석 사 학 위 논 문

Master's Thesis

다중 라디오 다중 채널 무선 메쉬 네트워크에서의 안전한 채널 할당을 위한 인증 기법에 관한 연구

A Study on authentication scheme for channel assignment mechanism in multi-radio multi-channel wireless mesh networks

신 승 목 (申 昇 沐 Shin, Sung-Mok)

정보통신공학과

Department of Information and Communications Engineering

한 국 과 학 기 술 원

Korea Advanced Institute of Science and Technology

2010

다중 라디오 다중 채널 무선 메쉬 네트워크에서의 안전한 채널 할당을 위한 인증 기법에 관한 연구

A Study on authentication scheme for channel assignment mechanism in multi-radio multi-channel wireless mesh networks

A Study on authentication scheme for channel assignment mechanism in multi-radio multi-channel wireless mesh networks

Advisor : Professor Kim, Kwang Jo

by

Shin, Sung-Mok
Department of Information and Communications Engineering
Korea Advanced Institute of Science and Technology

A thesis submitted to the faculty of the Korea Advanced Institute of Science and Technology in partial fulfillment of the requirements for the degree of Master of Engineering in the Department of Information and Communications Engineering

Daejeon, Korea
2009. 12. 18.
Approved by

Professor Kim, Kwang Jo
Advisor

다중 라디오 다중 채널 무선 메쉬 네트워크에서의 안전한 채널 할당을 위한 인증 기법에 관한 연구

신 승 목

위 논문은 한국과학기술원 석사학위논문으로 학위논문심사 위원회에서 심사 통과하였음.

2009년 12월 18일

심사위원장 김 광 조 (인)

심사위원 김 명 철 (인)

심사위원 이 병 천 (인)

MICE
20084236

신 승 목. Shin, Sung-Mok. A Study on authentication scheme for channel assignment mechanism in multi-radio multi-channel wireless mesh networks. 다중 라디오 다중 채널 무선 메쉬 네트워크에서의 안전한 채널 할당을 위한 인증 기법에 관한 연구. Department of Information and Communications Engineering . 2010. 29p. Advisor Prof. Kim, Kwang Jo. Text in English.

Abstract

Hyancinth is one of the popular node architectures proposed by *Ashish et al.* for efficient channel assignment in multi-radio multi-channel(MRMC) wireless mesh network(WMN). However, we found out that *Hyacinth* was designed without considering the security mechanism. A fake channel control packet from an external attacker can degrade the network goodput. Also, an internal attacker *e.g.,* compromised node, can launch denial of service(DoS) attacks by two methods: malicious channel switching(MCS), and consecutive channel switching(CCS) attack. In this thesis, we propose an authenticated channel assignment mechanism for MRMC WMN, and provide secure channel control, and message verification module to prevent the known attacks. First, we provide *secure channel control* to protect the channel assignment process from an external attacker. We use cryptographic primitive *e.g.,* a block cipher to encrypt the channel control message. Second, we add additional module called, Message verification module, which consists of three phase, *Channel status gathering*, *Discrepancy checking* and *Message verification*. In *channel status gathering*, one node collects the channel status of other nodes within the interference range, and selects the candidate preferred channel. In *discrepancy checking* phase, each node within the interference range checks the discrepancy of current channel and interface from the requested channel and interface. In *message verification* phase, each node compares the number of the requested channel from the PARENT node with his candidate preferred channel to verify whether the change request is legitimate or not. Our simulation result using NS-2 simulator shows that proposed scheme can protect channel assignment process from both external and internal attacker in the presence of the attacker that launches MCS and CCS attacks together.

Contents

List of Tables

List of Figures

1. Introduction

A wireless *ad hoc* network is a decentralized wireless network[20]. The network is *ad hoc* because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. The earliest wireless *ad hoc* networks were the "packet radio" network (PRNET) from the 1970s, sponsored by DARPA after the ALOHAnet project[7].

A wireless mesh network(WMN) can be seen as a special type of wireless ad-hoc network. It is often assumed that all nodes in the WMN are immobile but this need not be so. The mesh routers may be highly mobile. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, WMN differs from an ad-hoc network since all of these nodes are not always constrained by resources. Such networks may operate by themselves or may be connected to the larger Internet. Mesh networks may involve either fixed or mobile devices. The applications are diverse;for example in difficult environments such as emergency situations, tunnels and oil rigs to battlefield surveillance and high speed mobile video applications on board public transport or real time racing car telemetry. A significant application for wireless mesh networks is Voice over IP(VoIP). By using a quality of service scheme, the wireless mesh may support local telephone calls to be routed through the mesh.

Despite significant advances in physical layer technologies, the current wireless LAN still cannot offer the same level of sustained bandwidth as their wired connections. The advertised 54 Mbps bandwidth for IEEE 802.11a/g based hardware is the peak link-level data rate[11]. When all the overheads, media access control(MAC) contention, IEEE 802.11 headers, ACK and packet errors are accounted for, the actual goodput available to applications is almost halved. The bandwidth problem is further aggravated for multi-hop *ad hoc* networks because of interference from adjacent hops in the same path as well as from neighboring paths. Fortunately, the IEEE 802.11b/802.11g standards[1] and IEEE 802.11a standard[2] provide 3 and 12 non-overlapping frequency channels, respectively, that could be used simultaneously with a neighborhood. An ability to utilize multiple channels within the same network substantially increases the effective bandwidth available to wireless net-

work nodes. Such bandwidth aggregation is routinely used when an 802.11-based wireless LAN operates in infrastructure mode, where traffic to and from wireless nodes is distributed among multiple interfaces of an access point or among multiple access points to avoid congestion.

On the other hand, assigning channel to each interface is not a simple problem. Let us think about mesh topology of multiple nodes equipped with three Network Interface Cards (NICs). A sender and a receiver should use the same channel with the corresponding interface. Due to this characteristic, a channel dependency problem always happens during the channel assignment process[18]. To solve this problem, *Hyacinth* was proposed to manage safe and stable channel assignment[18].

However, *Hyacinth* suffers from security vulnerabilities by a malicious attacker. Attacker model is classified into two categories : external and internal attacker. External attacker does not have precise knowledge about the network *e.g.,* secret key. Internal attacker can impersonate to be compromised nodes who know the shared secret key among each node.

Based on the explained attacker type, three vulnerabilities exist in the channel assignment algorithm. First, external attacker can propagate false channel control message, interrupting the stable channel assignment. Second, malicious channel switching(MCS) attack will severely degrades the performance of WMN by modifying the normal channel of a node into the heavily loaded channel. Third, consecutive channel switching(CCS) attack rapidly broadcasts channel change message which leads to WMN into quasi-stable state.

In this thesis, we modified current *Hyacinth* architecture to solve the known vulnerabilities. First, we provide *secure channel control* to protect the channel assignment process from external attacker. We use cryptographic primitive *e.g.,* block cipher to encrypt the channel control message. Second, we add additional module called, Message verification module. This module consists of three phase, *Channel status gathering*, *Discrepancy checking* and *Message verification*. In *channel status gathering*, one node collects the channel status of other nodes within the interference range, and selects the candidate preferred channel. In *discrepancy checking* phase, each node within the interference range checks the discrepancy of current channel and interface from the requested channel and interface. In *message verification* phase, each node compares the number of the requested channel from the PARENT node with his candidate preferred channel to verify whether the change request is legitimate or not. Our simulation result using NS-2 simulator shows that proposed scheme can protect channel assignment process from both external and internal attacker in the presence of attacker that launches MCS and CCS attacks.

2. Characteristics of wireless mesh network

2.1 Definitions: WMN

"A wireless mesh network is a communications network made up of radio nodes organized in a mesh topology" by *Wikipedia*. Wireless mesh networks often consist of mesh clients, mesh routers and gateways[3]. The typical entities of mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may not be connected to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Accessing to this mesh cloud depends on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy;when one node can no longer operate, the remaining nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks can be implemented with various wireless technology including IEEE 802.11, 802.16, cellular technologies or combinations of more than one type.

A wireless mesh network can be seen as a special type of wireless *ad-hoc* network. It is often assumed that all nodes in a wireless mesh network are immobile but need not to be so. The mesh routers may be highly mobile. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an *ad-hoc* network since all of these nodes are often constrained by resources.

2.2 Node architecture

In general, WMN consists of two types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/repeater functions as in a conventional wireless router, a wireless mesh router contains additional routing functions to support mesh networking. To improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. Compared with a conventional wireless router, a wireless mesh router can achieve the same coverage with much lower transmission power through multi-hop communica-

tions. The medium access control (MAC) protocol in a mesh router is enhanced with good scalability in a multi-hop mesh environment. In spite of all these differences, mesh and conventional wireless routers are usually built based on a similar hardware platform. Mesh routers can be built based on dedicated computer systems (*e.g.,* embedded systems) as shown in Figure 2.1. They can also be built based on general-purpose computer sys-

Figure 2.1: Examples of mesh routers based on different embedded systems: (a) PowerPC (b) Advanced RISC Machines(ARM) [8]

tems (*e.g.,* laptop/ desktop PC). Mesh clients also have necessary functions for mesh networking, and thus, can also work as a router. However, gateway or bridge functions do not exist in these nodes. In addition, mesh clients usually have only one wireless interface. As a consequence, the hardware platform and the software for mesh clients can be much simpler than those for mesh routers. Mesh clients have a higher variety of devices compared to mesh routers. They can be a laptop/desktop PC, pocket PC, PDA, IP phone, RFID reader, BACnet (Building Automation and Control network) controller, and many other device, as shown in Figure 2.2. The architecture of WMN can be classified into three main groups based on the functionality of the nodes:

- **Infrastructure/Backbone WMN** This type of WMN includes mesh routers forming an infrastructure for clients that connect to the routers. The infrastructure and backbone of WMN can be built using various types of radio technologies, in addition to the mostly used IEEE 802.11 technologies. The mesh routers form a mesh of self-configuring, self-healing links among themselves. With gateway functionality, mesh routers can be connected to the Internet. This approach, also known as infras-

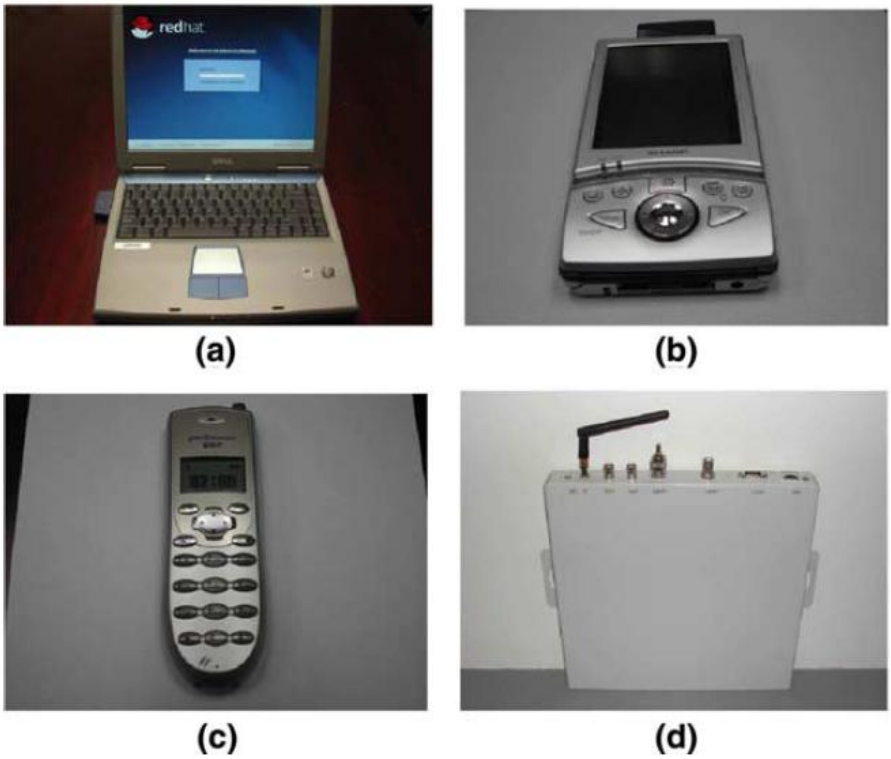

Figure 2.2: Examples of mesh clients: (a) Laptop, (b) PDA, (c) Wi-Fi IP Phone (d) Wi-Fi RFID Reader [8]

tructure meshing, provides backbone for conventional clients and enables integration of WMN with the existing wireless networks, through gateway/bridge functionalities in mesh routers. Conventional clients with Ethernet interface can be connected to mesh routers via Ethernet links. For conventional clients with the same radio technologies as mesh routers, they can directly communicate with mesh routers. If different radio technologies are used, clients must communicate with the base stations that have Ethernet connections to mesh routers. Infrastructure and backbone WMN is the most popular type. For example, community and neighborhood networks can be built using infrastructure meshing. The mesh routers are placed on the roof of houses in a neighborhood, which serves as access points for users inside the homes and along the roads. Typically, two types of radios are used in the routers, *i.e.,* for backbone communication and for user communication. The mesh backbone commu-

nication can be established using long-range communication techniques including directional antennas. The architecture is shown in Figure 2.3, where dash and solid lines indicate wireless and wired links, respectively.

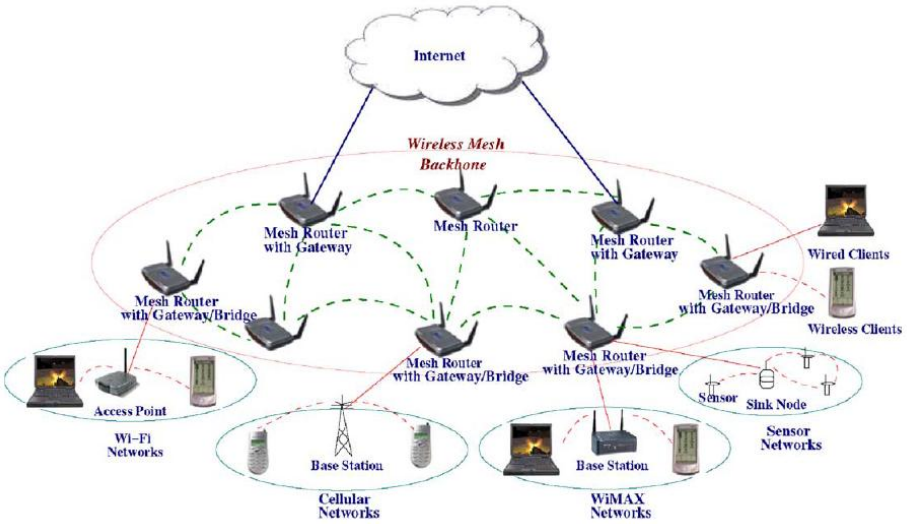

Figure 2.3: Infrastructure/backbone WMN [8]

- **Client WMN** Client meshing provides peer-to-peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end user applications to customers. Hence, a mesh router is not required for these types of networks. The basic architecture is shown in Figure 2.4. In Client WMN, a packet destined to a node in the network hops through multiple nodes to reach the destination. Client WMN is usually formed using one type of radios on devices. Moreover, the requirements on end-user devices is increased when compared to infrastructure meshing, since, in Client WMN, the end-users must perform additional functions such as routing and self-configuration.

- **Hybrid WMN** This architecture is the combination of infrastructure and client meshing as shown in Figure 2.5. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved con-

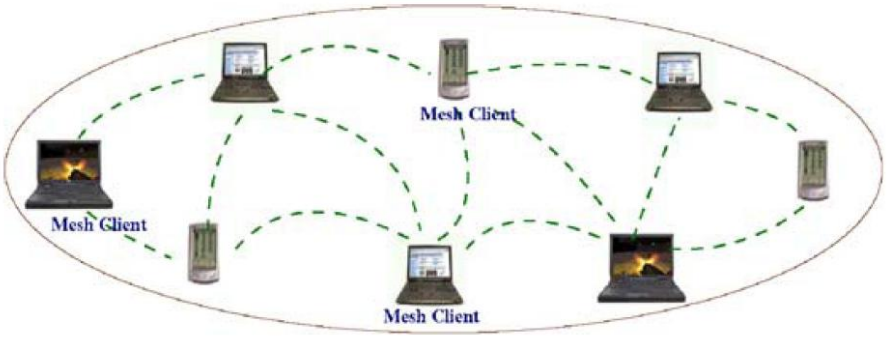

Figure 2.4: Client WMN [8]

nectivity and coverage inside the WMN. We believe that the hybrid architecture will be the best application.

2.3 Characteristic

The characteristics of WMN are explained as follows:

- **Multi-hop wireless network** A goal of developing WMN is to extend the coverage range of current wireless networks without sacrificing the channel capacity. Another objective is to provide non-line-of-sight (NLOS) connectivity among the users without direct line-of-sight (LOS) links. To meet these requirements, the mesh-style multi-hopping is indispensable[10], which achieves higher throughput without sacrificing effective radio range via shorter link distances, less interference between the nodes, and more efficient frequency re-utilization.

- **Support for *ad hoc* networking, and capability of self-forming, self-healing, and self-organization** WMN enhances network performance, because of flexible network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity, *i.e.,* multipoint-to-multipoint communications[19]. Due to these features, WMN has low upfront investment requirement, and the network can grow gradually as needed.

- **Mobility dependence on the type of mesh nodes** Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes.

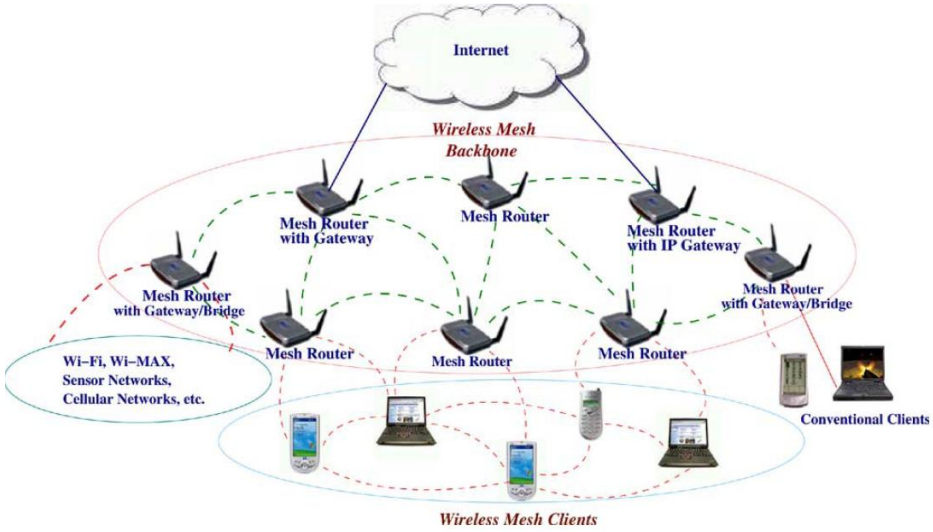

Figure 2.5: Hybrid WMN [8]

- **Multiple types of network access** In WMN, both backhaul access to the Internet and peer-to-peer (P2P) communications are supported[8]. In addition, the integration of WMN with other wireless networks and providing services to end-users of these networks can be accomplished through WMN.

- Dependence of power-consumption constraints on the type of mesh nodes Mesh routers usually do not have strict constraints on power consumption. However, mesh clients may require power efficient protocols. As an example, a mesh-capable sensor[15] requires efficient communication protocol. Thus, the MAC or routing protocols optimized for mesh routers may not be appropriate for mesh clients such as sensors, because power efficiency is the primary concern for wireless sensor networks.

- **Compatibility and interoperability with existing wireless network** For example, WMN built based on IEEE 802.11 technologies must be compatible with IEEE 802.11 standards in the sense of supporting both mesh-capable and conventional Wi-Fi clients. Such WMN also needs to be inter-operable with other wireless networks such as WiMAX, Zig-Bee, and cellular networks.

Based on their characteristics, WMN is generally considered as a type of *ad-hoc* networks due to the lack of wired infrastructure that exists in cellular or Wi-Fi networks through deployment of base stations or access points. While *ad hoc* networking techniques

are required by WMN, the additional capabilities require more sophisticated algorithms and design principles for the realization of WMN. More specifically, instead of being a type of *ad-hoc* networking, WMN aims to diversify the capabilities of *ad hoc* networks. Consequently, *ad hoc* networks can actually be considered as a subset of WMN. To illustrate this point, the differences between WMN and *ad hoc* networks are described below. In this comparison, the hybrid architecture is considered, since it comprises all the advantages of WMN.

- Wireless infrastructure/backbone. As discussed before, WMN consists of a wireless backbone with mesh routers. The wireless backbone provides large coverage, connectivity, and robustness in the wireless domain. However, the connectivity in *ad hoc* networks depends on the individual contributions of end-users which may not be reliable.

- Integration. WMN supports conventional clients that use the same radio technologies as a mesh router. This is accomplished through host-routing function available in mesh routers. WMN also enables integration of various existing networks such as Wi-Fi, Internet, and sensor networks through gateway/bridge functionalities in the mesh routers. Consequently, users in one network are provided with services in other networks, through the use of the wireless infrastructure. The integrated wireless networks through WMN resemble the Internet backbone, since the physical location of network nodes becomes less important than the capacity and network topology.

- Dedicated routing and configuration. In *ad hoc* networks, end-user devices also perform routing and configuration functionalities for all other nodes. However, WMN contains mesh routers for these functionalities. Hence, the load on end-user devices is significantly decreased, which provides lower energy consumption and high-end application capabilities to possibly mobile and energy constrained end-users. Moreover, the end-user requirements are limited which decreases the cost of devices that can be used in WMN.

- Multiple radios. As discussed before, mesh routers can be equipped with multiple radios to perform routing and access functionalities. This enables separation of two main types of traffic in the wireless domain. While routing and configuration are performed between mesh routers, the access to the network by end users can be carried out on a different radio. This significantly improves the capacity of the network. On the other hand, in *ad hoc* networks, these functionalities are performed in the same channel, and as a result, the performance decreases.

- Mobility. Since *ad hoc* networks provide routing using the end-user devices, the network topology and connectivity depend on the movement of users. This imposes additional challenges on routing protocols as well as on network configuration and deployment.

3. Background and related work

In this Section, we explain the channel assignment mechanism of *Hyacinth* and observe possible attacks that disrupt the channel assignment process in WMN.

3.1 Interference in WMN

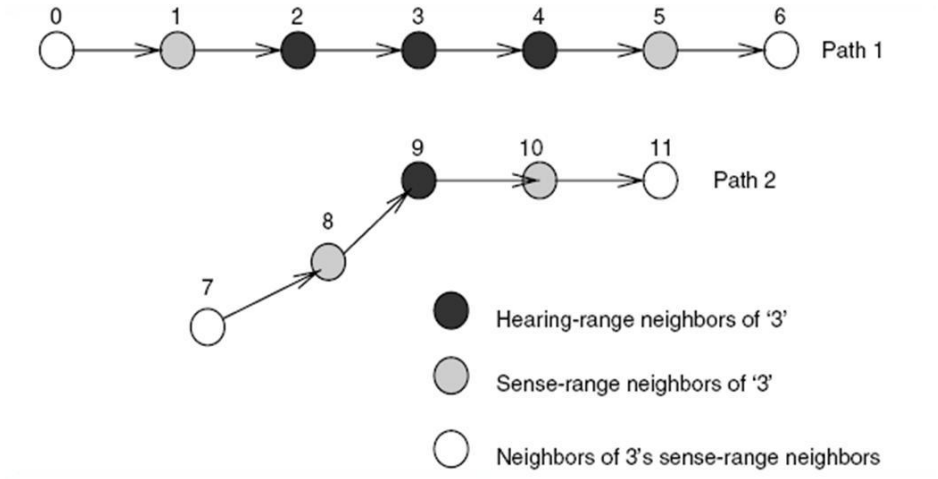

Figure 3.1: Intra-path and Inter-path interference in a single-channel multi-hop *ad hoc* network

Despite significant advances in physical layer technologies, the current wireless LAN still cannot offer the same level of sustained bandwidth as their wired connections. The advertised 54 Mbps bandwidth for IEEE 802.11a/g based hardware is the peak link-level data rate. When all the overheads, MAC contention, 802.11 headers, ACK and packet errors are accounted for, the actual goodput available to applications is almost halved. In addition, the maximum link-layer data rate falls quickly with increasing distance between the transmitter and the receiver. The bandwidth problem is further aggravated for multi-hop *ad hoc* networks because of interference from adjacent hops in the same path as well as from neighboring paths. Figure 3.1 shows an example of such interference. For-

tunately, the IEEE 802.11b/802.11g standards[1] and IEEE 802.11a standard[2] provide 3 and 12 non-overlapping frequency channels, respectively, that could be used simultaneously within a neighborhood. An ability to utilize multiple channels within the same network substantially increases the effective bandwidth available to wireless network nodes. Such bandwidth aggregation is routinely used when an 802.11-based wireless LAN operates in infrastructure mode, where traffic to and from wireless nodes is distributed among multiple interfaces of an access point or among multiple access points to avoid congestion. However, bandwidth aggregation is rarely applied to 802.11-based LANs that operates in the *ad hoc* mode.

3.2 Channel dependency problem

Figure 3.2 shows the channel dependency problem that can happen during channel assignment over WMN. Each number on the straight line between nodes indicates channel num-

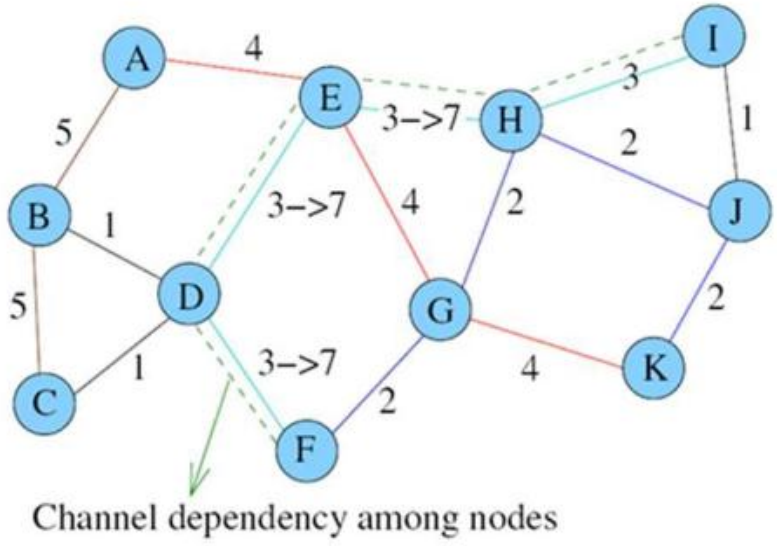

Figure 3.2: Channel dependency problem

ber. IEEE 802.11 a/g specification supports 3 and 12 non-overlapped frequency channels. This feature can solve the bandwidth degradation problem in multi-hop WMN. However, switching one of nodes channel to another one is not as simple as it looks. In Figure 3.2,

a node equips with two NICs. Therefore, it is able to use two channels simultaneously. Node E is currently using channels 3 and 4. After receiving traffic load information from other nodes in within the interference range, node E finds out that channel 7 is relatively less crowded than other channel. Thus, node E switches the interface from 3 to 7. Then, node D that is communicating with node E using channel 3 should also change the channel interface from 3 to 7. This ripple effect also goes all the way to other nodes including nodes F, I and *etc.* This would affect the bandwidth usage over entire WMN. Therefore, we need stable and efficient channel assignment algorithm that overcomes channel dependency problem.

3.3 *Hyacinth*

3.3.1 Multi-channel Multi-radio WMN

Hyacinth is a multi-channel WMN architecture that equips each node with multiple 802.11 based NICs. To utilize multiple interfaces equipped in each node, we need intelligent channel assignment algorithm which decides the performance of multi-channel WMN.

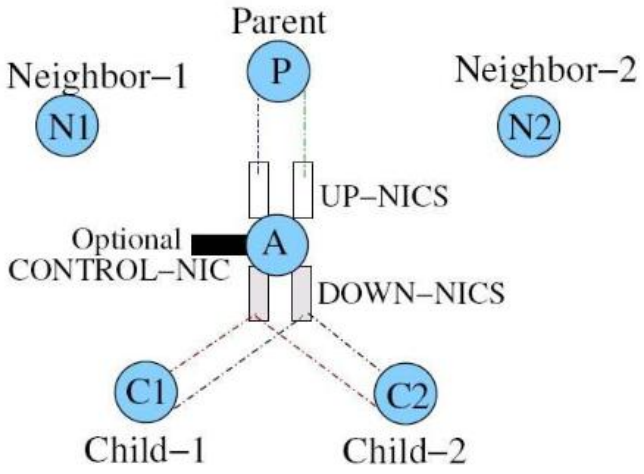

Figure 3.3: Interface structure of *Hyacinth* node

3.3.2 Distributed channel assignment algorithm

Figure 3.3 describes the interface structure of *Hyacinth* node. *Hyacinth* separates the interface of each node into two NICSs, UP-NICs and DOWN-NICs. UP-NICs of each node are filled with channel used by the parent node. Thus, a child node does not have to consider the channel assignment of the UP-NICs. Other than UP-NICs, each node only has to consider about channel assignment of the DOWN-NICs. In CHNL_CHANGE message, interface ID, current channel and new channel is specified. Also in CHNL_USAGE message, node ID, Interface ID, current channel, hop count and bandwidth usage is specified. *Hyacinth* proposes distributed channel assignment algorithm that takes advantage of load information based on local traffic. Local traffic load information is propagated among nodes within the interference range using CHNL_USAGE message. Based on the information from received CHNL_USAGE message, each node makes their decision whether to change their interface to less-loaded channel or fix it to an old channel as it was. If any node finds relatively less-loaded channel within the interference range, he changes his interface to that less loaded channel, and sends CHNL_CHANGE message to the child node for changing a channel as well.

3.4 Security vulnerabilities in channel assignment algorithm

3.4.1 Assumptions

We assume that a malicious attacker can compromise any node in WMN. By compromising the relaying node, attacker can transmit false CHNL_USAGE or CHNL_CHANGE information to neighboring nodes. A compromised node has correct secret key to communicate with neighboring nodes. Thus, neighboring nodes accept any messages that come from the compromised node.

3.4.2 Flooding false channel control message

Channel assignment algorithm in *Hyacinth* does not provide any means of secure transmission of channel control message, which means this algorithm is not designed with security in mind. In this way, if any external attacker broadcasts false channel control message into WMN, any node accept, and change their channel status as received message. If any external attacker *e.g.,* lap-top class attacker, continuously broadcast same CHNL_CHANGE

message to neighboring nodes, making every nodes use the same channel, entire WMN falls into denial of service status.

3.4.3 Malicious channel switching

Any compromised node can change the down interface. Upper interface of each node is conformed to the down interface of the PARENT node. Therefore, if compromised node deliberately change the down interface with heavily loaded channel[12]. This results bandwidth problem of entire WMN. Node M is the node that is compromised by malicious attacker. Attack sequence of MCS is as follows :

1. Node M receives CHNL_USAGE message from neighboring nodes within the interference range.
2. Node M finds out that channels k and l are relatively much loaded than other channel.
3. Node M switches channel l to channel k, and channel j to channel n, respectively.
4. Node M then transmits CHNL_CHANGE message to both node F and node H.
5. All links that locates comes before node M suffers from performance degradation due to heavily loaded channel

Figure 3.4 shows the simulation of *Hyacinth* under MCS attack.

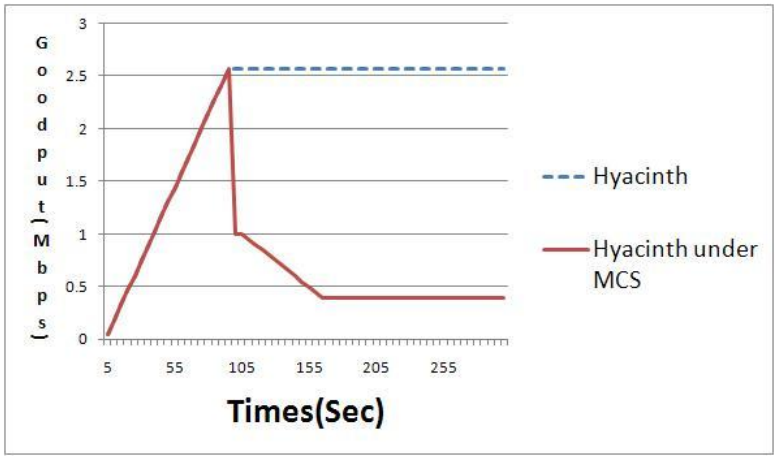

Figure 3.4: Simulation result of MCS attack

3.4.4 Consecutive channel switching

The purpose of CCS attack is to put WMN into a quasi-stable state. Quasi-stable state means that each node are forced to change their channel so frequently that networks can not support stable bandwidth to user. Attack sequence of CCS is as follows:

1. Node M receives CHNL_USAGE message from neighboring nodes within the interference range.
2. Node M randomly selects one of the channels in the channel list that are normally loaded.
3. Node M then constructs CHNL_USAGE message with selected channel assignments and broadcasts it the neighboring nodes.

Figure 3.5 shows the simulation of *Hyacinth* under CCS attack. Unlike MCS attack, CCS doesn't deliberately change any channel assignment of the DOWN-NICs. Instead, it just selects middle priority channels, and propagates CHNL_USAGE which results in propagation of change upwards in the routing tree. Heavily loaded channels are not selected because such selections will affect the links closer to gateway resulting in quick adjustment to the change and hence no ripple effect will be created. We first measure bandwidth usage under normal multi-radio multi-channel WMN. Attack simulation is performed using NS2 simulator. First, we measure the bandwidth usage under MCS and CCS attacks. Under CCS, bandwidth shows unstable state due to frequent channel switching.

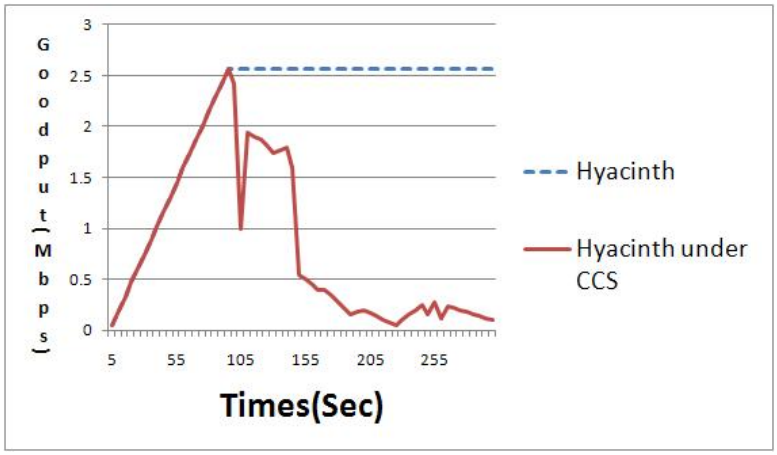

Figure 3.5: Simulation result of CCS attack

4. Our proposed scheme

In this Section, we propose secure channel control and message verification module to prevent attacks mentioned in Section 2. First, secure channel control provides authenticated channel assignment process between each node, thus preventing external attacker from propagating fabricated channel control message. Second, message verification module prevents inside attacker from disabling the stable channel assignment process.

4.1 Network model

A wireless mesh network can be modeled as a connected graph $G = (V,E)$, where V is the set of N mesh nodes and $E \subset V \times V$ is the set of wireless links. We assume that each node uses omni-directional antennas and all wireless links are bi-directional[4]. A wireless link exists between nodes i and j if the distance between the two nodes, $d_{i,j}$, is smaller than R_t, where R_t is a fixed transmission range. For simplicity, we assume that a transceiver has the same receiving and transmission range. Thus, in our context, each edge $(i, j) \in E$ represents an undirected edge of the graph G. Let the set of channels supported by the 802.11 spectrum be denoted as K, where $K = 1, 2, \ldots, k$, and the number of radios on each node as $M_i \leq |K|$, $\forall i \in V$. We assume that all channels are orthogonal, so the interference exists between two links if they are within the interference range and are assigned the same channel. We believe that our model can be easily extended to account for non-orthogonal channels. To model the interference we consider a conflict graph $G_c = (V_c, I)$, where $V_c = E$ and $I \subset E \times E$. Two links (i, j) and (u, v) interfere with each other if they operate on the same channel and any of the quantities $d_{u,i}$, $d_{v,i}$, $d_{u,j}$, $d_{v,j}$ is smaller than sR_i, where R_i denotes the fixed interference range. Let $I_{i,j} \subset I$, $\forall (i, j) \subset E$, denote the set of all links in the network within the interference range of link (i, j). Let L be the load matrix of the network. Thus, $L_{i,j}$ is the expected traffic on link (i, j). This flow estimate of network traffic can be obtained using tools like the CoMo project[21]. We also make the following assumptions while modeling the channel assignment problem in wireless mesh networks.

- The traffic flow on the network is relatively stable over a period of time and is easy to predict. This is a fairly reasonable assumption for enterprise networks which are

designed for balanced network flows.

- Nodes are generally static. This ensures no major topology changes during the course of channel assignment.

4.2 Assumption

Our proposed scheme modifies *Hyacinth* to protect channel assignment procedure from external and inside attackers. We assume that each node has a capability of using multiple interface and radio. Our network consists of a set of mesh nodes, which communicate both wire and wireless medium. We assume that the radio link between neighboring devices is bidirectional. The network is operated by an authority. The authority controls the network membership and assigns a unique identity to each node. Each pair of nodes holds a shared secret key that can either be manually preloaded into the nodes during the deployment phase or can be generated during the network setup phase using key establishment protocols(*e.g.,* Perrig *et al.*[13];Eschenauer and Gligor[6]).

4.3 Attacker model

We consider an omnipresent but computationally bounded adversary. He/she controls the communication channel in the sense that she is able to eavesdrop, insert, modify, and block arbitrary messages by adding his/her own signal to the channel (*e.g.,* in order to jam the signal). We distinguish two attacker models: internal and external. In the external attacker model we assume that none of the nodes involved in the protocol are compromised. Thus, an external attacker cannot authenticate herself as an honest network node to other network nodes or to the central authority. An internal attacker, however, controls one or more network nodes. We assume that when a node is compromised, his secret keys are known to the attacker. Subsequently, compromised nodes can authenticate themselves as legitimate nodes to the authority and to other network nodes. A legitimate node can also misbehave because of legitimate corruptive processes such as software, hardware, or system faults. We classify these nodes likewise as internal attackers.

4.4 Secure channel control

We initially propose secure channel control scheme to prevent false channel control message of external attacker. We use cryptographic measure to authenticate the received con-

trol message. This scheme is designed to be run by two nodes that reside within the range of communication. Table 4.1 described each steps of secure channel control.

Table 4.1: Secure channel control

Secure channel control(SCS)
1. A → B : $ENC_{K_{AB}}$(CHNL_USAGE), $MAC_{K_{AB}}(CHNL\_USAGE)$)
2. B : Decrypt received message using K_{AB}
3. B : Verify $MAC_{K_{AB}}(CHNL\_USAGE)$
4. B → A : If verified, ACK
or, NEG_ACK

In this protocol, integrity and authenticity of channel control message are ensured through use of block cipher encryption, message authentication code and of a key K_{AB} shared between nodes A and B. This prevents external attackers from modifying values in the channel control message or in the acknowledgement packet, without being detected. Furthermore, the attacker cannot impersonate node B as she does not know the secret key K_{AB}.

4.5 Message verification module

We modified *Hyacinth* to prevent three major attacks explained in the previous Section. To prevent those attacks, we need additional module to verify two information messages, 'CHNL_USAGE' message and 'CHNL_CHANGE' message. In our scheme, we call this module as, 'message verification module'. This module consists of three phase. Followings are the key idea of message verification module :

A. Neighboring nodes retains similar interference range : In *Hyacinth*, each node shares channel usage status within (k+1) neighboring nodes. In other words, node that is close to each other used to have similar interference range. Therefore, each node can maintain similar channel usage information. This can help each node to independently judge whether the received channel usage information is correct or not based on other CHNL_USAGE information from neighboring nodes. In our proposed scheme, each node always maintain 'candidate channel' to compare with CHNL_CHANGE message from PARENT node.

B. UP-NIC of the CHILD node is dependent on the DOWN-NICs of the PARENT node : To prevent the channel dependency problem of channel assignment,

UP-NIC of each node is restricted to the DOWN-NIC of the PARENT node. In this way, each node only concentrates on assigning channel to the DOWN-NICs. Therefore, channel dependency problem can be prevented. This feature can be used efficiently to judge CHNL_USAGE information from PARENT node. For example, if one PARENT node is compromised and propagates falsely modified CHNL_USAGE message to the CHILD node, CHILD node can compare his own CHNL_USAGE with received message. Therefore, verification mechanism can be constructed.

Based on above concept, channel control message can be filtered through message verification module. Figure 4.1 describes a structure of message verification module.

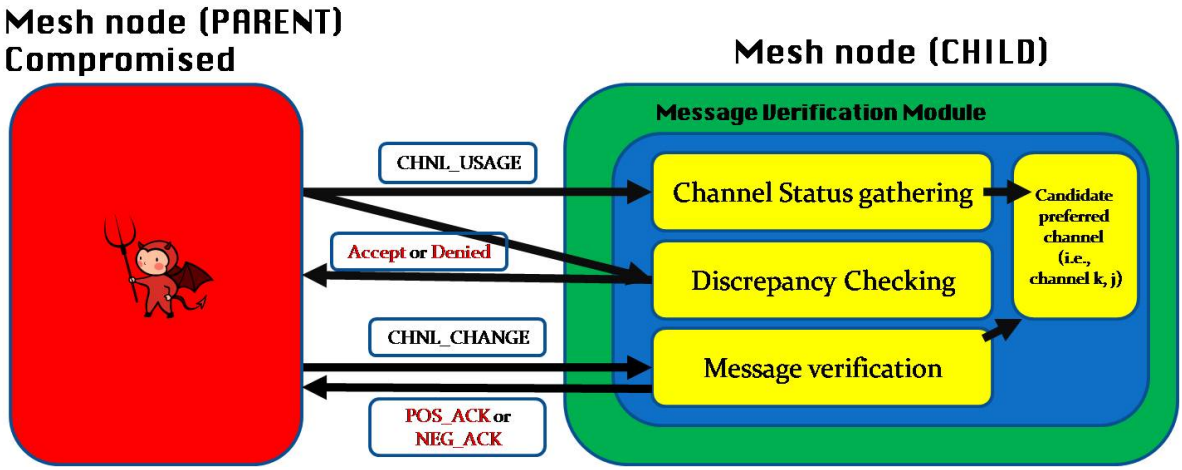

Figure 4.1: Message verification module

4.5.1 Channel status gathering phase

In *channel status gathering phase*, we decide candidate preferred channel by using CHNL_USAGE message received from neighboring in the interference domains of each nodes. Since CHNL_USAGE message is propagated to (k+1) hop range of each node, single node receives multiple CHNL_USAGE message from neighboring nodes. Then, that node sorts each message's interface list in an increasing order of bandwidth usage. Top list of each message indicates the least loaded channel. Checking consistency of above value, we can select which channel is the least loaded channel within the interference range even if there are malicious nodes broadcasting false CHNL_USAGE message. Pseudo code is described in Table

4.2.

Table 4.2: Channel status gathering phase

Algorithm 1 : Channel status gathering
+ collecting n CHNL_USAGE from neighboring nodes
+ for every CHNL_USAGE message from 1_{th} to n_{th}
- for every channel list in CHNL_USAGE
* sort the list in an increasing order depending on bandwidth usage
* select two topmost least loaded channels
- end for
+ mark the frequency of two topmost crowded channel
+ end for
+ select the two most frequently marked channel as a candidate preferred channel

4.5.2 Discrepancy checking

As described above, each node always maintain a n number of candidate preferred channel (n is a number of NICs). In this phase, we check the discrepancy between each DOWN-NICs and UP-NICs. Discrepancy means that the channel of the CHILD node which is assigned to one interface doesn't correspond to the channel and the interface of the PARENT node. We covered the concept that the UP-NICs of the CHILD node are restricted to DOWN-NICs of the PARENT node. This feature can be useful to prevent the CCS attack that forced ripple effect to neighboring node. Let's say that one node receives fabricated message that triggers CCS attack as shown below. Pseudo code is described in Table 4.3.

4.5.3 Message verification

False CHNL_USAGE message can be filtered using second phase by checking consistency of interface and channel between PARENT node and CHILD node. However, channel change process is different from CHNL_USAGE message propagation. In other words, channel change happens before the PARENT node sends CHNL_USAGE message to the CHILD node. Therefore, it is not possible for current *Hyacinth* architecture to prevent MCS at-

Table 4.3: Discrepancy checking phase

Algorithm 2 : Discrepancy checking
+ Receiving CHNL_USAGE message from the PARENT node
+ compare channel usage of the UP-NICs of each node with the one in CHNL_USAGE message from PARENT node
+ if
- the channel of the interface of PARENT node matches with channel of corresponding interface of the CHILD node
* CHNL_USAGE message is accepted
- else
* CHNL_USAGE message is discarded
end for

Table 4.4: Message verification phase

Algorithm 3 : Message verification
+ Receiving CHNL_CHANGE message from the PARENT node
+ compare requested channel with candidate preferred channel of the node
+ if
- requested channel matches candidate preferred channel
* channel switching is performed
- else
* channel switching is denied
+ end if

tack, in that compromised node deliberately changes the DOWN-NICs to heavily loaded channel. Thus, we modified current *Hyacinth* to send CHNL_USAGE message along with CHNL_CHANGE message. Previous channel switching is performed without the agreement of CHILD node. In our model, we transmit the CHNL_USAGE and CHNL_CHANGE simultaneously to compare the consistency of channel switching. If candidate preferred channel of the CHILD node is consistent with the switching channel of the PARENT node, channel switching is performed. However, if this is not consistent, channel switching is denied. Pseudo code is described in Table 4.4.

5. Performance and security analysis

We conducted performance evaluation using NS-2 simulator[11]. We implemented *Hyacinth* architecture and add security mechanism at the network layer protocol stack. We used a 15 node grid topology for physical placement of the nodes. The distance between each node was adjusted to restrict the interference domain of the nodes to two hop physical neighbors. The security mechanism was added to the *Hyacinth* channel assignment algorithm and the performance was compared between the *Hyacinth* model under attacks and the protected *Hyacinth* model using proposed security mechanism under attacks.

5.1 Performance analysis

We first measure the goodput of the target network when no attack is launched. Then, *Hyacinth* under each attack is simulated. Finally, *Hyacinth* with security mechanism under each attack is simulated to measure the network goodput. Figures 5.1 and 5.2 shows the simulation result under three circumstances; MCS and CCS attack, respectively. The result shows that goodput under each attack severely degrades the performance of WMN. However, our security mechanism can protect those attacks and preserve the stable goodput of WMN. Simulation parameter is as follows:

- Node / topology : 15 node / grid layout
- Interference range : Two hop range
- 802.11 Specification : b/g
- The number of non-overlapped radio channel : 3
- Flow type : Two Constant Bit Rate (CBR)
- Flow rate : $0 \sim 5$Mbps
- Encryption : AES-128 CBC

As can be shown in Figures 5.1 and 5.2, our proposed scheme is useful for protecting channel assignment process from malicious attack. We assume that attacker starts his/her attack at 100 second when the goodput of the network converges up to 2.5. Although MCS

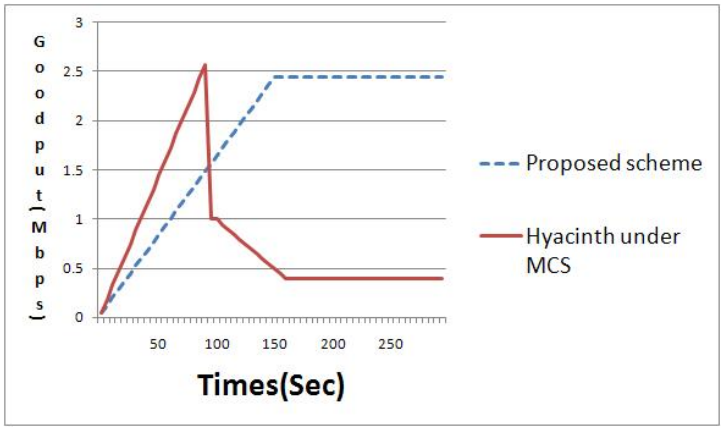

Figure 5.1: Simulation of proposed scheme under MCS attack

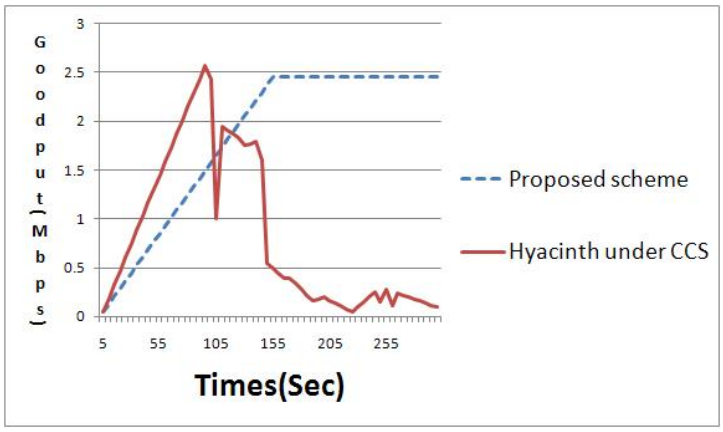

Figure 5.2: Simulation of proposed scheme under CCS attack

and CCS begin, goodput of entire network is not degraded. As can be shown in Fig 5.1 and 5.2, network goodput does not converge at the same time as normal *Hyacinth* does. The reason is that it consumes additional encryption overhead during the secure channel control phase. It takes an additional time to encrypt the communication channel between each node.

5.2 Security analysis

Security requirements of *Hyacinth* are as follows: confidentiality and availability. Normal *Hyacinth* was designed without considering these security considerations. However, our proposed scheme uses cryptographic measure to provide confidentiality. Also, message verification module guarantees availability of stable channel assignment by filtering the malicious channel control message generated by compromised node.

- **Confidentiality** CHNL_USAGE and CHNL_CHANGE messages are valuable to external attacker, investigating which channel the target node is using. If any specific node takes charge of significant role in WMN, disabling only those nodes would put entire WMN into poor performance. Moreover, leakage of channel information helps malicious attacker identifying the status of network, which leads to further attack attempt. Thus, protecting these channel related information is important task.

  Our proposed scheme encrypts CHNL_USAGE and CHNL_CHANGE message transmitting between each node, thus preventing external attacker from collecting these messages. If any external attacker without the knowledge of shared secret key propagates false channel control messages into the network, those messages are denied since they cannot be decrypted without proper secret key.

- **Availability** Attacks mentioned in Section 3.4 significantly degrades the performance of WMN. As the attacks continuously happen, whole WMN goes into DoS status. Those attacks are launched by compromised nodes, thus making it difficult to protect by cryptographic primitive. Using message verification module, each nodes filter the receiving control message from the neighboring nodes. Based on the inherent character of *Hyacinth*, receiver can judge if the CHNL_USAGE message originates from the legitimate nodes or not. Moreover, *candidate preferred channel* is periodically maintained on each nodes to judge if the demanding channel in the received CHNL_CHANGE message is proper or not. Even if the compromised nodes exist among the neighboring nodes, false channel control message is filtered through proposed filtering mechanism.

6. Conclusion

We explain the security vulnerabilities of channel assignment architecture *Hyacinth*. Attacker model is classified into two categories : external and internal attacker. External attacker does not have precise knowledge about the network *e.g.,* secret key. Internal attacker can be compromised nodes which know the shared secret key among each node.

External attacker can propagate false channel control message, interrupting the stable channel assignment. Also, internal attacker can transmit any fabricated CHNL_USAGE or CHNL_CHANGE message to neighboring nodes. Compromised node then can deliberately change the DOWN-NICs with heavily loaded channel, so that bandwidth usage over entire WMN is degraded. Moreover, propagating wrong CHNL_USAGE message triggers further channel switching to reverse direction of spanning tree of nodes. We define these attacks as MCS and CCS.

In this thesis, we modified the current *Hyacinth* architecture to prevent from the two attacks. First, we provide *secure channel control* to protect the channel assignment process from external attacker. We use cryptographic primitive *e.g.,* block cipher to encrypt the channel control message. Second, we add an additional module called, Message verification module. This module consists of three phase, *Channel status gathering*, *Discrepancy checking* and *Message verification*. In *channel status gathering*, node collects CHNL_USAGE message from neighboring nodes and selects the candidate preferred channel. In *discrepancy checking* phase, node check the discrepancy of the channel and interface from requested channel and interface. In *message verification* phase, node compares requested switching channel from PARENT node with the candidate preferred channel to verify the integrity of CHNL_CHANGE message. Our simulation result using NS-2 simulator shows that proposed scheme can protect channel assignment process from both external and internal attacker in the presence of attacker that launches MCS and CCS attacks.

요 약 문

다중 라디오 다중 채널 무선 메쉬 네트워크에서의 안전한 채널 할당을 위한 인증 기법에 관한 연구

*Hyacinth*는 *Ashish* 등에 의해 제안된 다중-라디오 다중-채널 무선 메시 네트워크를 위한 효율적인 채널 할당 알고리즘이다. 그러나 본 학위논문에서는 *Hyacinth*가 보안 메커니즘을 고려하지 않고 디자인되었다는 점을 지적한다. 외부 공격자로부터의 위조 채널 제어 패킷은 네트워크 굿풋을 저하시킨다. 또한 탈취 노드와 같은 내부 공격자로부터의 서비스 거부 공격:MCS(malicious channel switching), CCS(consecutive channel switching)은 채널 할당 알고리즘을 서비스 거부 상태에 빠뜨릴 수 있다. 본 학위논문에서는 외부와 내부 공격자로부터의 공격에 안전한 다중-라디오 다중-채널 무선 메시네트워크를 위한 채널 할당 알고리즘을 제안한다. 본 논문의 채널 할당 알고리즘은 첫번째로, 외부 공격자로부터의 위조 제어 패킷에 대응하기 위해 *Secure channel control*, 둘째로 내부 공격자로부터의 서비스 거부 공격을 막기 위해 *Message verification module*을 제공한다. NS2를 사용한 시뮬레이션을 통해 제안방식이 외부와 내부 공격자로부터의 공격을 효율적으로 막아, 안정적인 채널 할당을 유지해준다.

References

[1] A. Acharya, A. Misra, S. Bansal. High-performance architectures for IP-based multi-hop 802.11 networks. IEEE Wireless Communications 10 (5). 2003.

[2] A. Adya, P. Bahl, J. Padhye, A. Wolman, L. Zhou. A multi-radio unification protocol for IEEE 802.11 wireless networks. International Conferences on Broadband Networks (BroadNets). 2004.

[3] Ian F. Akyildiz , Xudong Wang , Weilin Wang. Wireless Mesh Networks: a Survey. Computer Networks and ISDN Systems. 2005.

[4] S. Bellofiore, J. Foutz, R. Govindaradjula, I. Bahceci, C.A. Balanis, A.S. Spanias, J.M. Capone, T.M. Duman. Smart antenna system analysis. integration and performance for mobile ad hoc networks (MANET). IEEE Transactions on Antennas and Propagation. 2002.

[5] S. Corson and J. Macker. Book Mobile ad hoc networking(MANET). IETFRFC 2501, 1999.

[6] L. Eschenauer and V. Gligor. A Key Management Scheme for Distributed Sensor Networks. In 9th ACM Conference on Computer and Communication Security. 2002.

[7] Kuo F. Fraklin. The ALOHA system. ACM Computer Communication Review, 1995.

[8] J. Jun, M.L. Sichitiu. The nominal capacity of wireless mesh networks. IEEE Wireless Communications 10 (5). 2003.

[9] Murali Kodialam, Thyaga Nandagopal. Characterizing the capacity region in multi-radio multi-channel wireless mesh networks. In proceedings of Mobile Computing and Networking. 2005.

[10] L. Krishnamurthy, S. Conner, M. Yarvis, J. Chhabra, C. Ellison, C. Brabenac, E. Tsui. Meeting the demands of the digital home with high-speed multi-hop wireless networks. Intel Technology Journal 6 (4). 2002.

[11] S. Kurkowski, T. Camp and M. Colagrosso. MANET Simulation Studies: The Incredibles. ACM SIGMOBILE Mobile Computing and Communication Review, Vol. 9, Issue 4. 2005.

[12] Anjum Naveed and Salil S. Kanhere. Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks. IEEE Globecom'06, Nov 2006.

[13] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler. SPINS: Security Protocols for Sensor Networks. Proceedings of Seventh Annual International Conference on Mobile Computing and Networks. 2001.

[14] R. Poor. Wireless mesh networks. Sensors. 2003.

[15] R. Poor. Wireless mesh links everyday devices. Electronic Engineering Times. 2004.

[16] Krishna N. Ramachandran, Elizabeth M. Belding, Kevin C. Almeroth, Milind M. Buddhikot. Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks. In Proceedings of IEEE Infocom'06. 2006.

[17] Ashish Raniwala, Kartik Gopalan, Tzicker Chiueh. Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networs. In ACM SIGMOBILE Mobile Computing and Communications Review (MC2R). 2004.

[18] Ashish Raniwala, Tzi-cker Chiueh. Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network. In proceedings of IEEE InfoCom'05. 2005.

[19] S. Tierney. Mesh Networks. whitepaper of communitynetworking.org.

[20] C. K. Toh. Ad Hoc Mobile Wireless Networks. Pretice Hall Publisher, 2002.

[21] The CoMo Project, http://www.como.intel-research.net.

감 사 의 글

암호와 정보보안 연구실에서 2년간 연구의 기회를 허락해주신 김광조 교수님께 먼저 감사 드립니다. 변변치 못한 논문들, 영어 및 문법부터 세부 아이디어까지 수정해주신 교수님의 노고가 없었다면, 오늘 이렇게 학위 논문 제출할 수 없었을 것입니다. 그리고 심사위원으로 학위 논문을 검토해주신 김명철, 이병천 교수님께 감사의 말씀드립니다. 특히 Wireless mesh network 수업에서 논문의 모티브를 제공해주신 김명철 교수님 감사합니다. 또한 연구실 선후배님들에게도 감사드립니다. 신입생때부터 논문 작성에 관해 많은 도움을 주신 현록형, 작은 아이디어를 들고가면 더 크고 좋은 아이디어로 만들어 주신 장성이형, 날카로운 안목으로 논문 아이디어의 장단점을 지적해주시는 진이형, 끝없는 호기심으로 논문에 대해 질문해주시는 규석형, 2년간 연구, 수업, 과제를 같이 해왔던 동기 명한과 임성, 똘똘하고 일 잘하는 후배 준현, 모두가 있어줘서 무사히 석사 생활 마칠 수 있었습니다. 기도로 제 뒤를 항상 밀어주시는 어머니와 말씀은 안하시지만 항상 저를 걱정하시는 아버지, 사랑합니다.

Curriculum Vitae

Name : Sungmok Shin

Date of Birth : January 21, 1982

Birthplace : 69-3, Guseo-dong, Gumjung-gu, Busan, 609-310 KOREA

Domicile : 327-3, Gumgang-dong, Dong-gu, Daegu, 701-330 KOREA

Address : R504, 109 Munjiro, Yusong-gu, Daejeon, 305-714 KOREA

E-mail : cabin15@kaist.ac.kr

Educations

2001. 3. – 2008. 2. Computer Multimedia Engineering, Pukyung National University (B.S.)

2008. 2. – 2010. 2. Information and Communications Engineering, KAIST (MS course)

Career

2007. 3. – 2008. 2. Development of Sensor Tag and Sensor Node Technique for RFID/USN by ETRI

2008. 11. – 2008. 11. 신승목, 이현록, 김광조, "Security Analysis of current Coexistence Proof protocol in RFID system", 9th CJK workshop, 24 25 Nov, 2008, Jeju.

2009. 1. – 2009. 12. Research on the Next Generation Standard of EPCglobal by ETRI

2009. 2. – 2009. 9. Developing Distributed Authentication Technique for USN by Samsung Electronics

2009. 7. – 2009. 7. 신승목, 이현록, 김광조, "Mitigating the effect of node compromise: Self-healing mechanism for EPC Sensor network", 10th CJK workshop, 31 Jul 1 Aug, 2009, Shanghai, China

2009. 7. – 2009. 8. WinnerDigm Co, Internship program.

Publications

1. **신승목**, 이현록, Divyan M Konidala, *비트 스크램블을 통해 개선된 RFIDsec07의 상호 인증 프로토콜*, 2008년도 한국정보보호학회 영남지부 학술발표회 논문집, pp.89-93, 2008, 2008.2.20, 동서대학교, 부산.
2. **신승목**, 최임성, 김광조, *무선 센서 네트워크에서의 안전한 네트워크 재프로그래밍 기법*, CISC-S'08 Proceedings vol.18, no.1, pp.162-167, 2008.6.26, 순천향대학교, 천안.
3. **신승목**, 김광조, *수중 음향 센서 네트워크를 위한 안전한 시간 동기화 기법 연구*, CISC-W'08 Proceedings, pp.191-196, 2008.12.6, 고려대학교, 서울.
4. **신승목**, 이현록, 김광조, *능동형 RFID 태그 시스템을 위한 위치정보 보호기법에 대한 연구*, 한국정보보호학회 동계학술대회, 2009년도 한국정보보호학회 영남지부 학술발표회 논문집, 2009.2.20, 대구대학교, 대구.
5. **신승목**, 김광조, *아마존 S3를 통해 본 클라우드 컴퓨팅 환경에서의 스토리지 보안*, CISC-S'09 Proceedings, pp.406-410, 2009.6.19, 강원대학교, 삼척.
6. **신승목**, 이기열, 김광조, *모바일 환경을 위해 수정된 TPM이 장착된 디바이스의 원격 익명 입증 프로토콜*, CISC-W'09 Proceedings, pp.382-386, 2009.6.19, 연세대학교, 서울.
7. **Sungmok Shin** and Kwangjo Kim, *A Study on authentication scheme for channel assignment mechanism in multi-radio multi-channel wireless mesh networks*, Symposium on Cryptography and Information Security (SCIS), Jan. 19-22, Kagawa, Japan. (to appear)