Securing Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks

Aftabul Haq, Anjum Naveed and Salil S. Kanhere
Networks Group
School of Computer Science and Engineering
University of New South Wales
Sydney, Australia
{ahaq,anaveed,salilk}@cse.unsw.edu.au

UNSW-CSE-TR-0622
October 04, 2006

THE UNIVERSITY OF NEW SOUTH WALES

SYDNEY · AUSTRALIA

Abstract

In order to fully exploit the aggregate bandwidth available in the radio spectrum, future Wireless Mesh Networks (WMN) are expected to take advantage of multiple orthogonal channels, where the nodes have the ability to communicate with multiple neighbours simultaneously using multiple radios (NICs) over orthogonal channels. Dynamic channel assignment is critical for ensuring effective utilization of the non-overlapping channels. Several algorithms have been proposed in recent years, which aim at achieving this. However, all these schemes inherently assume that the mesh nodes are well-behaved without any malicious intentions. A recent work has exposed the vulnerabilities in channel assignment algorithms. In this paper, a mechanism is proposed to secure the channel assignment algorithms, addressing the security vulnerabilities in the existing algorithms. The proposed mechanism successfully prevents the WMN from the recently exposed attacks. The simulation based experiments show the effectiveness of the proposed solution. The experiments also show that the incurred overhead because of security is negligible.

1 Introduction

Wireless Mesh Networks (WMNs) are multi-hop wireless networks consisting of mesh routers and mesh clients. Generally, mesh routers have limited mobility and provide the connectivity to mobile mesh clients over multiple hops. Some of the mesh routers are equipped with wired interface and serve the purpose of gateway to provide the connectivity with the Internet. The capability of self-organization and self-configuration have made WMNs a promising technology for numerous applications like broadband home networking, enterprise networking and building automation. To increase the available bandwidth, each mesh router is equipped with multiple radios (NICs). Orthogonal channels are used for each interface of the node which ensures simultaneous communication using all the wireless interfaces. A large number of orthogonal channels can ensure interference free communication, however, the number of available orthogonal channels in the radio spectrum is limited (3 in IEEE 802.11b [1] and 12 in IEEE 802.11g [2]). Dynamic channel assignment is required to assign the channels to the network links to ensure the optimum channel usage that can fulfill the routing as well as the bandwidth requirements of the network.

Various joint channel assignment and routing algorithms have been proposed for Multi-Radio Multi-Channel WMN (MRMC-WMN) [3–10]. In the centralized approach, the mesh nodes transmit the required information to a central node, the channel assignment decision is made centrally and the nodes are informed about the decision [3, 4]. On the other hand, in distributed algorithms [5], mesh nodes make the independent decision and inform the neighbouring nodes about the required information for neighbours to make their decisions independently using the provided information. However, the underlying assumption in all these channel assignment algorithms is that the mesh nodes are well-behaved. Therefore, in centralized as well as the distributed algorithms, the information provided by the mesh nodes is not verified for correctness. Further, in distributed channel assignment algorithms, the nodes make independent decision about their channel assignment which again is not verified. This assumed trust amongst the neighbouring nodes makes these algorithms vulnerable to security attacks. Naveed et. al. [11] have recently identified that the independent decision making of the nodes about their channel assignment and non-verification of the node decision make channel assignment algorithms vulnerable to the security attacks.

This paper addresses the security issues in channel assignment algorithms that were raised in [11]. A security mechanism is proposed to secure the channel assignment algorithms, aimed at improving the performance of WMNs by eliminating the affect of malicious nodes on channel assignment. The proposed security mechanism address the vulnerabilities that exist in almost all known dynamic channel assignment algorithms. The proposed

security mechanism not only detects the malicious nodes in the network but the necessary action is taken in order to prevent the attacks launched by the malicious nodes. We use Hyacinth model [5] to show the effectiveness of the mechanism, however, the mechanism is easily applicable to other channel assignment algorithms [3, 4]. Although various secure routing algorithms have been proposed for multi-hop wireless networks, to the best of our knowledge, this paper is the first to address the security issues in channel assignment of MRMC-WMN.

The rest of the paper is organized as follows. Section 2 reviews various channel assignment algorithms that have been proposed. In Section 3, the Hyacinth model [5] is discussed. The vulnerabilities in the channel assignment algorithms and attacks exploiting these vulnerabilities are also discussed. Section 4 describes the security mechanism for the channel assignment algorithms using the hyacinth model as example. Simulation results are presented in Section 5 and Section 6 concludes the paper with a roadmap for future work.

2 Related Work

Various techniques have been proposed to utilize multiple interfaces and increase the bandwidth of MRMC-WMN [3–10]. Use of multiple radios per node to increase the bandwidth of WMN was first proposed by Bahl et. al. [10]. The Authors proposed the centralized Multi-Radio Link Quality Source Routing (MR-LQSR) which requires the global information about the bandwidth, loss-rate and channel assignment in order to select the optimum routing paths. The information is transmitted by the nodes to central location where the decision is made. Raniwala et. al. [4] developed a set of centralized channel assignment, bandwidth allocation, and routing algorithms for MRMC-WMNs. The proposed neighbour partitioning scheme and the load-aware channel assignment requires the nodes to maintain channel assignment information of the neighbouring nodes. In a subsequent publication, Raniwala and Chiueh [5] proposed a distributed channel assignment algorithm, referred to as the *Hyacinth model*, which utilizes only local topology and local traffic load information to dynamically assign channels to the network links. Hyacinth model is explained in more detail in section 3.1. Ramachandran et. al. [3] have proposed a centralized interference-aware channel assignment algorithm and a corresponding channel assignment protocol. The protocol uses the knowledge of interference in the mesh network as well as the surrounding networks to perform channel assignment.

However, the primary focus of all the above mentioned algorithms is to improve the capacity of MRMC-WMN without any consideration for the security issues like the affect of misbehaving malicious nodes, compromised nodes, the threat of Denial of Service (DoS) attacks and the loss of confi-

dentiality. All these algorithms completely rely on the information provided by the nodes which is not verified for correctness. Further, in distributed channel assignment algorithms, the nodes make independent decision about their channel assignment which again is not verified. Independent decision by the nodes about their channel assignment and non-verification of this decision as well as non-verification of the information transmitted by the nodes about their channel assignment, make these algorithms vulnerable to security attacks [11].

A number of security protocols have been proposed to address the routing vulnerabilities in multi hop wireless networks. Yang et. al. [13] have proposed the self organized network layer security solution which address the routing anomalies in mobile ad hoc networks. The solution is based on distributed neighbour collaboration and information cross-validation, resulting in self-organized/self-healing network. Awerbuch et. al. [12] have proposed an on-demand secure routing protocol resilient to Byzantine failures. The authors use adaptive probing technique to detect the malicious links and multiplicatively increase their weights. These links are avoided by selecting the path with the least weight. Note that these protocols address the security issues in routing protocols of multi hop wireless networks which is a different problem from the one being addressed by this paper. The security mechanism proposed in this paper solves the security issues in channel assignment algorithms, a problem that has recently been identified and has not been addressed so far.

3 Problem Formulation

3.1 The Hyacinth Model

We cover the relevant details of the hyacinth model in this section and use the model in rest of the paper to show how the proposed security mechanism helps secure the channel assignment algorithms. Note that the proposed mechanism is general enough to be applicable on the most of the known channel assignment algorithms (See Section 4).

Hyacinth nodes use bandwidth usage, hop-count distance from the wired gateway and the channel assignment of the neighbouring nodes to decide the channel assignment for their interfaces. Interfaces of each node are divided into UP-NICs and DOWN-NICs used to communicate with parent nodes (closer to wired gateway than the node itself) and the child nodes (farther from gateway than the node) respectively. Channel assignment for UP-NICs of the node is the responsibility of its parent while the node assigns channels to its DOWN-NICs only. The channels used by the links closer to the wired gateway have higher priority. The cost associated with channel usage for a particular link is determined by the aggregate bandwidth usage of the channel within its interference domain. A node uses the least loaded channel

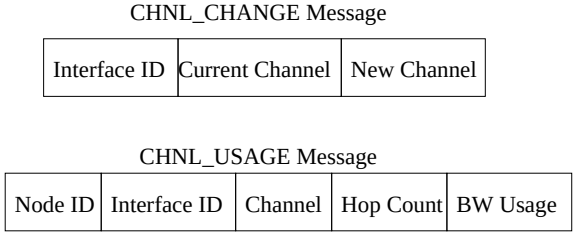


Figure 1: CHNL_CHANGE and CHNL_USAGE message format

that is not being used by any higher priority node within its interference domain.

Nodes periodically exchange their channel assignment and usage information with their interference domain neighbours using CHNL_USAGE message. The neighbour nodes, upon receiving the message, recalculate their channel assignment and update the assignments if required, in order to minimize the interference. When the node decides to change its channel assignment, it informs the affected child nodes of the change by sending the CHNL_CHANGE message. After successfully transmitting the message, the parent node switches to the new channel while the child node switches to the new channel upon receiving the message. The format of CHNL_USAGE message and the CHNL_CHANGE message is shown in figure 1. Note that all the known dynamic channel assignment algorithms require the mesh nodes to transmit the messages similar to CHNL_USAGE and CHNL_CHANGE for the purpose of information dissemination and channel change respectively. Therefore, The security mechanism applicable to hyacinth model will also be applicable to the channel assignment algorithms like [3, 4].

3.2 Attacks and Vulnerabilities in Channel Assignment Algorithms

The dynamic channel assignment algorithms assume that the mesh nodes are well behaved and do not have any malicious intentions. Based on the assumed trust, the information disseminated by the nodes is not verified for correctness. Further, in distributed channel assignment algorithms, each node makes an independent decision about its channel assignment and informs its neighbours about the decision which again is not verified. *The independent decision making and non-verification of the node decision and the information it transmits to neighbouring nodes are the vulnerabilities in channel assignment algorithms.* A new set of attacks that exploit these vulnerabilities in channel assignment algorithms for MRMC-WMN have recently been identified in [11]. The authors have exposed three attacks namely: Network Endo-Parasite Attack (NEPA), Channel Ecto-Parasite

Attack (CEPA) and Low-Cost Ripple Effect Attack (LORA), which can be launched with relative ease by a malicious node causing significant degradation in the network performance. The authors have shown that NEPA and CEPA can reduce the available network bandwidth to 65% and 40% of the total capacity respectively while LORA reduces the available capacity ranging from 60% to 90%.

These attacks exploit the security vulnerabilities in the following two ways: First, during parasite attacks (NEPA and CEPA), the malicious node *modifies the channel assignment* of its DOWN-NICs (transmits CHNL_CHANGE message) to higher priority channels but *does not inform its neighbour nodes* about the change (CHNL_USAGE message is not modified to incorporate change). This leads to the hidden usage of the higher priority channel and a degraded performance in terms of available bandwidth. Second, during LORA, the malicious node *does not change the channel assignment* of its DOWN-NICs (No CHNL_CHANGE message transmitted) but transmits the maliciously calculated information, informing its neighbours that *it has changed the channel assignment* of its DOWN-NICs (Malicious CHNL_USAGE message transmitted). This information triggers further channel assignment changes and forces the network into quasi-stable state. Note that in both of the above cases, the malicious node makes an independent decision about its channel assignment which is not verified by the neighbouring nodes. The information transmitted by the malicious node (CHNL_CHANGE and CHNL_USAGE messages) again is not verified.

4 Securing the Channel Assignment Algorithms

The proposed security mechanism addresses the security vulnerabilities mentioned in the previous section. The mechanism is based on the concept of neighbour monitoring to identify the malicious nodes in the network and leads to the prevention of the network from security attacks exploiting channel assignment vulnerabilities. Note that the neighbour monitoring has also been employed to detect the routing and packet forwarding vulnerabilities [13]. The mechanism proposed in this paper can possibly be combined with those solutions into a single solution for network layer attacks. The mechanism works as follows. Each node maintains the Bad-credit counter, with initial value of 0, for all the neighbouring nodes. The information disseminated by each node about its channel assignment and the decision of the node for its channel assignment is verified by one hop neighbours (connected nodes only). The anomalies detected in the disseminated information and the channel assignment of a particular node are reported to the interference domain neighbours of the node, marking the node as suspicious. The interference domain neighbours individually verify the correctness of the detected anomalies. If the anomalies are actually found, the Bad-credit of the

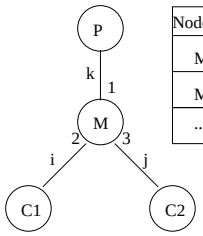
suspicious node is incremented upto a maximum upper bound and the information from that node is no longer trusted. If at a later stage in time, the misbehaving node starts behaving well, the Bad-credit of the node is decremented until it reaches 0 when the information from that node is trusted again by its neighbours. Note that the suspicious/malicious nodes are not removed from the network based on the misbehaviour in channel assignment. This is because of the fact that these nodes might still be performing useful functionality in terms of routing and packet forwarding. Detecting the routing and packet forwarding anomalies is beyond the scope of this work.

We use the hyacinth model (see section 3.1) and apply the security mechanism to the channel assignment algorithm to show the effectiveness of the mechanism. The security mechanism has two phases, the misbehaviour detection phase and the attack prevention phase which are described in detail in the subsequent sub sections with reference to hyacinth model.

4.1 Mis-behaviour Detection

The objective of the misbehaviour detection is to identify the anomalies in the channel assignment and the information transmitted by a particular node aabout its channel assignment. As mentioned in section 3.1, The CHNL_USAGE message is used by the nodes to disseminate their channel assignment information to the neighbouring nodes. Ideally, the neighbours of a particular node can perform channel scanning to detect the channel assignment anomalies of that node. In channel scanning, the neighbour node switches to all the available channels in the radio spectrum sequentially and listens at the channel for a short duration of time, to verify the information contained in the CHNL_USAGE message for correctness. However, channel scanning is a resource extensive process and performing the channel scan for every CHNL_USAGE message received by the node from neighbourhood is infeasible. We propose an efficient mechanism where the anomalies are detected by the child nodes of the suspected node using their own channel assignment and usage information. The information about detected anomalies is disseminated using a single MONITOR_REQUEST message. The neighbouring nodes of the suspected node only rely on their own channel assignment and usage information to verify the correctness of the CHNL_USAGE message and make an individual decision about the particular node.

We use the *Smart Children mechanism* for the purpose of misbehaviour detection. The mechanism gets the name because the child nodes detect the misbehaviour of the parent node. Child nodes, being the neighbours of the parent node, receive the CHNL_USAGE message from the parent node. For a child node to be connected to the parent node, its UP_NIC must be using the same channel as one of the DOWN_NICs of the parent node. Therefore, the child nodes can individually verify the correctness of the information



Node ID	Interface ID	Channel	Hop Count	BW usage
M	2	k	X	X
M	3	n	X	X
...	...	...	...	...

Malicious/Incorrect CHNL_USAGE Message

Figure 2: Malicious/Outdated CHNL_USAGE message transmitted from node M

contained in the CHNL_USAGE message. Consider the example shown in figure 2. Suppose the node M is the malicious node and it transmits the maliciously calculated or outdated CHNL_USAGE message shown in figure. When the child node C_1 receives this CHNL_USAGE message, it will find the discrepancy on first row of the message which indicates that the parent node is using channel k for interface 2. The anomaly is detected because the child node C_1 is connected with interface 2 of the parent node and is itself using channel i for this link suggesting that the parent node's interface 2 must use channel i for communication to occur. Similarly, the child node C_2 will identify the anomaly at second row of the message. Note that except the leaf nodes in the tree topology created by hyacinth, every node in the WMN has child nodes which can act as smart children. Further, the leaf nodes do not participate in channel assignment because they do not have any children. Therefore, the *smart children mechanism* can successfully detect the misbehaviour of the parent nodes in the entire network.

The neighbour nodes of a particular node (including child nodes) use Algorithm 1 upon receiving the CHNL_USAGE message, prior to executing the normal hyacinth procedure. Each node maintains the *Bad-credit* for each of its neighbours, where $0 \leq$*Bad-credit*$\leq K$. Suspicious count indicates the degree of misbehaviour of the node. Value of 0 means the node is well behaving and the value of K means the node is misbehaving while the intermediate values mark the node as suspicious. Note that K is the cap value for the *Bad-credit*, however, all values of *Bad-credit*> 0 are treated the same way in algorithm. The cap value ensures that no node is punished forever because of the misbehavior at a particular time. The selection of value K is left as a design parameter. The algorithm shows that the child nodes, upon receiving the CHNL_USAGE message, first check for the discrepancies. If the discrepancy is found, the MONITOR_REQUEST message is created which contains the identity of the suspicious node and the identified discrepancy. The child nodes broadcast the message to its own interference domain neighbours on all the available channels. If the CHNL_USAGE message received by the child node does not contain the discrepancy and if the

parent node is well behaved (*Bad-credit*= 0), the CHNL_USAGE message is processed normally. The neighbour nodes (other than child nodes) of the parent node wait for time T_w. If MONITOR_REQUEST message(s) is(are) received within the time duration and the request is verified to be valid, the *Bad-credit* is incremented by number of messages and the CHNL_USAGE message is discarded. If no MONITOR_REQUEST message is received and the parent node is well behaved the nodes process the CHNL_USAGE message according to normal hyacinth procedure.

Note that the neighbouring nodes do not need to collaborate in order to declare a node to be misbehaving. Each node individually decides if a particular node is misbehaving and acts accordingly by discarding the incorrect CHNL_USAGE messages from that node. Further, every node is being monitored by its child nodes, therefore, the neighbour node cannot falsely accuse a particular node in the network as malicious, otherwise its own CHNL_USAGE messages will be identified as malicious by the child nodes. The issue that needs attention is the fact that the child node may misbehave by falsely accusing the parent node as suspicious by transmitting MONITOR_REQUEST messages. We cater for this situation in Algorithm 1. On line 15 of the algorithm, the neighbouring nodes verify the requests by looking into the CHNL_USAGE message of the child node that sent the MONITOR_REQUEST. Comparing the UP_NIC information of the child node with the discrepancy listed in MONITOR_REQUEST message can confirm the correctness of the message. The verification of the MONITOR_REQUEST message ensures the protection of the parent node if the child node misbehaves by falsely accusing the parent. Another way of child misbehavior can be the transmission of same MONITOR_REQUEST message multiple times. However, only distinct MONITOR_REQUEST messages are selected by neighbouring nodes (Line 17 of the algorithm) discarding the duplicates of same message.

4.2 Attack Prevention

The algorithm defined in the previous section successfully detects the LORA attack as well as prevents the network the attack. This is because the malicious CHNL_USAGE message created by the malicious node is discarded by the neighbour nodes. Therefore, no channel adjustment is made based on the malicious CHNL_USAGE message. Consequently, no ripple effect is created in the network. The mechanism also successfully detects the parasite attacks (NEPA and CEPA) by detecting the anomalies in the CHNL_USAGE message. However, the mechanism is insufficient to prevent the WMN from these attacks because of the following fact. The parasite attacks are launched by the malicious node when it switches its DOWN_NICs to higher priority heavily loaded channels (i.e. by sending CHNL_CHANGE message to affected child nodes) but does not inform its neighbours of the change (i.e.

Algorithm 1 Response to the CHNL_USAGE message

```
1: if Child of the originating node then
2:    if CHNL_USAGE message has discrepancies then
3:       Create MONITOR_REQUEST message and broadcast.
4:       if Bad-credit<K then
5:          Increment Suspicious count.
6:       end if
7:    else if Bad-credit ≠ 0 then
8:       Decrement Bad-credit.
9:    else
10:      Process CHNL_USAGE using normal Hyacinth procedure.
11:   end if
12: else if Interference domain neighbour of the originating node then
13:   Wait for time T_w. {Expected time to receive MONITOR_REQUEST message}
14:   if MONITOR_REQUEST message(s) received then
15:      Verify MONITOR_REQUESTs using CHNL_USAGE messages from request
         sending nodes.
16:      if requests verified AND Bad-credit ≠ K then
17:         Increment Bad-credit by number of distinct messages received
18:         return
19:      end if
20:   end if
21:   if Bad-credit ≠ 0 then
22:      Decrement Bad-credit.
23:   else
24:      Process CHNL_USAGE using normal Hyacinth procedure.
25:   end if
26: end if
```

outdated CHNL_USAGE message is transmitted). Note that the smart children detect the outdated CHNL_USAGE messages only after the attack is launched. Further, the algorithm defined in previous section does not counteract the parasite attacks. In order to prevent the parasite attacks and we modify the hyacinth further by increasing the role of smart children.

In order to prevent the network from parasite attacks, the child nodes of the malicious node should be able to verify the CHNL_CHANGE messages from the parent. We base the verification of the CHNL_CHANGE message on the fact that the interference domain neighbours of the adjacent nodes (i.e. parent and child node) are approximately same. Therefore, the child nodes can partially verify the information held by the parent node. Based on the above fact, we modify the hyacinth procedure of channel change as follows. The parent node should transmit its channel assignment and usage information along with the CHNL_CHANGE message. The parent node then waits for the acknowledgement of the message. The child nodes, upon receiving the CHNL_CHANGE message, can verify most of the transmitted information by comparing it with its own channel assignment and usage information. The child node then calculates the approximate channel assignment based on the information provided by the parent node.

If the information about channel assignment and usage and the requested change in the CHNL_CHANGE message are found consistent with the information held and calculated by child node, the child node will reply with a POSITIVE_ACK message. Otherwise, the child node will reply with a NEGATIVE_ACK message. The parent node can only change the channel assignment if it successfully receives the POSITIVE_ACK.

The essence of the parasite attacks is the fact that the node makes independent decision about its channel assignment which is not verified (See section 3.2. Based on the above mechanism, the parent node is unable to change its channel assignment without agreement from child node (No independent decision). Child node only agrees to the channel assignment changes if it successfully verifies the correctness of the requested change. Therefore, the network can successfully be prevented from parasite attacks.

5 Simulation Results

We tested the performance of the proposed security mechanism through simulation based experiments using Qualnet simulator. We implemented the hyacinth channel assignment and routing algorithm [5] at the network layer of the protocol stack. The security mechanism was added to the hyacinth channel assignment algorithm and the performance was compared between the hyacinth model without attack, hyacinth model under attacks and the protected hyacinth model using proposed security mechanism under attacks. We also evaluated the overhead induced because of the security mechanism on the hyacinth model. We used a 36 node grid topology for physical placement of the nodes. The internode distance was adjusted to restrict the interference domain of the nodes to two hop physical neighbours. Two constant bit rate (CBR) traffic flows were used to generate the traffic.

The possible overhead of the security mechanism is primarily because of the MONITOR_REQUEST messages transmitted in response to the anomaly detection by the child nodes. Therefore, we evaluate the effect of the security provisioning on end-to-end propagation delay and the aggregate goodput of the network. The propagation delay did not change within one set of experiments. For example, the propagation delay, for a particular set of experiments, for both hyacinth without security mechanism and hyacinth with security mechanism under attack was 12.3 msec. Figure 3 shows the graph between the goodput acheived when the hyacinth model is used without security mechanism and the goodput achieved when hyacinth model is protected by the security mechanism and the network is attacked by LORA. The graph shows that the goodput is exactly same for both the cases. This is because the MONITOR_REQUEST messages are transmitted in response to the anomalies in CHNL_USAGE messages. The CHNL_USAGE messages are transmitted by the nodes every T_a units of time (See [5]). Con-

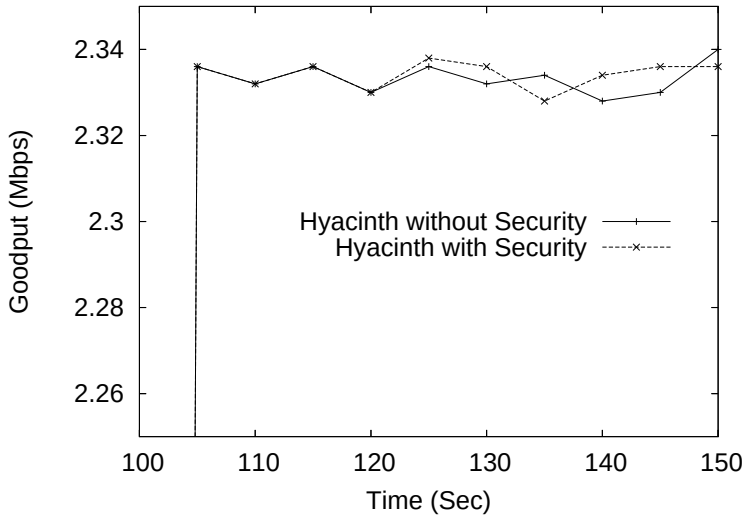


Figure 3: Effect of Security mechanism on Goodput of the Network

sequently, MONITOR_REQUEST messages are also triggered infrequently, causing negligible effect on goodput of the network.

Figures 4,5,6 shows the effectiveness of the security mechanism against the attacks NEPA CEPA and LORA. The figures show that the transmission starts at time 100 sec while the attacks NEPA CEPA and LORA are launched at time 115 sec in figures 4, 5 and 6 respectively. The graphs in these figures compare the goodput acheived when hyacinth channel assignment and routing algorithm runs without security mechanism and attacks, hyacinth under attack without security mechanism and hyacinth under attack with security mechanism. Figures show that the security mechanism provides complete protection against all three attacks and no decrease in the goodput is observed if hyacinth is protected by the security mechanism.

6 Conclusion and Future Work

In this paper, A security mechanism is proposed to secure the channel assignment algorithms. The mechanism addresses the security vulnerabilities that exist in most of the channel assignment algorithms. The effectiveness of the mechanism is shown using the example of hyacinth model. The simulation results show that the mechanism provides complete protection against the security attacks and the overhead caused is negligible. We intend to explore the following research directions in the future.

We intend to consider the effect of colluding malicious nodes on the security mechanism and the channel assignment algorithms. We also intend to

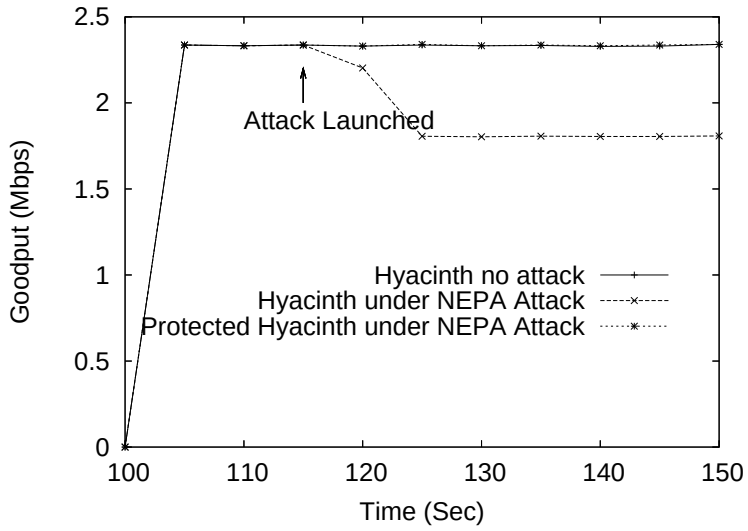


Figure 4: Goodput comparison for hyacinth model without protection and with protection using security mechanism under NEPA

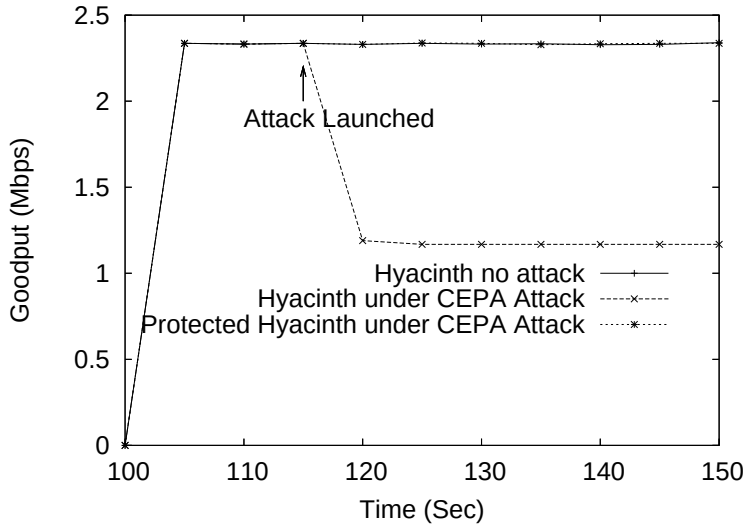


Figure 5: Goodput comparison for hyacinth model without protection and with protection using security mechanism under CEPA

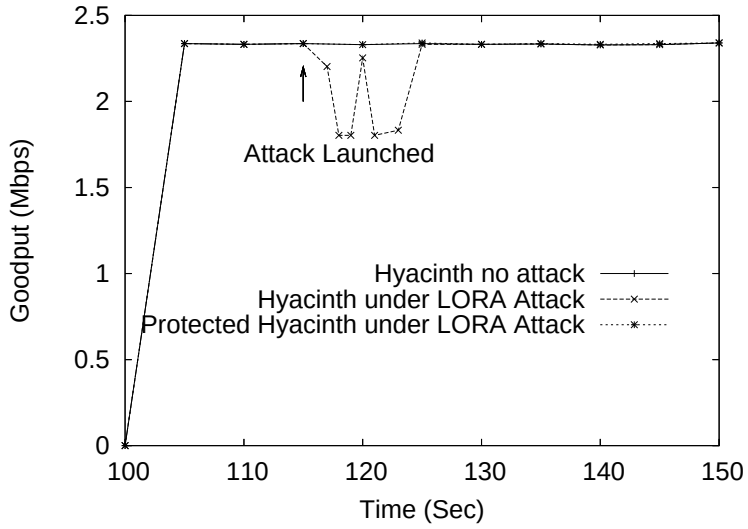


Figure 6: Goodput comparison for hyacinth model without protection and with protection using security mechanism under LORA

propose the security mechanism that can detect the malicious nodes exploiting the routing and packet forwarding functionality as well as the channel assignment algorithms.

7 Acknowledgements

This research is partially funded by Smart Internet Technologies - Cooperative Research Center (SIT-CRC).

References

[1] IEEE 802.11b, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[2] IEEE Standard 802.11a, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specificationsAmendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

[3] 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.

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

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

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

[7] Mansoor Alicherry, Randeep Bhatia, Li (Erran) Li. *Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks.* In proceedings of Mobile Computing and Networking. August 2005

[8] Paramvir Bahl, Ranveer Chandra, John Dunagan. *SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad-Hoc Wireless Networks.* In Proceedings of Mobile Computing and Networking. Sept 2004

[9] Pradeep Kyasanur, Nitin H. Vaidya. *Capacity of Multi-Channel Wireless Networks: Impact of number of channels and Interfaces.* In proceedings of Mobile Computing and Networking. August 2005.

[10] Paramvir Bahl, Atul Adya, Jitendra Padhye, Alec Wolman. *Reconsidering the Wireless LAN Platform with Multiple Radios.* In SIGCOMM Computer Communication Review (CCR), July 2004.

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

[12] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, Herbert Rubens. *An on-demand secure routing protocol resilient to byzantine failures*. In proceedings of the 3rd ACM workshop on Wireless security (WiSe 2002), Pages 21-30, September 2002.

[13] Hao Yang, Shu. J, Xiaoqiao Meng, Songwu Lu. *SCAN: self-organized network-layer security in mobile ad hoc networks*, Appears in: IEEE Journal on Selected Areas in Communications, Volume: 24, Issue: 2, pages 261- 273, Februry 2006.