Indian Journal of Communication Engineering and Systems (IJCES)
Vol.2.No.1 2014 pp 21-26.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

AVOID IMPACT OF JAMMING USING MULTIPATH ROUTING BASED ON WIRELESS MESH NETWORKS

N.Denif qury gordiliya, S.Mothilal Nehru
Department of Electronics and communication
Pallavan College of engineering
Chennai-25, India
denifff@gmail.com mothilalnehru@gmail.com

ABSTRACT

Various wireless mesh network standards have been actively constituted for the last several years. Because of its flexible network architecture, wireless mesh network can provide alternative paths even when some of wireless links are broken by node failures or intended attacks. Among various types of mesh network, we focus on the IEEE 802.11s based on the widely used Wi-Fi networks and its resiliency to jamming attack. In this demo, we show jamming effects on wireless mesh network and the performance of the hybrid wireless mesh protocol (HWMP) defined in IEEE 802.11s and our proposed jamming defense. Service continuity is a critical issue in wireless networks. Unfortunately, jamming attacks seriously threatens the continuity of wireless networks. The open nature of wireless mediums makes it vulnerable to any wireless capable devices. There are only few researches address the issue of how the service providers should deploy its topology or allocate its resources to minimize the impact of jamming attacks launched by malicious attackers.

Index Terms—Network Attack and Defense, Jamming Attack, Network Survivability, Resource Allocation, Incomplete Information, Wireless Mesh Networks (WMN)

1. INTRODUCTION

All As a result of the convenience and increasing importance of wireless network, service providers have to deal with a variety of wireless threats. There is a category of attacks that seriously jeopardize the continuity of wireless network, which are jamming attacks. Currently, there are several approaches to alleviate the impact of jamming although many constraints have to be fulfilled. Previous works have classified the countermeasures of jamming attack into attack mitigation and attack prevention most of them are mitigation techniques. There are two major difficulties of jamming prevention. First, the open nature of the medium makes it vulnerable to any wireless capable devices. Second, the channel had already been jammed when the defender aware of the presence of jamming attack. There is not any symptom before jamming attack launched. As a result, attack prevention is not an easy task. Since the impact of jamming attack cannot be avoided, intuitively, removing the jammers becomes a great option. Localization of wireless devices is not a brand new idea. There had been many works of localization, such as trilateral and trigonometric measurement, but the idea of jammer localization has not been addressed until recent years. There are two main categories of localization techniques. In signal processing localization techniques require special, additional hardware to achieve the goal, such as ultrasound, infrared or laser infrastructures. Received signal strength (RSS) based techniques require measurement of the RSS and have to deliver the information out of the jammed area. Therefore, the techniques of both categories have some limits. However, there are only few works address the issue of how the service provider should deploy nodes or allocate resources to minimize the impact of jamming attacks launched by malicious attackers. Thus, an attack and defense scenario in wireless mesh network which the defender attempt to maintain the level of quality of service when attackers try to launch malicious attacks and

jamming attacks to maximize service disruption is considered. Both defender and attackers have budget constraint and various strategies to choose.

Wireless mesh network enables a flexible network structure by providing multi-hop connectivity between the communicating ends which are distant away from each other. In addition to this extended wireless coverage, wireless mesh network also provides high service availability through the multiple routes, thus making the network more reliable against the single point of failure. Over the past decade, many mesh standards constituted to support various types of wireless networks show high demand on this flexible network architecture.

The path redundancy supported by multiple routes manages to mitigate the small scale link or node failure. However, wireless mesh network can suffer from large scale network failure by intentional attacks such as jamming. Specifically, an adversary can cut off some network flows in the network by emitting intentional noise to interrupt the legitimate communication. Although jamming is traditionally perceived as a physical-layer attack, an attacker can use the cross-layer information to more effectively interfere with the communication over the entire network. Therefore, this type of attack should be considered as a serious network layer threat which significantly degrades the routing performance in wireless mesh network. Among many mesh protocols, we focus on the hybrid wire-less mesh protocol (HWMP) in the IEEE 802.11s standard which is based on the popular Wi-Fi networks. After reviewing widely used network simulators such as ns2 and Opnet, we realize that no network simulator can suffice our requirements to study the jamming effects on wireless mesh network. Most network simulators emulate either physical layer or link/network layer, but not both of them sufficiently. Thus, we decide to build an easily configurable network simulator to observe the cross-layer jamming effects on the IEEE 802.11s mesh network.

In this demo, we provide a simulator to study the jamming effect on wireless mesh network and the network resiliency by mesh protocols. Furthermore, we propose a jamming defense mechanism and show its performance under jamming on our simulator.

2. METHODOLOGY

A. Network Survivability

Describing the degree of ability of a system providing services under an abnormal condition is an important criterion. Survivability is one of the pioneer studies in military since the failure of military systems could be fatal. Though this metric has been applied to a variety of fields, such as computer networks, ecological and biological systems, the definition of survivability has not been unified. In this paper, the definition of survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

Many other works studying survivability adopt the concept of Contest Success Function (CSF) to determine the outcome of an attacker launching a malicious attack on the target node. The idea of CSF is originated from economy theory. It models the success probability of participants in a battle as a function of all players' efforts. Generally, the attackers allocating more resources on the target have higher success probability.

B. Deception Based Defence Mechanisms

A computer system designed to deceive malicious attackers to improve the current network system survivability is one of deception mechanisms. Learning the behavior of attackers, act as a false target, or waste the resources of attackers are possible objectives. In wireless networks, generally, there is no difference of the function of deception mechanisms between wired and wireless networks. Yet, Misra, proposed a novel technique which applies deception based resources to prevent wireless communication channel from being jammed, this provides a new manner to enhance the robustness of wireless networks.

C. Malicious Jamming Attacks

Jamming attack can be viewed as a subclass of denial of service attacks. The objective of such attacks focuses on interdiction of any communication on the targeted channels or a range of frequency. Most of the network types of previous researches which address the problem of jamming attack are wireless sensor networks (WSNs). The reason is probable that WSNs have been used in many safe-critical systems, such as monitoring of patients or children. Therefore, the survivability requirement of these systems is raised since in such systems even a temporal disruption of the proper data stream may lead to disastrous results. Nevertheless, jamming attacks may exist in any category of wireless networks. Thus, no matter what type of wireless network is, the threat of jamming attacks should not be ignored. W. Xu had reviewed a wide range of jammers and provided a summary which listing four type of jammers that have been proven to be effective.

C. Jamming Countermeasures

The general approach of jamming countermeasures includes three steps, attack detection, attack prevention and attack mitigation. Detection of jamming attacks can be done through observing quality of service. If there are lots of unreachable

mesh routers in the same neighborhood, the probability of being jammed is high. S.Misra, proposed an attack prevention technique. We define honey nodes as secondary interfaces present on base-stations which guard the frequency of operation of the actual communicating nodes by sending out a fake signal on a nearby frequency to prevent the attack by deceiving the attacking entity to attack the honey node. Though the technique does prevent jamming attacks in some case, however, the effectiveness greatly depends on the behavior of jammers and the number of jammers in the network. Existing attack mitigation techniques have some limitations.

Spatial Retreat requires jammed nodes to physically move away from the jammed region. In Jammed-Area Mapping method, jammed-area will be mapped out. Thus, part of the network is inoperable. Channel Surfing, as stated in, is able to assure service continuity with minimal service disruption and additional requirement comparing to former techniques. Unlike Spread Spectrum techniques, Channel Surfing does not have to consume a large amount of bandwidth. In addition, it can apply to wireless infrastructure and wireless infrastructure-less (ad–hoc) networks. Consequently, this technique is widely applied.

D. Jammer Localization Schemes

Localization of jammers provides some addition strategies for network operator. In the effect of jamming can be neutralized through human intervention, or provide information for routing protocols to redesign a route that avoids jammed areas. Generally, there are two restrictions of jammer localization:

First, extra hardware is required. Second, disturbed network communications makes it impossible to transmit signal out of jammed areas. To address these difficulties, K. Pelechrinis, proposed a lightweight jammer localization technique, which based on the idea PDR has lower values as we move closer to the jammer. But this approach only finds out the locations of nodes which reside on the boundary of jammed range, which is not able to precisely indicate the location of jammers. Range-free approaches, such as Centroid Localization (CL) and Weighted Centroid Localization (WCL), do not rely on the property of received signals. The positions of jammers are derived from the position of jammed nodes. H. Liu, proposed a novel approach, Virtual Force Iterative Localization (VFIF), which is less sensitive to node density. In this approach, another category of nodes which are useful in jammers localization, boundary nodes, is recognized. A boundary node is not jammed, but part of its neighbor is jammed. This idea is further extend. The proposed algorithm uses least-squares approach (LSQ) to localize the jammer by exploiting jammed nodes hearing ranges based on free space propagation model.

3. SIMULATION ASSUMPTIONS

We describe the path selection protocols used in wireless mesh network and our simulation setup. We then briefly describe our jamming defense mechanism.

A. IEEE 802.11S Mesh Protocol

We assume a wireless mesh network consists of widely deployed Wi-Fi nodes. The network follows the IEEE 802.11s WLAN mesh network standard. The network purely consists of mesh clients without any root node, which is similar to the non-hierarchical ad hoc network configuration.

The IEEE 802.11s mesh network standard adopts a mesh path selection protocol HWMP. It consists of the on-demand mode, which is similar to Ad Hoc On-Demand Distance Vector (AODV) protocol (IETF RFC 3561), and the proactive mode, which builds a tree structure by a root mesh station. Both modes are used concurrently. In HWMP, a node selects a path based on the airtime link metric which includes the link speed and the frame error rate (FER).

HWMP itself does not support a multi-path selection mechanism. When the jamming attack is launched in wireless mesh network, HWMP updates forwarding path after a source node detects the link failure by jamming and builds a new path by broadcasting path request message into the network. Moreover, the airtime link metric is based on the link speed affected by link adaptation algorithm and the FER, and they are generally lagging indicators to reflect the attacked link status.

B. Simulation Setup

Fig. 1 shows the working example of our wireless mesh network simulator. In this example, two jammers are interfering with the mesh network which consists of 50 wireless nodes. We implement the on-demand path selection of HWMP in IEEE 802.11s. The simulation follows the line-of-sight (LOS) signal propagation model to calculate received signal strength in each node. We set all the antenna gains to 1, and set the path-loss exponent to 2.4. On the center frequency of 2.4 GHz ISM band, the wavelength is set to = 0:1249m. We also set the clear channel assessment threshold to -82 dB, the noise floor to -95 dB. In accordance with the standard IEEE 802.11g parameters, each node also changes its rate from BPSK 1/2 to 64-QAM 3/4 depending on the signal to interference noise ratio observed from previous frame transmission.

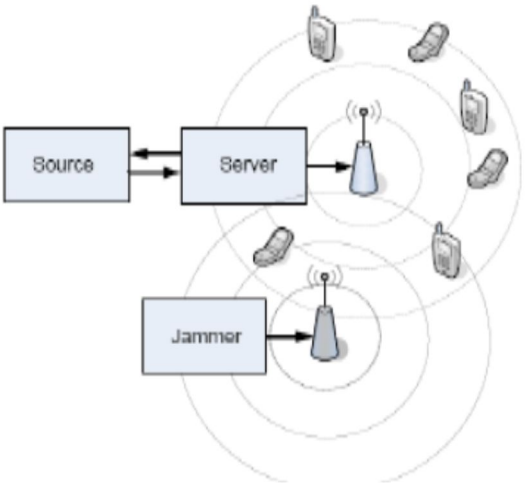

Figure. 1: Jamming effect on wireless mesh network

4. PROBLEM FORMULATION

For service providers, it is extremely important to assure the quality of service. Thus, in this work, the problem of jamming attack in wireless mesh network is addressed. There are two roles, the defender and attackers, in this problem. For the defender, deploying mesh routers to construct an infrastructure based wireless mesh network is the first step before providing services. Since attackers' objective is to jam the network, before doing that, topology information gathering is a critical task. Accordingly, the defender has to appropriately allocate defense resources, both deception based and non-deception based resources, to maintain the level of Quality of service. In addition, attackers have different attacking strategies corresponding to distinct goals.

On the contrary, to maximize the effect of jamming attack, attackers have to gather topology information first. Obtaining complete information of target network before launching jamming attack is not realistic. Consequently, figuring out the spread of mesh routers and related defense information by compromising devices is an essential step. In general, attackers' actions can be classified into two periods: "Preparing Phase" and "Attacking Phase". The former is the stage in which attackers try to collect information from the network; then attackers launch jamming attack in Attacking Phase.

Likewise, the defender tries to deploy defense resources effectively to minimize the effect of jamming attacks. "Planning Phase" is the stage for the defender to deploy resources before attackers invade the network. In most cases, when the defender is aware of the presence of jamming attacks, the Quality of service level has already declined.

As a result, defense resources have to be deployed before jamming attacks occurring. Hence, not only node compromising attempts but also the negative effects caused by jamming attack are serious problems for the defender to handle in Defending Phase. The time sequence of those phases mentioned above is illustrated in figure 1. In order to clearly detail the attack and defense scenario addressed in this paper, both defender and attacker's perspectives are discussed in following sections respectively.

A. DEFENDER PERSPECTIVE

In this paper, infrastructure-based network is the main concern, and the security issue of jamming attacks in WMNs is addressed. In order to provide service as well as maintain the Quality of service level, there are four types (but not limit to) of nodes in the network environment, including base stations (BSs), mesh routers, honey nodes and jammer locators. The usage of defense budget in Planning Phase is not only to construct the nodes mentioned above but also to deploy three categories of defense resources:

- ***Topology planning:***
  The defender has to spend part of the finite budget to build the BSs, purchase mesh routers and deploy them in the field for providing services.

- ***Non-deception based defense resources planning*:**
  Decisions made in this category of resources including proactive defense resources and localization resources. Proactive defense resources stand for techniques that prevent nodes from being compromised, such as firewall, antivirus software and introduction protection system (IPS). Localization resources mean those can be applied to localize the jammers.

- ***Deception based defense resources planning***
  This category of resources is not only capable to deceive attackers and jammers but also waste attack resources. Mitigating the impact as well as reduce the duration of jamming attacks in wireless networks is another purpose.

B. DEFENDING STRATEGY

In defending phase, there are two strategies, which are population re-allocation and jammer removing. The former strategy can reduce the effect of jamming attack. When the defender knows that there is an attacker who tried to compromise a certain node, he/she can re-allocate the population on the target and its neighbors to ease the negative effect caused by the jamming attack. As for jammer removing, there is a sub-decision to make, which is the priority of jammer removing. There are two

possible heuristics, importance oriented and difficulty oriented. The intention of importance oriented strategy is to retrieve Quality of service level. The defender determines the sequence of jammer removing by the importance of corresponding jammed nodes despite of the complexity of the network environment. Regarding difficulty oriented strategy, however, the defender removes the jammers according to the difficulty of jammer removal.

C.ATTACKER PERSPECTIVE

For describing attackers, several attributes are considered, including budget, capability, aggressiveness, goal, strategy and preference.

- ***Budget***

To maximize the impact of jamming attacks, Acquisition of the information regarding topology and defense resources allocation is the primary task. Owing to limited budget, the balance of allocating resources on node compromising and jammer purchasing is important.

- ***Capability***

This attribute stands for how good an attacker is on attacking. The capabilities of compromising nodes, seeing through false targets and fake routing table information are taken into consideration. Experienced attackers are more skillful in node compromising. In addition, they are more likely to penetrate if the compromised node is a honey node. While the attacker aware of the gained information might be artificial, they can choose not to make decision depending on it or try to act in reverse.

- ***Aggressiveness***

Aggressiveness describes the degree of risk acceptance for an attacker. Generally, an attacker which is risk tolerant is more likely to take chances on uncertainty. For instance, he may spend less on each attempt of node compromising attempt in spite of the fact the probability of success is much lower. On the other hand, attackers who tend to avoid risk will spend more to ensure the outcome. In other words, aggressiveness is the wanted compromise success probability of an attacker.

D. GOAL, STRATEGY AND PREFERENCE

The behaviors of attackers are complicated since every single decision depends on their goal, strategies, preference of next hop selecting criteria, information gathered and the network environment at the instants. In this paper, some possible goals and strategies are considered for attackers:

- ***Goal***

Maximizing attack effectiveness and maximizing jammed range are two different goals. The attackers pursuing the first goal tend to increase the difficulty of jammer removal to maximize attack effectiveness. Thus, they prefer to buy high quality jammers and spend more resources on compromising nodes which may contain valuable information, such as those with high defense strength or with high traffic amount. As for attackers chasing for maximizing jammed range, they do not care the effectiveness of jammers; As a result, they purchase lots of cheap jammers and try to jam as many nodes as possible. In this case, they are less willing to spend large amount of budget on node compromising.

- ***Strategies***

The effectiveness of jamming attack is affected by strategies of the defender as well as attackers. As Fred Cohen said, Attackers can select from many techniques for their attack, but the problem is when and which technique they should choose. Consequently, based on several possible strategies are summarized for attackers in attacking phase, including aggressive, least resistance, stealthy, easiest to find, topology extending, and random strategies.

Attackers applying aggressive strategy prefer to compromise nodes with high defense strength since those are more likely to be important nodes. Regarding utilizing least resistance strategy attackers, they target nodes which are easiest for them to compromise. In this case, ideal nodes may be those with low defense resources. Some attackers choose to conceal themselves to avoid being detected. They prefer to apply stealthy strategy. The ideal nodes are those with low traffic rate since they are seldom used.

As to easiest to find strategy, its characteristic is to choose the most obvious node, such as high traffic or signal strength. In such way, the attackers can spend less time on searching for next victim. The purpose of topology extending strategy is to extend its knowledge of underlying topology for further decision making, for instance, to predict the real location of the BSs. Some attackers just try whatever they happen to come across as an idea on any given day. This is called random strategy.

In attacking phase, initially, the attackers are able to gain some “Surface Information” through the wireless medium, such as defense strength, signal strength or traffic amount to make preliminary decisions. Attackers then apply different strategies to achieve their goal. With different strategies, corresponding preference of next hop selecting criteria are distinct. For example, an attacker who tends to maximize jamming effectiveness may choose “Aggressive” strategy since he believes the nodes with highest defense strength must contain valuable information. Find strategy just selects the nearest node.

5. DEMO SPECIFICATION

The wireless mesh network simulator is fully coded with a visual studio environment (visual basic .net). The script also uses the simulator can randomly generate a mesh network and store it into a text file. For the ease of demo, we will use the pre configured text files for the mesh network and the jamming model. The simulator includes simple GUI which any audience can easily execute the path selection simulation. The simulator animates the frame propagation with the text information.

6. RESULTS & DISCUSSION

Different resource allocation schemes lead to diverse results. In this section, Initial allocation heuristics are discussed. For wireless service providers, the distribution of user is one of the most important issues. However, it is almost impossible to acquire this information in advance. As a consequence, two other important factors which can be derived instantly from the topology are proposed.

6. CONCLUSION

We show the jamming effects on wireless mesh network and how the standard HWMP defined in IEEE 802.11s and the proposed distributed path selection protocol achieve the network resiliency against jamming attack in this demo. Our wireless network simulator will help understanding how each path selection mechanism works and how good the performance of the proposed mechanism is. We expect that this tool will also be useful for related studies.

ACKNOWLEDGMENT

This work was supported by Mr.P.SENTHIL NATHAN, INNOTRON technologies, kanchipuram.

REFERENCES

[1] W. Xu, “jamming sensor networks: attack and defense strategies”, network, IEEE, vol.20, pp.41-47, 2006

[2] H. Liu “localizing jammers in wireless networks, “in pervasive computing and communication, 2009.percom2009.IEEE international conference on, 2009, ppl.1-6

[3] R.J. Ellison, survivable network system: An Emerging Discipline," Technical Report CMU/SEI-97-TR-013, 1997 (Revised: May 1999).

[4] K.Hausken and G. Levi tin, "Protection vs. false targets in series systems, “Reliability engineering and system safety, vol. 94, pp. 973-981, 2009.

[5]A.Mpitziopoulos, “A survey on jamming attack and countermeasures in WSN’s” communication surveys and tutorials, IEEE, vol.11, pp.42-56, 2009

[6] G. Levi tin and K.Hausken, “False target efficiency in defense strategy, “European Journal of Operational Research, vol.194, pp.155-162, 2009

[7] M.Sink. The Use of honey pots and intrusion detection
Available:
http://www.lib.iup.edu/comscisee/SANSpapers/msink.htm

[8] P.E.Heegaard and K.S.Trivedi, “Network survivability modeling, “computer networks, vol.53, pp. 1215-1234, 2009