect wormhole attacks and disable the wormhole node using Hello packets. The original AODV routing protocol has no mechanisms to against wormhole attack, the malicious can tamper the hop number of RREQ to cause huge amounts of packets gathering into wormhole node. In our proposed method, it can effectively prevent the wormhole attack on MANETs. Also, the Hello messages can auto disable the wormhole node, we call this is "Auto-resilient". Indeed, the simulation results showed that wormhole nodes are disappeared gradually.

6.2 Future Work

Our proposed routing protocol is mainly used in AODV routing protocol. However, we think the most of Ad hoc routing protocols have some similar characteristics including the step of finding the routing path and routing maintain. In the future, our method can be ported to other routing protocols like: DSDV (Destination-Sequenced Distance-Vector Routing), this routing protocol used Bellman–Ford algorithm to find the routing path; DSR (Dynamic Source Routing), this routing protocol also has the Routing Request packets, so we can port our method easily to DSR.

Reference

[1] (AODV) Routing,” IETF MANET Working Group, Internet Draft 2003. Computer, vol. 35, no.10, pp. 54-62, 2002.

[2] Lionel M. Ni , Philip K. McKinley, A Survey of Wormhole Routing Techniques in Direct Networks, Computer, February 1993 , v.26 n.2, p.62-76

[3] Y. Hu, A. Perrig, D. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: IEEE Annual Conference on Computer Communications (INFOCOM), 2003, pp. 1976–1986.

[4] W. Wang, B. Bhargava, Visualization of wormholes in sensor networks, in: Proceedings of the ACM workshop on Wireless security (Wise’04), 2004, pp. 51–60.

[5] L. Lazos, R. Poovendran, C. Meadows, P. Syverson and L.W. Chang, Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach, IEEE Wireless Communications and Networking Conference (WCNC05) 2 (13–17) (2005), pp. 1193–1199

[6] Hu, L. and Evans, D. 2003b. Using directional antennas to prevent wormhole attacks. In Proceedings of the 11th Network and Distributed System Security Symposium. 131--141.

[7] Ns-2 [Online]. Available: http://www.isi.deu/nanam/ns/ .

[8] B. Dahill, B. N. Levine, E. Royer, and C. Shields, “A secure routing protocol for ad-hoc networks,” Electrical Engineering and Computer Science, University of Michigan,Tech. Rep. UM-CS-2001-037, August 2001.

[9] P. Papadimitratos and Z. Haas, “Secure routing for mobile ad hoc networks,” in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[10] Y. C. Hu, A. Perrig, and D.B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

[11] Radha Poovendran , Loukas Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks, Wireless Networks, v.13 n.1, p.27-59, January 2007 [doi>10.1007/s11276-006-3723-x]

[12] Khalil, I., Bagchi, S., and Shroff, N. B. 2006. MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks. In IEEE International Conference on Security and Privacy in Communication Networks.

[13] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. 2002.

[14] Elizabeth M. Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. Technical report, University of California and Georgia

Institute of Technology, USA, 1999.

[15] C. Santivanez and R. Ramanathan, Hazy Sighted Link State (HSLS) Routing: A Scalable Link State Algorithm Cambridge, MA: BBN Technologies, Aug. 2001, BBN Tech. Memo BBN-TM-1301.

[16] Zygmunt J. Haas , Marc R. Pearlman, ZRP: a hybrid framework for routing in Ad Hoc networks, Ad hoc networking, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 2001.