SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2009; **2**:373–391
Published online 6 July 2009 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.127

Collaborative attacks in WiMAX networks

Bharat Bhargava[1], Yu Zhang[1*,†], Nwokedi Idika[1], Leszek Lilien[2] and Mehdi Azarmi[1]

[1] *Purdue University, West Lafayette, IN 47907, U.S.A.*
[2] *Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008-5200, U.S.A.*

Summary

In this paper, we discuss security problems, with a focus on collaborative attacks, in the Worldwide Interoperability for Microwave Access (WiMAX) scenario. The WiMAX protocol suite, which includes but is not limited to DOCSIS, DES, and AES, consists of a large number of protocols. We present briefly the WiMAX standard and its vulnerabilities. We pinpoint the problems with individual protocols in the WiMAX protocol suite, and discuss collaborative attacks on WiMAX systems. We present several typical WiMAX attack scenarios, including: bringing a large number of attackers to increase their computation power and break WiMAX protocols; assembling a sufficient number of attackers to influence the decision-making of core machines, which includes routing attacks and Sybil attacks; and exploiting implementations that do not conform to the WiMAX specification completely, causing interoperability problems among various protocols, including the ones in typical WiMAX/WiFi/LAN deployment scenarios. We present theoretical models and practical solutions to profile, model, and analyze collaborative attacks in WiMAX. We employ attack graphs to do vulnerability analysis. Experimental results verify our models and validate our analysis. Copyright © 2009 John Wiley & Sons, Ltd.

KEY WORDS: WiMAX; security; collaborative attacks; computer networks

1. Introduction

Security is a key challenge in today's Internet since most Internet protocols were designed without considering any prevention against miscreants. In addition, many emerging technologies make the Internet even more vulnerable. Wireless networks represent an important example of such scenarios where capturing and forging packets is relatively easy. Attacks against networked systems are becoming more complex and powerful. Individual attackers can collaborate to cause more problems for the intruder-identification and defense mechanisms. Models for cooperation need to be studied along with defense mechanisms. We also need to characterize various types and models of attacks through studies of detailed attack logs that are available from various intrusion detection systems (IDS).

In this paper, we study the impacts of collaborative attacks on throughput, data delivery, and routing in the worldwide interoperability for microwave access (WiMAX) scenarios.

Traditionally users employ one of the following three approaches to access Internet:

[*] Correspondence to: Yu Zhang, Department of Computer Sciences, Purdue University, 300 University Street, West Lafayette, IN, USA.
[†] E-mail: zhangyu@cs.purdue.edu

- Wired access, such as DSL.
- Telephone access (dial-up)
- IEEE 802.11 wireless access, such as in WiFi Hotspots.

However, each of the above approaches has its own drawbacks: the wired access requires a physical connection; the dial-up telephone access provides limited bandwidth; and the IEEE 802.11 wireless access was designed for small areas and provides limited coverage. The WiMAX (IEEE 802.16) standard, integrating the benefits of broadband and WiFi, provides high-speed wireless access with a broad coverage. Mobile devices, such as cellphones, can employ the 'mobile WiMAX' technology to access Internet (using the IEEE 802.16e standard, which is a mobility-supporting amendment to IEEE 802.16).

As shown in Figure 1 [1], WiMAX uses towers and receivers to transmit information. The maximum range of WiMAX, around 30 miles, is much larger than the range of WiFi. The bandwidth of WiMAX with the 802.16m standard (1 Gbps) is also expected to be much higher than for WiFi. The IEEE 802.16 WiMAX standard incorporates a large number of existing technologies that have been proven robust. Hence, the WiMAX network should be immune to a large number of attack methods.

The current approaches to security in WiMAX systems deploy individualized security solutions. For example, antiviral software is used to defend against worms and viruses, intrusion detection tools guard against scanning and denial-of-service (DoS) attacks, firewalls aim to protect against unwanted connection attempts, and mail filtering tries to foil spam and phishing attempts. Accordingly, most research done today also focuses on improving these individual tools.

An important piece missing from the current research is understanding of ways in which attackers can collaborate when targeting WiMAX networks.

Collaborative attacks are those launched by multiple malicious adversaries that synchronize their activities to accomplish disruption, deception, usurpation, and disclosure against some targeted organizations or network entities. Collaborative attacks may cause more devastating impacts since they combine efforts of many attackers. For instance, an illegal DNS zone transfer (typically used to reveal the IP addresses of hosts present in an organization) followed by scanning attempts to find vulnerable machines can be a coordinated attack by attackers with varying expertise [2]. The vulnerable machines, misled by the attackers, could then initiate web requests to download backdoors from malicious sites, and join attacker's army of zombie

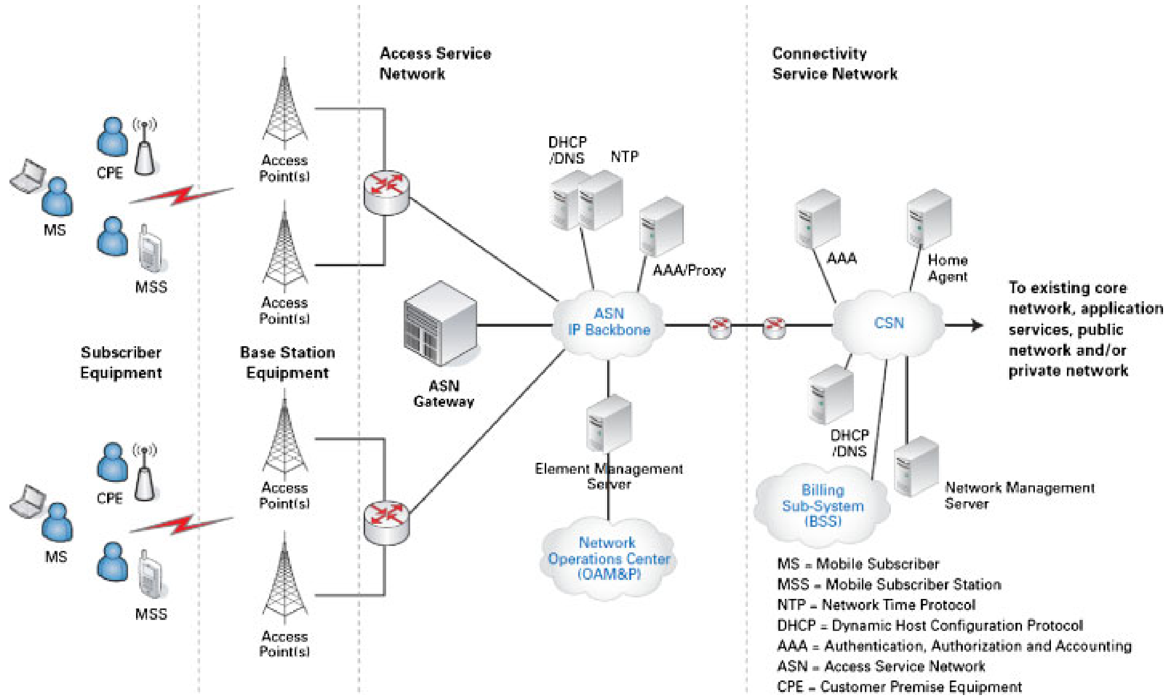
Access Service Network
Connectivity Service Network
CPE
MS
MSS
Access Point(s)
Access Point(s)
Subscriber Equipment
Base Station Equipment
DHCP /DNS
NTP
AAA/Proxy
ASN IP Backbone
ASN Gateway
Element Management Server
Network Operations Center (OAM&P)
AAA
Home Agent
CSN
To existing core network, application services, public network and/or private network
DHCP /DNS
Billing Sub-System (BSS)
Network Management Server
CPE
MS
MSS
Access Point(s)
Access Point(s)
MS = Mobile Subscriber
MSS = Mobile Subscriber Station
NTP = Network Time Protocol
DHCP = Dynamic Host Configuration Protocol
AAA = Authentication, Authorization and Accounting
ASN = Access Service Network
CPE = Customer Premise Equipment

Fig. 1. Typical WiMAX scenario [1]. Motorola and the stylized Ⓜ logo are registered in the US Patent & Trademark office. All other product or service names are the property of their respective owners. © Motorola, Inc 2009. All rights reserved.

DOI: 10.1002/sec

machines. Similarly, spammers could collaborate with other attackers who control a set of Internet routers to install hijacked routes temporarily. These routes can then be used to send spam and phishing emails without fear of detection. As yet another example, identification of malicious activity in the mobile *ad hoc* networks (especially the IEEE 802.16j multi-hop WiMAX network) is hard when one node misbehaves in route formation [3,4]. If multiple nodes act maliciously, simultaneously, or alternately, the schemes to deal with them become very slow and difficult to use at most nodes.

The WiMAX standard employs a number of robust security features, including the DES and AES encryption standards. The standard imposes security processors on base stations. End-to-end communication is secured by the data over cable service interface specification (DOCSIS), which defines the baseline privacy interface plus (BPI+) specifications.

Although individual protocols in the WiMAX protocol suite are believed to be secure, WiMAX is not completely secure under collaborative attacks. For instance, WiMAX is vulnerable to the following three types of collaborative WiMAX attacks:

(a) One can bring a large number of attackers to increase the computation power. Attackers have employed this approach in the past. For instance, in 1999, more than 100 000 PCs were used to crack the DES challenge of RSA [5].
(b) One can assemble a reasonable number of attackers to influence the decision-making of core machines, these include routing and Sybil attacks in the WiMAX.
(c) One can look for implementations that do not conform to the specification completely, and issues that arise during the interoperation of various protocols, including the typical WiMAX/WiFi/LAN deployment scenario.

In addition, collaborative attacks can happen in other forms, such as the compromise of individual nodes. Hence, a complete understanding of collaborative attacks in the WiMAX is needed.

In this paper, we characterize, model, and analyze vulnerabilities and collaborative attacks in the WiMAX systems. We develop and enhance the science to deal with such attacks through theoretical models and experiments. The rest of the paper is organized as follows. Section 2 discusses related work. Section 3 reviews vulnerabilities in WiMAX. Section 4 discusses ways to leverage attack graph in WiMAX. Section 5 presents how to profile, model, and analyze collaborative attacks in WiMAX. Section 6 concludes our paper.

2. Related Work

2.1. Prior Work on Collaborative Attacks in Internet and WiMAX

Many researchers have characterized specific Internet attacks or phenomenon using one or more sources of data. For instance, Reference [6] has characterized spammer behavior. References [7,8] focus on specific worm outbreaks and Reference [9] characterizes DoS attacks in the Internet. Very few works have focused on correlating various attacks. One of them is Reference [10], in which the authors analyze data, logged by the Dshield project [11] on a large number of IDSs, to find out related, possibly collaborative, attacks. Reference [12] focuses on the problems of IEEE 802.16d, including ranging response (*RNG-RSP*) and authorization request. References [13,14] introduced the disclosure of security context during the initial network entry, the lack of secure communication in access networks, and the lack of support for integrity protection of management frames.

2.2. Coordinated Attacks of SYN Floods and Slammer Worms

A SYN flood attack is launched by sending more TCP connection requests than a target machine can process. A slammer worm uses random scanning to find and infect susceptible hosts.

Both the SYN flood attack and the slammer worm, even if launched separately, can cause a significant damage [7,15]. If they are launched together in a coordinated way, the resulting consequences will be more devastating: the SYN flood attack will effectively block TCP connections while the Slammer worms will propagate via UDP connections. The coupled attack is not only more powerful but also more difficult to deal with.

2.3. Sybil Attacks

Douceur [16] discusses Sybil attacks, in which a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. In this way, the malicious nodes can control the decisions of the system, especially if the decision process involves voting or any other type of collaboration.

DOI: 10.1002/sec

Trust relationships can be created in social networks to limit the number of nodes a malicious node can create. In such an approach, we need to consider trust, security, and privacy issues together, and in a systematic way, preferably at the policy level. In addition, a deliberate collaboration model is needed.

Generic Sybil attacks can be found in Internet as well. For example, BGP would greatly suffer from the aforementioned attacks. Researchers at UCLA have proposed ways to detect invalid routing announcements in RIP [17] but mere detection cannot solve the problem thoroughly. Responding after detection and defending against such attacks, possibly coordinated, remains a challenge.

2.4. Modeling Multistep Cyber Attacks for Attack Scenario Recognition

Cheung *et al.* [18] state that many cyber attacks can be decomposed into multiple sub-attacks. The authors develop methods and a language for modeling multistep attack scenarios based on typical isolated alerts about attack steps.

The idea of trust relationship [16,19,20] is used to limit the number of clones a malicious node can have and defend against Sybil attacks. However, no collaborative model is discussed in these works. In the RIP protocol [17], detection of invalid routing announcements has been suggested. The response after detection and ways to defend against such attacks remains a challenge. Many approaches are proposed. A stochastic model of collaborative internal and external attacks is used in Reference [21]. Data routing information (DRI) table and cross checking [22] can be used to identify multiple cooperating black hole nodes. An on-demand routing protocol for ad hoc wireless networks can provide resilience to Byzantine failures caused by individual or colluding nodes [23]. A signature-based model can be used to detect collaborative attacks [24]. Clustering and merging functions can be used to recognize alerts that correspond to the same occurrence of an attack and create a new combined alert [25]. A collaborative system using Multicast, annotated topology information, and blind detection techniques can be used to detect distributed DoS (DDoS) attacks [26]. Hidden Markov models can be used to detect collaborative attacks [27].

3. Vulnerabilities in WiMAX

IEEE 802.16 standards specify some powerful security controls, including PKMv2, EAP-based authentication, and over-the-air AES-based encryption. But secure technology does not, in itself, constitute a secure end-to-end network, and, consequently, WiMAX presents a range of security vulnerabilities.

In the next subsections, we discuss some of potential vulnerabilities of IEEE 802.16 standards. Although the individual protocols in the WiMAX protocol suite are reasonably secure (except DES), WiMAX is not completely secure under collaborative attacks. We will investigate below some types of collaborative attacks on WiMAX.

Supporting DES is one of the most obvious vulnerabilities in WiMAX standards. DES can be broken by collaborative attacks. First, the attackers can compromise other systems and then use them in their attacks as subordinate zombies. For instance, more than 100 000 PCs were used to crack a system in the DES challenge of RSA in 1999 [5].

3.1. Vulnerabilities in IEEE 802.16-2004 Standard

We can not focus only on security improvements done in new drafts of the 802.16 standards since most of the current WiMAX equipment is based on the old IEEE 802.16-2004 standard. In the past few years, several vulnerabilities in IEEE 802.16 network architecture have been discovered [12,28]. The vulnerabilities analyzed here in some detail are: ranging response (*RNG-RSP*) and authorization request.

Based on the IEEE 802.16-2004 standard, the ranging response (*RNG-RSP*) is a process of acquiring the correct timing offset and power adjustments such that subscriber station (SS) transmissions are aligned to a symbol that marks the beginning of a mini-slot boundary in the physical layer.

During the first part of WiMAX network initialization, when SS tries to join a WiMAX network for the first time, it sends a ranging request (*RNG-REQ*) message to the base station (BS). The message asks for following information: SS requests transmission timing, power, frequency, and burst profile information. After receiving the *RNG-REQ* message from SS, BS sends its *RNG-RSP* message to SS. The first security problem is as follows: the *RNG-RSP* message can do more than merely fine-tune SS transmission times; BS can use this message to direct SS to change its timing, power level, offset frequency, ranging status, and other ranging parameters [29]. This capability can cause a lot of abnormal events if malicious activity is involved. Since ranging response messages are not encrypted or authenticated in the IEEE 802.16-2004 standard (in

DOI: 10.1002/sec

contrast to IEEE 802.16e-2005), malicious attackers can easily modify ranging messages. This type of attack is very easy to use as a part of DDoS or other collaborative attacks. For instance, the most popular exploitation is to send *RNG-RSP* messages with the *ranging status* field set to 2, which means 'abort'. When SS receives such a *RNG-RSP* message during a ranging procedure, the ranging request will not be answered with an initial value of a ranging status. Therefore, this vulnerability, interrupting a normal SS ranging request process, can be used in a DoS or DDoS attack.

Attacks using *auth request* message have their origin in a vulnerability of the *authorization state machine* in PKM. In the authorization request attack, the message sent at the beginning of a the process of *authorization key* exchange includes security-related contents, such as SS certificate, security capabilities, security capabilities digest, and security association identification (*SAID*). The aim of *authorization request* messages are used to negotiate a cryptographic suite and request an authorization from BS. If the shared security capabilities are not the same for SS and BS, BS sends a *perm auth reject* message to SS. Upon receiving a *perm auth reject* message, SS goes into the silent state of its authorization state machine. Malicious attackers can modify security-capability attributes in an *auth request* message in such a way that BS infers that SS cannot provide an appropriate cryptographic suite; thus BS causes a permanent error condition by sending the *perm auth reject* message. Fortunately, all PKMv2 messages in the mobile WiMAX standard IEEE 802.16e-2005 are protected by message authentication schemes with the *HMAC-CMAC* tuple.

Another critical vulnerability which can be used to conduct a *man-in-the-middle attack* (*MITM*), allows for adding a forged BS or hijacking a BS. In these cases, any SS can be compromised by a forged BS since there is no authentication to validate the identity of BS. A forged BS can intercept any information sent by any SS. In IEEE 802.16-2004 using PKMv1, the *auth request* message allows only for SS authentication but not for the corresponding BS authentication. When SS tries to establish a connection to BS, there is no way to confirm whether this BS is authentic or not. Thus, an attacker can masquerade as BS after sniffing an auth-related message from SS.

There are two additional significant security issues in IEEE 802.16-2004. First, the encryption keys are generated solely by BS instead of having both SS and BS equally contributing to key generation. Second, IEEE 802.16-2004 does not determine how to manage, store, renew, and revoke certificates.

3.2. Vulnerabilities in IEEE 802.16e-2005 Standard

Exploiting the fake BS vulnerability is difficult in mobile WiMAX using PKMv2 because mutual authentication between SS and BS is mandatory during the authorization process. (It is a welcome contrast to the original IEEE 802.16-2004 standard using the flawed PKMv1.) The authorization state machine of PKMv2 has two modes of mutual authentication has two modes. In one mode, RSA-based mutual authentication is used for mutual authentication only. In the other mode, used during the initial entry process, RSA-based mutual authentication is followed by the EAP authentication.

Despite many advanced security features introduced in mobile WiMAX, it still has some vulnerabilities. They include a disclosure of security context during the initial network entry, a lack of secure communication in access networks, and a lack of support for integrity protection of management frames.

Shon and Choi [13] discovered the first two of these vulnerabilities. The first vulnerability exists in the initial network entry phase. The initial *network entry* process begins by establishing a connection to a mobile WiMAX network. Many physical parameters, performance factors, and security contexts between SS and BS are determined during this process. However, the SS basic capability (*SBC*) negotiation parameters and PKM security contexts do not have any security measures to keep their confidentiality. This results in a possibility of exposure to malicious users during an initial *network entry* process. Mobile WiMAX has a message authentication scheme using HMAC/CMAC codes and a traffic encryption scheme using AES-CCM based on PKMv2. However, the security schemes are applied only to normal data traffic following the initial network entry process, but not to control messages exchanged during an initial network entry. We need a solution to protect important messages—such as security negotiation parameters in SBC messages and security contexts in PKM messages—during an initial network entry.

The second vulnerability of 802.16e-2005 detected by Shon and Choi [13] stems from a weak authentication between subsystems. The network reference model (NRM), proposed by the WiMAX Forum, is a logical representation of mobile WiMAX architecture. It consists of the following entities: SS, access service network (ASN), and connectivity service network (CSN). NRM defines a set of functions for communication between SS and BS only. This means that the security architecture given by the IEEE 802.16

DOI: 10.1002/sec

standards does not cover intra-ASN and ASN-to-CSN communications.

The third vulnerability is the lack of support for integrity protection of management frames. This creates a potential risk of DoS attacks, since MAC management messages are never encrypted and not always authenticated. There are authentication mechanisms for management messages in the MAC layer: the *hashed* message authentication code (HMAC) tuple, and *one-key* message authentication code (OMAC) tuple. OMAC is AES-based and includes replay protection, but HMAC does not. The authentication mechanism to be used for messages of the MAC-layer management is negotiated by a node during its network entry.

A standard has been given in Reference [14] and the security flaws of EAP-based handover procedures are analyzed.

These security weaknesses in authentication of management messages open the door to aggressions such as MITM attack, active attack, and replay attack. Using HMAC cannot prevent this problem. But if one-key MAC (OMAC) is used then modification of management messages by an attacker is unlikely. In all cases, the impact of an MITM, active, or replay exploit is high because it can broadly affect the operation of the WiMAX communications. A second line of defense against such attacks should be provided.

3.3. Potential Vulnerabilities in Recent and Future IEEE Standard

The IEEE 802.16j task group [30] works on incorporating multihop relay capabilities into mobile WiMAX. This amendment will be fully compatible with 802.16e-2005 mobile and subscriber stations, but a BS specific to 802.16j will be required for relays to operate. The standard introduces a new device called a *relay station* (RS) which is less complex and cheaper than BS with relay capabilities. RSs will be used to multiplex all traffic from an organization or a building and then relay it to a BS. Based on the fact that RSs are cheaper and smaller than BSs, hijacking or inserting an RS into an attacked network by hackers will be easier and thus more probable.

This vulnerability can be exploited for DoS collaborative and MITM attacks. Based on the IEEE 802.16j, RSs can create a mesh and cooperate with each other. It means they can behave like *ad hoc* network and relay traffic of other RSs [31]. Therefore, attackers can hijack or insert few RSs and influence critical processes like routing among RSs.

The most relevant attacks in the IEEE 802.16j standard include: (a) *black hole attacks* [32], in which a compromised RS node transmits a malicious broadcast informing that it has the shortest path to the destination (aiming to attract as many as possible messages); (b) *wormhole attack* [33,34] in which an attacker records packets (or bits) at one location in the network, tunnels them to another location, and forwards them to nodes there; (3) *denial-of-message* (DoM) attacks [35], in which malicious RSs may prevent some honest RSs from receiving broadcast messages by interfering with their radio tranmission; and (d) *sybil attack* [36] in which a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system, enabling the attakers to affect or control critical decisions of the system,(especially if the decision process involves voting or any other type of collaboration).

Another standard under development is IEEE 802.16h. It aimed at enabling coexistence of license-exempt systems based on IEEE 802.16,and facilitating coexistence of such systems with primary users [37,38]. Networks based on IEEE 802.11, as well as *ad hoc* networks that work in the license-exempt frequency bands, are among license-exempt systems. License-exempt systems may include networks based on IEEE 802.11 and *ad hoc* networks. Coexistence with such networks will enable attackers to exploit the inherent vulnerabilities of self-organized and infrastructure-less subnetworks to attack networks containing them.

Providing architectures with strong QoS support was one of the main design goals for IEEE 802.16 standards. DoS attacks are a major problem for applications with strict QoS requirements. DoS attacks on WiMAX networks, DoS attack can be executed by flooding a victim with a high number of messages to authenticate. This type of attack, likely to occur, remains a challenge to be addressed in the future.

3.4. Potential Vulnerabilities in WiMAX Networks in the Context of 4G and Heterogeneous Networks

There is no doubt that WiMAX networks are considered to be one of the most secure network architectures. However, in real-world scenarios WiMAX networks need to be deployed in conjunction with other access technologies, such as next generation networks (NGNs), WiFi, and third generation partnership project (3GPP).

The heterogeneity of WiMAX operating environment stems from the fact that the battle of access

DOI: 10.1002/sec

technologies has no absolute winner yet. The fourth generation (4G) networks are emerging as the future wave of wireless networks, so we need to look at them. Possible security risks arise mostly due to the following issues. First of all, in 4G we can see a large number of external connectivity points, with peer operators, with third-party application providers, with the public Internet, and with numerous heterogeneous technologies accessing the infrastructure. All of them are potential security holes if their security solutions do not fully interoperate. Second, multiple 4G service providers share the core network infrastructure, meaning that compromise of a single provider may result in a collapse of the entire network infrastructure. Finally, service theft and billing fraud can take place in 4G if fraudulent third parties masquerading as legitimate ones are successful in their attacks. As a result, WiMAX networks coexisting with 4G networks will suffer.

Another potential source of vulnerabilities in this context are the incompatibilities between WiMAX devices, especially if some of them are not fully compatible with the standards. Implementation bugs are another, and obvious, source of vulnerabilities, with poorly implemented security features opening the door for service disruption and theft [39].

4. Leveraging Attack Graphs for WiMAX

Given the many advantages of using WiMAX, it is not difficult to imagine that organizations will leverage its use to accomplish business critical tasks. One salient way organizations may take advantage of WiMAX is by allowing its workers to telecommute. While telecommuting increases the flexibility of an employees ability to work, such an arrangement could introduce unwanted vulnerabilities. The range of WiMAX can be anywhere from 4 to 30 miles. While this feature makes broadband access widely accessible over a physical geographical area, this accessibility gives malicious attackers are greater opportunity to become a part of a network with potentially many unaware victims. Hence, the question becomes, ‘how can organizations allow the flexibility that telecommuting and using hot spots provide, while mitigating some of the risk’? One solution involves the usage of attack graphs.

4.1. Attack Graphs

A method used by network administrators for vulnerability analysis is attack graph generation. Attack graphs provide a way for a network administrator to deal with the barrage of vulnerabilities that are released by vulnerability tracking organizations. Attack graphs provide multistage, multihost attacks that an attacker may perform based on a network’s existing vulnerabilities. With thousands of vulnerability alerts being released annually, it is unreasonable to assume that a single network administrator will have the ability to understand all the implications associated the possible many vulnerabilities existing in her network. For example, a network administrator may find and identify a vulnerability in her web server that provides read access to an attacker. She may also identify a vulnerability in her file sever that would allow an attacker who successfully exploited the vulnerability to execute arbitrary code. Because this vulnerability on the file server is a local exploit, the network administrator believes of the immediate patching that vulnerability is nonessential as the only people with accounts on the file server are trusted. A local exploit is a vulnerability that does not send packets over the network to be realized. An attack that begins with a remote login and finishes with exploiting a local vulnerability would still be considered a local exploit. Now, assume that web server has some credential information that is stored in a log file. An attacker could use these credentials to attempt to remotely log into the file server. Once the attacker was able to successfully log onto the file server, he could take advantage of the local exploit extant on the file server. The above example is straightforward to imagine; however, the task becomes more difficult as the number and type of vulnerabilities increase.

Reasons for delayed vulnerability removal: a rational question may be ‘why would the network administrator leave vulnerabilities in a system’? There could be many reasons for why a network administrator may leave vulnerabilities in a system. One reason could be that a patch for the vulnerability has not been released yet. Another reason could be that the patch is released, but the patch itself has vulnerabilities in it which trades an old set of problems for a new set of problems. Some organizations have strict policies that entail long evaluation periods before a new piece of software can be included into the organizations running system. An alternative reason could be that availability is critical to your business, and you cannot afford to take your machines offline for an extended period of time to patch the extant vulnerabilities. A reason that is often overlooked is that an organization may not allocate enough funds to properly patch their systems. Given these, and possibly other, reasons, the attack graph is a critical tool for analyzing and maintaining the security of a network.

DOI: 10.1002/sec

Generating Attack Graphs: the typical process for collecting information for generating an attack graph includes the following steps. First, the network administrator collects all the vulnerabilities from networked hosts using some type of vulnerability scanner (e.g., References [40,41]). The preconditions, postconditions, and effects of these vulnerabilities are determined by using information provided by organizations like CERT and NVD [42,43]. The vulnerabilities, preconditions, postconditions, and effects are transmuted to a consistent machine readable form. The connectivity of the network is determined. The connectivity of two machines is captured usually by specifying the source and destination machines, the protocol being used, and the destination port. Network connectivity captures the effects that any filtering device in the network may have on host connectivity. With this information, an attack graph can be generated. Figure. 2 is a simplified example from Reference [44]. The security policy for this figure is that a user on host 1 should not be able to obtain exec (i.e., execute) or su (i.e., superuser) privileges on host 3. appPwAuth represents the ability to authenticate *via* the PwAuth program. xdmLogin represents the X window display manager (xdm) login attack. wuFtpd represents an attack on the FTP server software wuarchive-ftpd.

A Major Drawback of Current Attack Graph Generation Process: The attack graph generation process detailed above works without issue when the hosts in the network are considered to be static. Once hosts are able to be mobile, *via* the use of WiMAX for example, the above methodology for generating attack graphs is no longer sufficient. In the case where hosts are allowed to move in and out of a network freely, a form of hypothetical analysis is required. For example, a network that is composed solely of Windows operating systems, produces a different attack graph from a network that has a primarily Windows operating systems and a few Unix and Linux hosts. Subsequently, the approach a network administrator may use to safeguard these two types of networks could be dramatically different. However, if there is a possibility that either one of these networks may arise in practice, how does a network administrator choose a set of countermeasures to ensure the security of her network? In previous work [45], we have outlined a methodology that helps a network administrator choose an optimal set of countermeasures given her budget. The approach is based on modeling the network administrator's problem of determining what countermeasures to implement as the binary knapsack problem [46]. We solve the problem using dynamic programming [47]. We are currently in the process of modifying this algorithm to account for the scenario where hosts have the ability to dynamically enter and leave a network. More specifically, we are determining suitable ways to modify the algorithm's value function to account for the probability of particular types of hosts being present in a network. Given the mobile nature of hosts belonging to WiMAX networks, such an algorithm could be instrumental in helping a network administrator determine how to harden her network.

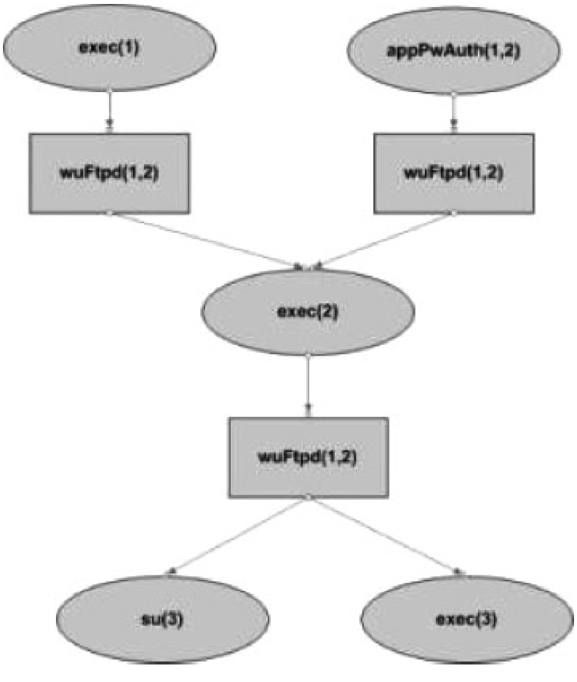

Fig. 2. Generated attack graph example.

The attack graph captures a wealth of information regarding the security of a network. This information is extracted through the use of attack graph analyses. Attack graph analyses of particular interest are those that constitute network security metrics. Using network security metrics, we can help ensure that our telecommuter only enters WiMAX networks that are deemed safe according to some security metric. For example, in Reference [48], Phillips and Swiler propose a shortest path metric. The intuition of this metric is that in order for an attacker to violate a security policy, he may have to perform a series of exploits. If we assume that each exploit requires approximately the same amount of effort, then the security of the network is given by the attack path requiring the least amount of effort. The attack path requiring the least amount of effort corresponds to the shortest attack path in the attack graph. So if one were to compare two attack

DOI: 10.1002/sec

graphs, and attack graph 1 had a shortest path of length 3, and the attack graph 2 had a shortest attack path of length 5, then the network underlying attack graph 2 would be deemed more secure than the network model underlying attack graph 1. Such a security metric could be leveraged in WiMAX networks.

4.2. Security-level Aware Hot Spots

WiMAX networks can contain special monitoring hosts. These hosts would be responsible for monitoring what hosts are present in the network. These monitoring hosts will accept queries from hosts in the network. A query a monitoring host would be able to respond to is 'what is the security level of this network'? The attack graph would be computed such that the querying host would be the attack goal. The security policy that will be checked is whether an attacker could execute arbitrary code on the querying host. Determining the feasibility of an attacker executing arbitrary code on a querying host is useful because such an action could violate each component of security: confidentiality, integrity, or availability. The monitoring hosts can be extended to deal with more specialized queries (e.g., 'Am I vulnerable to a DoS attack in this network'?). The monitoring hosts will respond with some security metric value. Based on the returned value, the querying host can determine whether or not, it would like to participate in the given network.

For example, assume that there are 10 hosts in a given WiMAX network. The hosts are labeled 1 through 10. The 10th host, is the monitoring host, M. If M, receives a query from new host, host 11, M could respond with a value 3, using the shortest path security metric. Host 11 has a policy that mandates that it may only participate in WiMAX networks having a shortest path security metric of 3 or greater. In other words, the security metric says that an attacker would have to exploit three vulnerabilities in order to execute arbitrary code on host 11. Host 11 may have this policy because it may have deduced that the probability of an attacker exploiting 3 vulnerabilities in order to violate its security is tolerably small. Since this is host 11's policy for participating in a WiMAX network, host 11's security mechanism would allow host 11 to use the WiMAX network under consideration. A scheme that relies on security metrics must be certain that the security metric produces reliable values. Although there has been many security metrics proposed in the literature (e.g., References [48–55]), we are currently in the process of creating an improved security metric that is both reliable and practical.

5. Profiling, Modeling, and Analysis of Collaborative Attacks on WiMAX

5.1. Research Problems

We address here the collaborative attacks on WiMAX through theoretical models and experiments.

5.1.1. Characterizing collaborative attacks on WiMAX networks

We need to understand the characteristics of collaborative attacks. As a first step, data from thousands of IDSs will be characterized and correlated to help in answering questions such as the following ones:

(1) What systems are the most likely attack targets over short and long periods of time?
(2) What kind of attack vectors do various organizations witness?
(3) Is there any correlation between the attack vectors at various organizations?
(4) Could future attacks be predicted based on attack sequences that have already been witnessed?
(5) How stable is the set of attackers over time?

5.1.2. Profiling collaborative attacks on WiMAX

A comprehensive understanding of collaborative attacks is essential for defending against the attacks on WiMAX. Data gathered from IDSs (as mentioned above) and synthetic data for possible collaborative attacks will serve as training data. They will be used to profile different types of collaborative attacks. When a new attack on WiMAX occurs, we can utilize the profiles to determine and classify the collaborative attacks.

5.1.3. Modeling collaborative attacks on WiMAX

We develop theoretical models to help understand, analyze, and defend against such attacks. This requires a comprehensive characterization and addressing the following issues:

(1) What are the most relevant aspects that should be included in models?
(2) What kinds of collaborations should be considered (e.g., collaboration between internal attacker, between external attackers, or between both internal and external attackers)?

DOI: 10.1002/sec

(3) What metrics should be defined and analyzed so that the resulting insights can be easily utilized by practitioners?
(4) Should models of collaborative attacks be stochastic or deterministic?
(5) How should cascading attacks (i.e., a sequence of coordinated attacks) be modeled?
(6) Which aspects and parameters of a WiMAX system have a significant impact on its security?
(7) How to tune WiMAX system configurations or parameters in order to improve security?

5.1.4. Power of collaborative attacks on WiMAX

The issues here include the following:

(1) Can we quantify the power gains of attackers due to their coordination?
(2) Can we turn the tables and use some aspects of coordination of attackers against them? If yes, can we quantify the possible gains of defender's power due to attackers' coordination?

As we will show below, novel models based on Fibonacci numbers can be built to cope with these issues.

5.1.5. Collaboration strategies among attackers on WiMAX

The important issues include here the following:

(1) How to model different ways of collaboration by attackers?
(2) How to incorporate the fact that not all attackers are equal?
(3) How do collaborative attackers divide the attack actions among themselves?
(4) How to represent the fact that newly infected host might join the existing attackers?
(5) In the Internet, can the coordinated attacks cause more damage to computer networks and systems? If yes, under what conditions? Similarly, under what conditions can this be false, or uncertain?
(6) In the Internet, can coordinated attacks leave more traces and evidences than individual attacks? If yes, under what conditions? Similarly, under what conditions can this be false, or uncertain?

Furthermore, research questions include identification, classification, and modeling of the following scenarios:

(1) It is possible that coordinated attacks, when launched together, can leave more evidence and traces, and have a higher probability of being detected than attacks that are launched individually or not coordinated.
(2) It is also possible that coordinated attacks can leave equal evidence and traces, and have equal probability of being detected as the attacks that are launched individually or not coordinated.
(3) Furthermore, attacks that are not properly coordinated may not only leave much more evidence and traces, and have much higher probability of being detected than individual or uncoordinated attacks, but may also impair performance of other attacks.

5.2. Profiling Collaborative Attacks on WiMAX

5.2.1. Some collaborative attacks on WiMAX

Our initial goal is to identify and classify attacks on WiMAX. Examples of attacks include replication attacks, Sybil attacks [16], spam attacks, phishing attacks, worms and viruses, DNS-related attacks, routing-related attacks, denial-of-message (DoM) attacks, and DoS attacks. A comprehensive feature analysis, encompassing feature detection and feature extraction, is a step toward a robust classification of collaborative attacks. A mechanism for learning the patterns of the attacks can be based on adaptive learning algorithms [56].

Three basic categories of attacks are as follows:

(1) *Independent* attacks, which have no knowledge of other attacks. They can be launched at the same time as other attacks but do not know other attacks.
(2) *Collaborative* attacks that are coordinated and can be launched simultaneously or sequentially. From the high-level or functional point of view, we further identify the relationships between the launched collaborative attacks and classify them as: (i) nonoverlapping (sequential); (ii) partially overlapping; and (iii) fully overlapping. Attacks may target different parts of a WiMAX network and aim at depleting resources of the defenders. From the low-level or technical point of view (e.g., techniques employed by attackers), attacks can be categorized into: (i) attacks that may substitute each other; (ii) attacks that may diminish the effects of each other; (iii) attacks that severely damage each other; (iv) attacks that expose other attacks; (v) attacks that

should be launched after each other; and (vi) attacks that may target different areas of a WiMAX network.

(3) *Replicated* attacks, in which adversaries can insert additional replicated hostile nodes into a WiMAX network after obtaining some secret information from the captured nodes or by infiltration [27]. Nodes replicated in this way are likely to uncover the shared secrets of the uncompromised neighboring nodes. Encrypted communication links can be established between a replicated node and the uncompromised nodes. It should be clear that compromising even a single node might allow an adversary to gain partial or even full control of a WiMAX network by producing many clones and deploying them in the original WiMAX network.

5.2.2. Dimensions of attack taxonomy

Our next goal is to classify the attacks into a comprehensive taxonomy facilitating quantitative security analyses.

The taxonomy includes a number of essential dimensions (that can also be metrics):

(1) *Attack type:* as already mentioned, the most relevant forms of attacks are: replication attacks, Sybil attacks, DoM attacks and DoS attacks. *Replication attacks* take place when adversaries are able to insert hostile nodes into the network by obtaining some secret information from the captured nodes or by infiltration. *Sybil attacks* occur when a node forges and uses several identities, and in this way obtains a greater control over the network allowing sniffing, packet dropping and delaying packets. *DoM attacks* are more common in wireless networks in which a node may be deprived of receiving broadcast messages due to activities of malicious nodes. *DoS attacks* occur when an attacker floods a server with requests exhausting the server's resources and thus its availability to respond to requests from other nodes.

(2) *Attack timing:* attackers may take advantage of temporal features of the network by choosing periods of higher susceptibility to perform the attack. Also they could coordinate when each attacks to maximize their effectiveness.

(3) *Attack severity and strength:* damage caused by an attack is an important factor in defining the defensive actions to be taken. For instance, an aggressive attack should be handled with a higher priority than non-aggressive attacks.

(4) *Attack extent:* An attack may affect the whole WiMAX network or a part of it. The extent of an attack also affects the priority of the actions taken by defenders against it.

(5) *Attacker's familiarity with attack target:* attacks may be conducted by insiders, quite familiar with attack targets, or outsiders. A more detailed categorization may include an attacker who is: a stranger, an acquaintance, a friend, etc. Inflicting damage is easier for an attacker more familiar with the attack target.

(6) *Attacker's role:* attackers can be, for instance, regular users, administrators, or guests.

(7) *Ranking of attackers:* attackers have usually distinct profiles. Some are more effective than others, and some have typical behavior while others are more difficult to characterize.

(8) *Composition and coordination of attack activities:* attackers can exhibit different abilities, including attack coordination abilities. In coordinated, well-organized attacks, attackers with the highest leadership skills will become commanders. Both leaders and followers must share information. How it is done is an important coordination characteristic to be captured in the model of coordination. The graphs of relationships among attackers used in the model can be tree-based and involve inheritance. Coordination lines can be employed to represent coordination.

(9) *Communication between attackers:* attackers can employ checkpointing and synchronization messages to communicate with each other. Coordination lines can again be employed, this time to represent communication. Finding the frequency and interval of attackers' communication can be very useful. Attackers can also utilize independent checkpointing, taking checkpoints of their own. They can also check later offline using other techniques, for instance, out-of-band communication.

(10) *Mutual feedback among attackers:* in a dynamic environment, coordinated attackers can benefit from exchange of feedback on their attack activities, including information on the results of their attacks. For example, attackers knowing that some ongoing attacks consume many resources of defenders can adjust their strategy. In this case, the attackers can:

(i) increase the power of the ongoing attacks; or

DOI: 10.1002/sec

(ii) employ more sophisticated or more focused strategies; or

(iii) fine-tune the timing of their attacks. Attackers can also adjust the strength of attacks dynamically. For instance, attackers can launch spasmatic attack lasting for a short time, making attack detection and attacker identification very difficult.

(11) *Attack and defense strategies:* the number of attackers affects the performance and power of attacks significantly. However, there are situations in which multiple attackers, not properly coordinated, could interfere with each other. Similarly, multiple defenders could also hamper each other. We plan to identify and describe strategies in which coordinated attacks provide synergistic effects, greater than the sum of individual attack effort.

Models can be defined from different subsets of these dimensions or metrics. For example, the impact of the attacks can be modeled as, impact = f(severity and strength of attack, extent of attack, communication between attackers, attack, and defense strategies).

5.2.3. Detecting collaborative attacks

An example application of the attack taxonomy is to detect whether the incoming attack on WiMAX is launched by collaborative attackers. By monitoring the WiMAX base stations, gateways, WiMAX access points, and related WiFi and Ethernet connections, essential data, both TCP and UDP, can be logged.

Analysis of the data can reveal collaborating groups, and indicate whether they are performing any malicious activities. Input parameters for the analysis include TCP connection data, UDP connection data, thresholds for collaboration (e.g., the number of IP address lookups per minute). The output parameters include identification of collaborating groups and show whether they are attackers.

To perform the analysis, we can use communication graphs, representing communication relationships among computers, and the content database, which stores the details of communication among computers. During the analysis, computers which exhibit similar communication behavior are grouped together, and thresholds are used to decide whether they are performing malicious activities (such as excessive number of IP address lookups done by collaborative port scanners).

5.3. Modeling Collaborative Attacks on WiMAX

5.3.1. Causal model for collaborative attacks on WiMAX

We borrow the idea of the causal model from database concurrency control [56–58] to apply it for modeling of collaborative attacks on WiMAX.The proposed causal model is intended for analyzing collaborative attacks and discovering vulnerabilities in both Internet and wireless networks.

An individual attacker is represented in the model by a state transition diagram, where a state represents a finite period of individual attack activities. Communication messages among attackers are modeled as state changes, and each state change constitutes an event. Then the causal relationships between these events are described by causal rules. A graphical representation of the causal rules, the causal graph, is constructed to assist in determining the possible event ordering.

A collaborative attack X can be modeled as a set of attacks $\{X_i\}$ such that X_i is the local attack launched by attacker *i*. Local attacks represent the local components of the overall distributed collaborative attack.

Each local attack X_i is modeled by an finite state machine (FSM) and has independent state and event specifications such as preconditions, post-conditions, and state transition rules. In simple distributed attacks such as collaborative port scan attacks, the FSMs of each local attack can be the same. However, in sophisticated collaborative attacks, FSMs of individual local attacks are not necessarily homogeneous.

Each local attack X_i can be formally defined as: $\langle S_i, E_i, M_i, D_i, L_i \rangle$, where S_i is a set of states in the local attack, E_i a set of events in the local attack, M_i a set of communication messages, D_i the local data structure, and L_i is a set of local operations on M_i. In collaborative attacks, the events within attacks occur in certain sequences. A given sequence of attack events may cause more damage to the system than other sequences. There are certain relationships among the events, and we model the relationships by causal rules.

A state of an individual attack represents a finite period of individual attack execution. Unlike the 'state' of a variable, the state refers here to a stage in the execution of the attack rather than the value of some variable. Attacker communication (collaboration), i.e., sending and receiving messages, must be modeled as state transitions. Examples of legal operations in a state include subversions of individual operating system, individual port scans, network packet preparation, buffer overflow exploits for individual program stacks, etc.

DOI: 10.1002/sec

An event causes an individual attack to change its state. There are two types of events, namely collaboration attack events and individual attack events. Collaboration events are characterized by communication between attackers. For example, sending or receiving a message constitutes a collaboration attack event. Individual attack events, which involve no communication between attackers, indicate transitions between individual attack states. Since each event is associated with a state transition of an individual attack and *vice versa*, the set of events for an individual attack can be viewed as the state transition function of the attack. An event is a member of the set $S_i \times S_i$.

5.3.2. The advantages of the causal model

The advantages of the causal model include the following:

(1) The causal model and causal relationships were originally invented for concurrency control in distributed computing. Hence, it is inherently a distributed model, and distributed computation can be used to speed up causal graph analysis, which is critical when analyzing large-scale networks.
(2) The causal model describes not only ‘sequential’ attacks but also concurrent attacks.
(3) The causal model can model coordination of node activities by exchange of messages. Even if the satisfied attack pre-conditions and attack post- conditions change dynamically, the causal model can still capture the changes that the state-of- the-art attack graph reduction techniques cannot.
(4) The causal model can describe timing of attacks. Attacks may need to be done within a specific time interval, and traditional attack graph analysis did not consider it.
(5) The causal model can represent unsuccessful attacks. Some attempted attacks are never successful and cannot be modeled by traditional attack graphs.

5.3.3. A hypothetical collaborative attack

In the hypothetical collaborative attack, the goal is to launch a DDoS attack against a target node T, as shown in Figure 3. Attackers $1, 2, \ldots, n$ are directly associated with router R1 with the firewall and target node T is associated with switch S1 without a firewall. To launch DDoS attacks, attackers need to send out a large number of abnormal packets, and those packets arrive at the first router, R1, before going to the Internet.

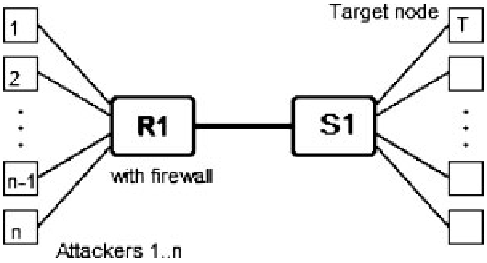

Fig. 3. The network topology of a hypothetical collaborative attack.

Since R1 is a sophisticated router with a firewall, it employs a packet filtering mechanism, and can automatically filter out the incoming packets from IP addresses that are sending out large amount of abnormal traffic. Hence, regular DDoS attack packets will be filtered out and the attack will fail. However, certain vulnerabilities in router R1 can be exploited to disable its firewall and packet filtering. In a collaborative attack, one attacker can attack router R1, while other attackers launch the DDoS attack after the first one successfully disables the firewall of router R1.

The notion of attack events and states is further illustrated by the state transition diagram of a hypothetic collaborative attack in Figure 4. Messages (such as ROUTING ACK) are represented by placing the message id within the transition arrow; each transition is marked with corresponding events, e0–e5.

The collaborative attack of Figure 4 works as follows. A local attacker waits for incoming attack transactions in the state S0 (the idle state). Upon receiving the request from a collaborative attack transaction (COLL_REQ), the local attacker broadcasts the message ROUTING_ATTACK_REQ to a number of other attack nodes (event e0) to initialize the attack on routers. The attacker must specify the target router. The attacker then waits for at least one acknowledgment (ROUTING_ACK) from another attacker before proceeding to broadcast a message DDOS_ATTACK_REQ to every other attack node, except the node that sent ROUTING_ACK, to initialize the DDoS attack. The attacker must specify the IP address of the target node. The attacker then waits for acknowledgement (DDOS_ACK) from all other attackers before proceeding to execute the transaction (in this case, attacking the target node for a long period of time, e.g., 24 h). This is implemented by local operations A_i^+ on the local variable A_i (not shown in Figure 4; discussed below). Event e8 represents the waiting loop for acknowledgments DDOS_ACKs. A DONE message will be broadcast to inform attackers at other nodes

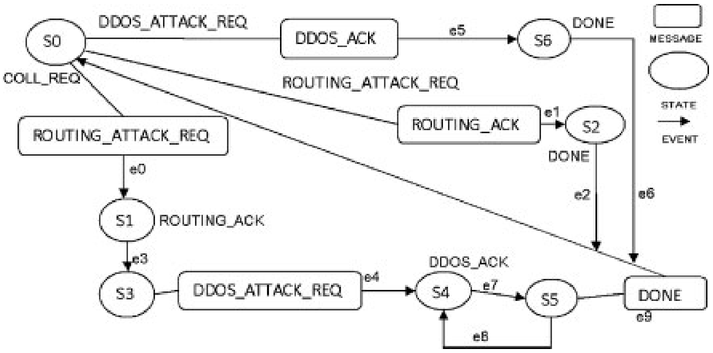

Fig. 4. The state transition diagram of a hypothetical collaborative attack.

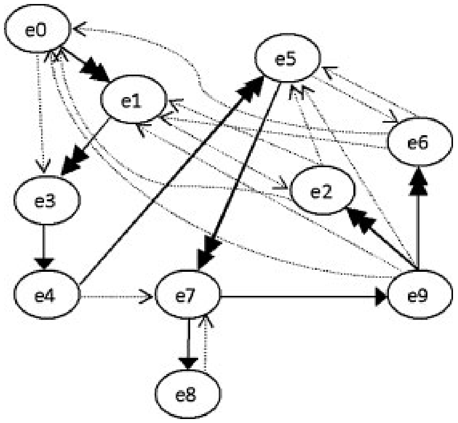

Fig. 5. The causal graph for the hypothetical collaborative attack.

that the collaborative attack transaction has completed.

If an attacker is in the idle state and receives a ROUTING_ATTACK_REQ message, it will send back the ROUTING_ACK message to acknowledge the request for launching the routing attack, and will keep attacking the packet filtering mechanism until a DONE message is received.

If an attacker is in the idle state and receives the DDOS_ATTACK_REQ message, it will send back the DDoS_ACK message to acknowledge the request for launching the DDoS attack, and will keep attacking until a DONE message is received.

The local variables used to describe local attacks in this hypothetical collaborative attack includes: (i) two counters for registering the acknowledgment messages ROUTING_ACK and DDOS_ACK; (ii) a timing variable for measuring how much time has elapsed since the DDoS attack has been launched; and (iii) codes implementing router and DDoS attacks. Let $X_i = \langle S_i, E_i, M_i, D_i, L_i \rangle$ be a local attack. Then

S_i: states = $\{$S0, S1, S2, S3, S4, S5, S6$\}$;

E_i: events $\{$e0, el, e2, e3, e4, e5, e6, e7, e8, e9$\}$;

M_i: message types = $\{$ROUTING_ATTACK_REQ, DDOS_ATTACK_REQ, ROUTING_ACK, DDOS_ACK, DONE$\}$;

D_i: local data structures =

- A_i: a counter for ROUTING_ACK responses;
- B_i: a counter for DDOS_ACK responses;
- T_i: a variable indicating how much time has elapsed since the DDoS attack has been launched;
- O_i: the malicious codes for routing and DDoS attacks;

L_i: local operations =

- A_i^+: increment by 1 the ROUTING_ACK counter;
- B_i^+: increment by 1 the DDOS_ACK counter;
- A_i^-: initialize to 0 the ROUTING_ACK counter;
- B_i^-: initialize to 0 the DDOS_ACK counter;
- Z_m^i[T]: keep executing attack codes for period T_i;
- W_m^i[O]: local accesses to attack codes (routing or DDoS) O_i by transaction *m*.

The causal model requires reasonable specification of the operational aspects of a collaborative attack before the analysis of the attack.

5.3.4. Causal model elements

The following definitions and discussions are adopted from Reference [58].

A causal rule U is a quintuple ⟨p, © , q, L, B⟩, where p and q are events, L is the local operation, B is a Boolean condition for Q to occur, and © is one of the causal relationships: $\{\rightarrow, \Rightarrow, \Rrightarrow\}$.

The causal relationship → specifies the ordering of non-message-related events. ⟨p, →, q, L, B⟩ is a causal

DOI: 10.1002/sec

rule if there are states x, y, z ∈ S_i such that p = ⟨x, y⟩, q = ⟨y, z⟩ (note that an event is a member of $S_i \times S_i$), the local operation L is performed in state y, B is a Boolean condition for q to occur, and no messages are involved in activating q. In other words, the attack of X_i must have the following state transition.

$$x \xrightarrow{\mathrm{p}} y \xrightarrow{\mathrm{q}} z$$

Intuitively, event p precedes event q on node i, and X_i executes event q following the occurrence of p without waiting for messages. Between these two events, the local operation L will take place. The predicate B must be defined over D_i and M_i (it can test the contents of previous messages). If ⟨p, →, q, L, B⟩ is a causal rule for some L and B, we say that event p precedes event q (or q follows p).

The other two causal relationships, ⇒ *and* ⇛, describe the ordering between message-related events. ⟨p, ⇒, q, L', B⟩ and ⟨r, ⇛, q, L'', D⟩ are causal rules iff there are states x, y, z ∈ S_i, u, v ∈ S_j, j ≠ i, such that p = ⟨x, y⟩, q = ⟨y, z⟩, r = ⟨u, v⟩, r is the event that node j sends a message to node i, and node i responds with event q at state y. L' is the local operation of node i in state y, which is independent of the message sent by the remote event r. L'' is the local operation of node i in state y that can be performed only after the message is received. B is the predicate that node i chooses to wait for messages after the event p, and D is the condition that the message of event r will be recognized by node i. Schematically, nodes i and j must have the following state transitions:

$$\text{node } i : u \xrightarrow{r} v$$

$$\text{node } j : x \xrightarrow[\mathrm{p}]{} y \xrightarrow[\mathrm{q}]{r} z$$

This notation means that node i, while waiting at state y, receives a message sent by event r of node j, and then executes event q in response. Event r is said to cause event q if ⟨r, ⇛, q, L, D⟩ is a causal rule for some L and D. Note that the causal rules ⟨p, ⇒, q, L', B⟩ and ⟨r, ⇛, q, L'', D⟩ are related to each other; no causal rules ⟨p, ⇒, q, L', B⟩ should exist without the corresponding ⟨r, ⇛, q, L'', D⟩ causal rules.

Either L or B in the above causal rules can be null. A null L signifies that no local operation is associated with the events involved, and a null B indicates that the causal relationships are unconditional, i.e., independent of local attack details or messages.

The predicate B of a causal rule ⟨p, ⇒, q, L', B⟩ can also be used to specify the sites receiving the message generated by event p. Hence, either message broadcasting or daisy-chain transmission can be described by a proper predicate B. The detailed semantics, such as the exact node id to which a message is sent, are in general not critical to the causal relationship ⇒.

The following notation is used in this paper to designate a causal rule ⟨p, © , q, L, B⟩:

$$\text{p© q} + \text{L if B}$$

A causal graph G = ⟨V, E⟩ for a set of causal rules of an attack is a labeled digraph with vertices V = {e | events} and edges E = {⟨p, q⟩ | there exists a causal relationship © , local operation L, and predicate B such that ⟨p, © , q, L, B⟩ is a causal rule}. The vertices and the edges are labeled with their corresponding events and causal relationships. The edges in a causal graph are referred to as → edges, ⇒ edges, or ⇛ edges according to their labels. Figure 5 shows the casual graph for the collaborative attack depicted in Figure 4.

5.3.5. Analysis of attacks using the causal model

By identifying all attack events that occur during individual and collaborative attacks and establishing a partial order (or causal relationships) among all attack events and produce a 'causal attack graph', we can get the following results from the causal model:

(1) Verify the security properties of the causal attack graph using model-checking techniques. Specifically, we study whether there exists a sequence of events that lets the security checker proceed from the initial state to the goal state.
(2) Identify the set of events that are critical for performing the attacks. Specifically, study how to find a minimum set of events that, once removed, would disable the attacks.
(3) Check whether the occurrences of some event/state transitions are based on message transmissions or collaboration.

An *Attack-extended Global-view Causal Graph* G(V, E) for a set of causal rules is a labeled diagraph with vertices V = V1 + V2, where V1 = {s | attack states} and V2 = {e | events}; and edges E = E1 + E2, where E1 = {e | attacker actions} and E2 = {⟨p, q⟩ | there exists a causal relationship © , local operation L, and predicate B such that ⟨p, © , q, L, B⟩ is a causal rule}.

We have performed experiments on the collaborative attack and generated the attack-extended global-view causal graph. We discuss it further in the experiments section.

Application of causal models and performance analysis of collaborative attacks. In our model for collaborative attacks, the notion of attack steps is used to model system behavior. The attack actions of collaborative attackers are modeled as a sequence of atomic attack steps. The events related to a particular attacker represents the order of the atomic attack steps.

The performance of a collaborative attack can be measured by several parameters, e.g., amount of bandwidth consumed, number of hosts disabled, number of attack packets sent, number of hosts subverted, the degree of collaboration, etc. Some of these parameters are dependent on the types of attack transactions while some others are based on the particular characteristics of the system parameters, e.g., the number of packets that needs to be sent to launch DDoS attacks, whether there is a security firewall in the system, and whether there are access control mechanisms in the system, etc.

We can infer the degree of collaboration and temporal ordering of events in the system under collaborative attack. A coordinator in a collaborative attack is modeled as an attacker which oversees the atomic attack steps of all attackers. All attack steps need the approval of the coordinator to proceed. If the coordinator determines that a particular attack cannot proceed (e.g., when an attack step requires root privilege which the attacker does not enjoy), it can change the atomic attack steps (e.g., perform some other attack steps on other machines which do not require the root privilege). If an attack requires less collaboration, attackers in the attack will have less conflicts. Therefore, by studying the communication and dependence between attackers, we can compare their degrees of collaboration.

The problem of attack graph generation is hard and current solutions are not very scalable. However, with the causal model, we can effectively determine if collaborative attackers can successfully launch the attacks. To determine the correct execution of a collaborative attack, the attack steps of the collaborative attack are tested against the known collaborative attack types.

5.3.6. Experimental results

We would like to verify the existence of collaborative attacks and that they can cause more damages or gain more control of the target system. We conducted experiments to verify the power of collaborative attacks, analyzed the collaborative attack using the causal model, and generated the attack-extended causal graph.

Input variable parameters include N: Number of normal TCP connections; M: the speed of link from each host to router, 10 Mb/s; B: buffer space at each router, 4K × N bytes; Size_packet: packet_size, 1K bytes; and MR: speed of the link between R1 and R2, 1.5 Mb/s.

For the regular DDoS attack, we modify the router information controller such that router will impose a limit on the number of SYN packets per second permitted to pass. After the limit is passed router will send SYN/ACK packets for the hosts.

Output performance metrics include round-trip time: the time for sending a echo request and getting a reply between two nodes in the system; and bandwidth: the bandwidth of the network connection.

We used SSFNet [59], and conducted the experiments in Linux 2.6.13 with Java runtime environment. The topology of the network is Dumbbell (Figure 3).

Steps of the experiment include:

(1) Initialize the system with various number of TCP connections, first with the regular DDoS attack scenario for various periods, such as 15 min.
(2) Initialize the system with various number of TCP connections, with the collaborative DDoS, and routing attack scenario for various periods such as 15 min.
(3) Start the system with two HTTP servers, one on each target node. The $N(10)$ TCP connections will send traffic for 2 s and restart. We run the DDoS attack after 5 min of system start and measure estimated RTT time.

We utilize the SSF.App.DDoS package and run the DDoSSession( ) function. Selection of master and zombie nodes is done randomly among the nodes directly connected to Router 1(R1). Two target nodes are selected among the nodes directly connected to Router 2(R2). For the regular DDoS attack, we modify the router information controller such that router will impose a limit on the number of SYN packets per second permitted to pass. After the limit is passed router will send SYN/ACK packets for the hosts. However, for collaborative attacks, a 'Trojan horse' is embedded in a router. As soon as the DDoS attack is launched, the master node will send out a secret message to the router such that a 'Trojan' embedded in the router will change the routing information such that the router will no longer impose such SYN packet limits.

DOI: 10.1002/sec

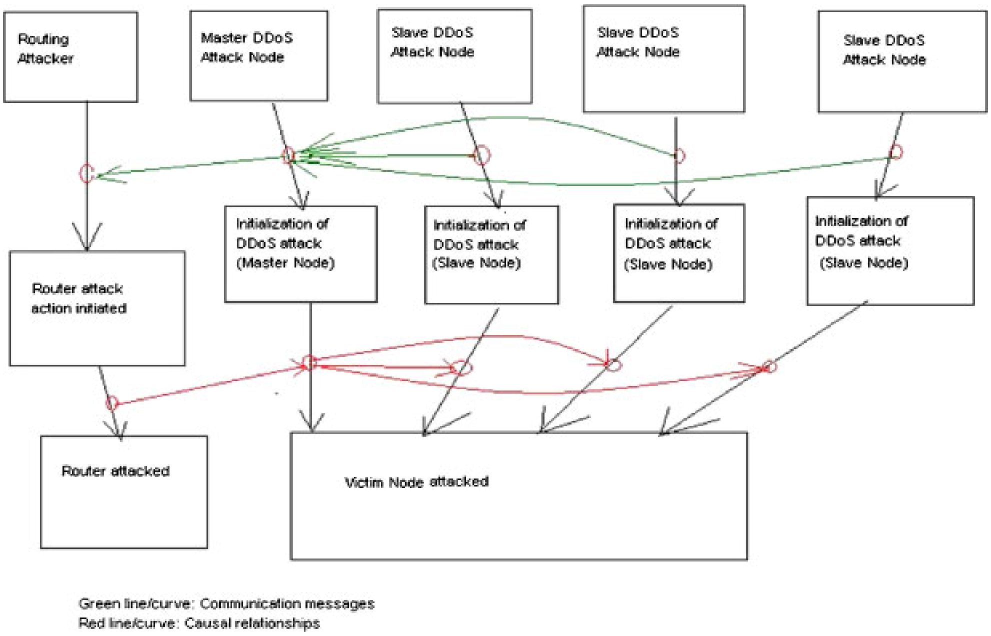
Routing Attacker
Master DDoS Attack Node
Slave DDoS Attack Node
Slave DDoS Attack Node
Slave DDoS Attack Node
Initialization of DDoS attack (Master Node)
Initialization of DDoS attack (Slave Node)
Initialization of DDoS attack (Slave Node)
Initialization of DDoS attack (Slave Node)
Router attack action initiated
Router attacked
Victim Node attacked
Green line/curve: Communication messages
Red line/curve: Causal relationships

Fig. 6. The attack-extended causal graph for the collaborative DDoS and routing attacks.

Our results show that causal model is a promising approach. We have applied causal model to analyze the collaborative DDoS and routing attacks. The causal graph generated is shown in Figure 6 (green and red arrows model the coordination between attackers).

Figure 7 shows that collaborative attacks can cause much more damage than single attacks. X-axis represents time (in minutes) and Y-axis represents RTT time (in seconds). In this example, the DDoS attacks were started at time $t = 5$ min. The red line shows the collaborative attacks of routing and DDoS. The blue line shows the regular DDoS attack. Because router has the defense mechanism built-in against DDoS attack, the regular attack did not accomplish its goal. However, in the collaborative attack case, when launched together with routing attacks, DDoS attack effectively blocked the user from establishing any new TCP connection.

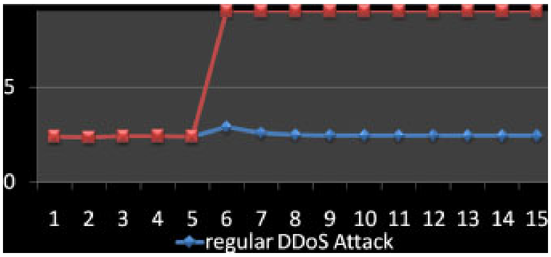

Fig. 7. RTT time (second) *versus* time in system (minute).

5.4. The Power of Collaborative Attacks on WiMAX

5.4.1. Motivation

A large number of attackers can collaborate to increase their computation power when needed to break WiMAX protocols. Attackers can also gain control of a required number of nodes to influence the decision-making process of core machines. Hence, we would like to quantitatively measure performance of multiple attackers, especially collaborating ones. For example, we can use it to study the malware propagation in WiMAX.

5.4.2. Malware propagation

It is clear that malware with different scanning and propagation strategies have different spread time. To address the issue of collaborative attack, we propose the discrete-time generic Fibonacci malware propagation (GFMP) model, which is inspired by the Fibonacci number sequence. In the Fibonacci rabbit problem, newly born rabbits cannot give birth to baby rabbits immediately. Instead, they need some time to get mature, which is reminiscent of the infection/propagation time problem discussed above: similarly, a host cannot scan and infect other hosts until maturity, i.e., completely infected. Due to space

DOI: 10.1002/sec

limitations, we omit the discussion of the GFMP model. Interested readers are referred to Reference [60] for details.

6. Conclusion

In this paper, we identify the problems with individual protocols in the WiMAX protocol suite, and discuss collaborative attacks in WiMAX systems. We present several typical security vulnerabilities and WiMAX attack scenarios. We leverage attack graphs to analyze collaborative attacks in WiMAX.

We emphasize the possibility of collaborative attacks in WiMAX, and present theoretical models and practical solutions to collaborative attacks in WiMAX. We characterize, model, and analyze collaborative attacks in the WiMAX. We perform experiments to verify our analysis of the collaborative attacks.

In our models, we omitted several specific but important applications over the WiMAX systems, including the voice over IP (VoIP) applications. Research on collaborative attacks to VoIP application in the WiMAX is the subject for future work.

In our analysis, we did not take attacks on quality of service (QoS) into consideration. Some systems and applications require reasonable packet loss rate, while others cannot tolerate long response time. Collaborative attacks on QoS, in which attacks might be adaptive, are more sophisticated and are the subject for future work.

Acknowledgment

The authors would like to thank Minaxi Gupta at Indiana University and Shouhai Xu at University of Texas at San Antonio for helpful discussions. This work was supported in part by grants from NSF-0242840 and NSF-0219110.

References

1. Motorola Inc. WiMAX security for real-world network service provider deployments. *White Paper*, 2007.
2. Chen S, Xu J, Kalbarczyk Z, Iyer R. Security vulnerabilities: from analysis to detection and masking techniques (invited paper). In *Proceedings of the IEEE*, Vol. 94, Issue 2, February 2006.
3. Molsa J. Cross-layer design for mitigating range attacks in ad hoc networks. In *Proceedings of the 24th IASTED International Conference on Parallel and Distributed Compting and Networks*, 2006.
4. Wang W, Lu Y, Bhargava B. On security study of two distance vector routing protocols for mobile ad hoc networks. In *Proceedings of IEEE International Conference on Pervasive Computing and Communications*, 2003.
5. http://www.sans.org/reading_room/whitepapers/vpns/the_day_des_died_722
6. Ramachandran A, Feamster N. Understanding the network-level behavior of spammers. In *ACM SIGCOMM*, Vol. 36, 2006.
7. Moore D, Paxson V, Savage S, Shannon C, Staniford S, Weaver N. Inside the slammer worm. *IEEE Security and Privacy Journal* 2003; **1**: 33–39.
8. Moore D, Shannon C, Brown J. Code-red: a case study on the spread and victims of an Internet worm. In *ACM/USENIX IMW*, 2002.
9. Moore D, Voelker GM, Savage S. Inferring Internet denial-of-service activity. In *Usenix Security Symposium*, 2001.
10. Katti S, Krishnamurthy B, Katabi D. Collaborating against common enemies. In *ACM Internet Measure Conference (IMC)*, 2005.
11. http://www.dshield.org/
12. Johnston D, Walker J. Overview of the 802.16 Security. *IEEE Security and Privacy* 2004; **2**(3): 40–48.
13. Shon T, Choi W. *An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions*. Springer: Berlin/Heidelberg, 2007.
14. Hur J, Shim H, Kim P, Yoon H, Song N. Security considerations for handover schemes in mobile WiMAX networks. In *IEEE WCNC*, 2008.
15. Schuba CL, Krsul IV, Kuhn MG, Spafford EH, Sundaram A, Zamboni D. Analysis of a denial of service attack on TCP. In *IEEE Symposium on Security and Privacy*, 1997.
16. Douceur J. The sybil attack. In *First International Workshop on Peer-to-Peer Systems*, 2002.
17. Pei D, Massey D, Zhang L. Detection of invalid routing announcements in the RIP protocol. In *GLOBECOM*, 2003.
18. Cheung S, Lindqvist U, Fong M. Modeling multistep cyber attacks for scenario recognition. In *DARPA Information Survivability Conference and Exposition*, 2003.
19. Yu H, Kaminsky M, Gibbons PB, Flaxman A. SybilGuard: defending against Sybil attacks via social networks. In *Proceedings of ACM SIGCOMM Conference*, September 2006.
20. Yu H, Gibbons PB, Kaminsky M. Toward an optimal social network defense against Sybil attacks. In *Proceedings of the 26th Annual ACM Symposium on Principles of Distributed Computing*, 2007.
21. Li X, Xu S. A stochastic modeling of coordinated internal and external attacks. *Technical Report*. Available at: http://www.cs.utsa.edu/~shxu/collaborative-attack-model.pdf
22. Ramaswamy S, Fu H, Nygard KE. Effect of cooperative black hole attack on mobile ad hoc networks. In *International Conference on Wireless Networks*, 2005.
23. Awerbuch B, Holmer D, NitaRotaru C, Rubens H. An on-demand secure routing protocol resilient to Byzantine failures. In *ACM Workshop on Wireless Security (WiSe) in Conjunction with MobiCom*, 2002.
24. Yang J, Ning P, Wang XS, Jajodia S. CARDS: A distributed system for detecting coordinated attacks. In *Proceedings of IFIP TC11 16th Annual Working Conference on Information Security*, 2000.
25. Cuppens F, Miege A. Alert correlation in a cooperative intrusion detection framework. In *IEEE Symposium on Security and Privacy*, 2002.
26. Hussain A, Heidemann J, Papadopoulos C. COSSACK: coordinated suppression of simultaneous attacks. In *DISCEX*, 2003.
27. Ourston D, Matzner S, Stump W, Hopkins B. Coordinated internet attacks: responding to attack complexity. *Journal of Computer Security* 2004; **12**(2): 165–190.

DOI: 10.1002/sec

28. Boom D. Denial Of service vulnerabilitie In IEEE 802.16 wireless networks. *Thesis*, Naval Postgraduate School Monterey, California, 2004.
29. The Institute of Electrical and Electronics Engineers. IEEE standard for local and metropolitan area networks part 16: air interface for fixed broadband wireless access systems. *IEEE Std 802.16-2004*, IEEE, 2004.
30. http://wirelessman.org/relay/
31. Sydir J. Harmonized contribution on 802.16j (mobile multihop relay) usage models. *IEEE 802.16j task group*, 2006.
32. Ramaswamy S, Fu H, Nygard K. Effect of cooperative black hole attack on mobile ad hoc networks. In *ICWN*, 2005.
33. Wang W, Bhargava B, Lu Y, Wu X. Defending against wormhole attacks in mobile ad hoc networks. In *WCMC*, Vol. 6, Issue 4, June 2006; 483–503.
34. Hu Y-C, Perrig A, Johnson DB. Packet leashes: a defense against wormhole attacks in wireless ad hoc networks. In *IEEE INFOCOM*, 2003.
35. McCune JM, Shi E, Perrig A, Reiter MK. Detection of denial-of-message attacks on sensor network broadcasts. In *IEEE Symposium on Security and Privacy*, 2005.
36. Yu H, Kaminsky M, Gibbons P, Flaxman A. SybilGuard: defending against Sybil attacks via social networks. In *ACM SIGCOMM*, 2006.
37. http://wirelessman.org/le/contrib/C80216h-05_045.pdf
38. Berlemann L. Unlicensed operation Of IEEE 802.16: coexistance with 802.11(A) In *Shared Frequency Bands*, PIMRC, 2006.
39. Nasreldin M, Aslan H, El-Hennawy M, El-Hennawy A. WiMAX security. In *Advanced Information Networking and Applications-Workshops*, 2008.
40. Nessus Security Scanner. Available at: http://www.nessus.org, 2008.
41. Security Administrator Tool for Analyzing Networks (SATAN). Available at: http://www.porcupine.org/satan, June 2008.
42. Computer Emergency Response Team (CERT). Available at: http://www.cert.org/, 2009.
43. NIST's National Vulnerability Database. Available at: http://nvd.nist.gov, 2009.
44. Noel S, Jajodia S. Managing attack graph complexity through visual hierarchical aggregation. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, 2004; 109–118.
45. Idika N, Marshall B, Bhargava B. Maximizing security given a limited budget. In *TAPIA'09: Richard Tapia Celebration of Diversity in Computing*, April 2009.
46. Martello S, Toth P. *Knapsack Problems: Algorithms and Computer Implementation*. Available at: http://www.or.deis.unibo.it/knapsack.html. John Wiley & Sons. ISBN 0-471-92420-2,1990.
47. Bellman R. The theory of dynamic programming. In *Proceedings of the National Academy of Sciences*, 1952; 716–719.
48. Phillips C, Swiler LP. A graph-based system for network-vulnerability analysis. In *NSPW'98: Proceedings of the 1998 Workshop on New Security Paradigms*, ACM, New York, NY, USA, 1998; 71–79.
49. Sheyner O, Haines J, Jha S, Lippmann R, Wing JM. Automated generation and analysis of attack graphs. In *IEEE Symposium on Security and Privacy*, 2002; 273–284.
50. Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs. In *Proceedings of the 15th IEEE Computer Security Foundations Workshop*, June 2002.
51. Noel S, Jajodia S, Berry BO, Jacobs M. Efficient minimum-cost network hardening via exploit dependency graphs. In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003)*, 2003.
52. Dantu R, Kolan P. Risk management using behavior based bayesian networks. *Intelligence and Security Informatics*, LNCS, Vol. 3495, 2005; 115–126.
53. Pamula J, Jajodia S, Ammann P, Swarup V. A weakest-adversary security metric for network configuration security analysis. In *Proceedings of the 2nd ACM Workshop on Quality of Protection*, 2006; 31–38.
54. Lippmann R, Ingols K, Scott C, *et al*. Validating and restoring defense in depth using attack graphs. In *Military Communications Conference*, October 2006.
55. Wang L, Singhal A, Jajodia S. Measuring overall security of network configurations using attack graphs. *Data and Applications Security XXI*, Vol. 4602, August 2007; 98–112.
56. Bhargava B, Riedl J. A formal model for adaptable systems for transaction processing. *IEEE Transactions on Knowledge and Data Engineering* 1989; **4**(1): 433–449.
57. Bhargava B, Browne S. Adaptable recovery using dynamic quorum assignments. In *Proceedings of the 16th International Conference on Very Large Data Bases (VLDB)*, 1990.
58. Bhargava B, Hua C. A causal model for analyzing distributed concurrency control algorithms. *IEEE Transactions on Software Engineering* 1983; **9**(4): 470–486.
59. http://www.ssfnet.org/homePage.html
60. Zhang Y, Bhargava B. The effects of threading, infection time, and multiple-attacker collaboration on malware propagation. In *The 28th IEEE International Symposium on Reliable Distributed Systems (SRDS)*, September 2009.

DOI: 10.1002/sec