Feasibility of Attacks: What is Possible in the Real World – A Framework for Threat Modeling

Ameya M Sanzgiri and Shambhu J. Upadhyaya
Computer Science and Engineering, University at Buffalo, Buffalo, NY, U.S.A

Abstract— *In this paper we present a new method to assess risks of attacks faced by a network. Our methodology approaches these risks from the perspective of an attacker in order to bridge the gap created by traditional security schemes which approach from the defender's perspective. These dual perspectives of risk analysis can lead to more effective solutions to security. We describe the various parameters that affect an attack in the real world and use these parameters to analyze the risks of an attack. We also create a model for formally analyzing the risk of an attack using the above parameters. We finally use a case study of jamming attacks on the MAC Layer of the OSI Stack as an illustration and assess the risks for different MAC protocols.*

Keywords: Jamming attacks, Perspectives of attack, Risk analysis,Threat modeling

1. Introduction

Current security schemes are designed to protect against attacks as seen by the defender based on the limitations and vulnerabilities of his system. From a defender's perspective, the *entire* system is vulnerable to attacks and needs to be secured. Thus, the goal of a defender is to secure the complete system against all possible attacks. However, an attacker's perspective which is orthogonal to the defender's perspective, is to focus on a part of the system and attack. This difference in perspective is further highlighted in their individual goals where an attacker tries to find *one* flaw in the system and leverage it while the defender tries to defend his *entire* system by designing a security scheme. Currently the process of designing a security scheme relies heavily on Attack Graphs [1] and Attack Surfaces [2], [3] which are two methods for formal assessment of risks. Attack surfaces is a conceptual tool used to increase the security of a software during development. Attack graph is an abstraction that divulges the ways by which an attacker can leverage the vulnerability of a system to violate a security policy. It must be noticed that in order to use the attack surface concept on a system, one has to know of all possible vulnerabilities and then optimize the available resources to cover the attack surface.

However, the inherent problem with the design of such schemes is that firstly, the defender does not have enough resources to completely secure his network.The countermeasures usually consider a single attack and are rarely feasible in terms of implementation complexity or cost to the network. Also, the defender is already at a disadvantage due to the fact that his perspective remains wide and vulnerable, while the attacker's perspective is more focused and specific. This methodology of designing security schemes has resulted in a performance as well as a feasibility gap of schemes in theory and practice which causes them to be reactive in nature. Thus, a paradigm shift is necessary to primarily reduce this gap and to minimize or eliminate the disadvantage of a defender. We propose that such a shift can be obtained by creating a new risk model which would include the attacker's perspective along with the traditional defender's perspective. Such a risk model would culminate in a new classification of attacks (from both perspectives) while providing insights on the kind of information needed by an adversary for an attack. Using the concepts of attack surfaces, one can visualize the objectives of the defender and the attacker as *a game* where the defender tries to minimize the attack surface of the system (securing the system) while the attacker tries to maximize it. This is different from the traditional approach as incorporating the attacker's perspective means the re-examination of some common assumptions with the goal of providing an effective yet practical outlook of the security of a system. The contributions of the paper are 1) A new risk model, 2) Classification of attacks, and 3) A means for proactive security schemes.

The rest of the paper is organized as follows. After discussing the related work and background in Section 2, we present our risk model including the assumptions of the model in Section 3. In Section 4 we discuss the steps of the attacker leading to an attack. Section 5 describes the different factors that need to be considered in an attack. Section 6 presents a qualitative analysis of our model, using jamming attacks as a case study. Section 7 discusses the future work and implications of the model, and then concludes the paper.

2. Background and Related Work

Currently, risk analysis enables the separation of the critical or major threats from the minor ones [4]. In understanding the risks, knowledge of the real threats helps place in context the complex landscape of security mechanisms.The evaluation in [4] is conducted according to three criteria: likelihood, impact and risk. The likelihood criterion ranks the possibility that a threat materializes as an attack. The impact

criterion ranks the consequences of an attack materializing a threat. The likelihood and impact criteria receive numerical values from one to three and for a given threat, the risk is defined as the product of the likelihood and impact. Depending on the numerical values received the risk is classified as minor, major and critical. While the approach is relatively simple the likelihood of an attack is based from the system administrator's point of view and does not consider the absence of *a priori* knowledge of the system that an attacker is likely to have. Secondly the evaluation requires the administrator to have expert knowledge of target systems or existing exploits [5]. Further, most risk analyses do not consider network characteristics and their effects. The aforementioned reasons contribute to the inadequacy of such evaluation techniques to correctly analyze risks. The authors of [6] state that an attack graph can provide a methodology for documenting the risks of a system when it is designed. However generation of the graph also requires analyzing the system's purpose and attacker goals which are seldom easy. They also describe how one can utilize the concept of attack graphs in assessing how a multistage attack occurs, where an attacker tries to utilize the intrusion into a system as launching point for other attacks, provided his intrusion is undetected. However, incorporation of network characteristics in traditional risk analysis can prove beneficial and provide the system administrator with some information. Duan et al. [7] present a theoretical analysis of minimum cost blocking attacks on multi-path routing protocols in Wireless Mesh Networks and prove that such an attack is completely infeasible in WMNs. Their evaluation considers the effect of the attack, the characteristics of the target network such as traffic generation patterns and the size of the network on the attack. However, they too make certain assumptions such as the attacker having a way to implement the attack and *a priori* knowledge of the network. Traditional risk models and their assumptions illustrate the extent of the gap between the theoretical and practical risk analysis. We propose to use the parameters that affect an attacker in his attack to analyze the risks of attacks in order to bridge this gap.

3. Risk Model

Existing security schemes are reactive due to the inability of the defender to foresee the domain of all possible attacks. Researchers make theoretical assumptions and develop complex security solutions yet systems can be compromised by an attacker through a simple, low cost and practical means that was not foreseen by the defender. This problem is exacerbated by the widening gap between the theoretical and practical aspects of security. Some of the attacks theorized by researchers, although wishful, may never occur in practice due to the high cost of attack on the part of the adversary or due to the practical limitations of hardware devices. Further, most formal tools like the ones discussed above require a thorough knowledge of the individual system components and their interaction with each other, the lack of which leads to inaccurate or ineffective security solutions. Hence one needs a new risk model that can classify the attacks from a more practical perspective that is not only feasible but also effective. To achieve this we re-examine the assumptions that are made in the literature and include both the attacker's and the defender's perspectives on an attack. Including the attacker's perspective on attacks however requires one to analyze and enumerate the factors that an attacker would consider in his attack.

3.1 Assumptions of the Model

The assumptions made by a model have a direct effect on the analysis of risks and can cause unreliable assessments. This can lead to a false sense of security or cause inefficient resource allocation by a system administrator. We assume that the attacker has no or very little *a priori* information about the target network. This includes knowledge about network components, its purpose or its usage. However, the attacker does have the resources and technical knowledge of implementing an attack and can gain the knowledge of the system he intends to attack. This is a valid assumption as we shall discuss in Section 4. We also apply the same constraints on the hardware the attacker possesses as in the real world. This however does not imply that the network is physically isolated, in the sense that an attacker is quite capable of both performing active and passive attacks on the target network. The scenarios of insider attacks and attacks resulting due to the mistake of a target network's user is not considered and is beyond the scope of this paper.

4. Modus Operandi of an Attack

Before we present the steps of an attack, we need to clearly define an attack. An attack is a series of intentional steps taken to gain some unauthorized result. Since the steps of any attacker are intentional and methodical, it should be generally quantifiable and can be represented as a process, which in turn would help in creating a proactive defence strategy. An attack generally follows a sequence of steps, viz. Reconnaissance, planning, collection, analysis and execution while targeting a system [8]. The goal of these steps is to first obtain the Information Content necessary for the attack in order to execute an attack. Thus, the procedure to gain information about the network, is the precursor to an attack. From an attacker's point of view, this would include gaining as much information of the system as one can so as to develop one's strategy for attack. What we can broadly classify as information content are the features of the target network such as the data in the network, components, protocols of the target network, etc. It is important to understand that from an attacker's perspective this information content comprises of all the factors that has to considered for staging an attack. In Section 5 we present a detailed analysis and motivation of these factors. While the exact amount of information

required for an attack depends on the skills of the attacker it can be fairly assumed that most of this information is essential for an attacker. In the current literature so far, it is usually assumed that the attacker already has the required information content. However, we believe that if a defender has to regain his advantage security schemes need to increase the cost of the process of collecting information content for the attacker.

5. Motivational Factors of an Attack

The goal of any risk model is to assess the risk of an attack and classify the threat it poses to a network. However, from the defender's perspective the risk of an attack should relate closely to a real world scenario so as to be able to efficiently allocate his resources. In most cases the risk analysis of an attack takes into account only the defender's perspective and knowledge, and presents a rather pessimistic scenario. However, if we were to take in factors from the attacker's perspective as well, the parameters that affect the analysis of a risk change. When we consider both these perspectives, the risk of an attack depends on – i) motivation of attacker, ii) probability of attack, iii) easier alternative, iv) target network characteristics and v) cost of attack. This is described next.

5.1 Motivation of an Attacker

This parameter directly affects the risk assessment of an attack and asymptotically either elevates or depreciates the risk of an attack. It is scientifically difficult to quantify this parameter as it depends on an attacker's behavior. However, one can try to quantify it by observing other factors such as the type, target and the purpose/effect of the attack. In [4], the authors state that an attacker's motivation can be categorized to be High, Medium and Low. Thus, both the purpose of attack and the motivation contribute to the overall risk of an attack. For example, a highly motivated attacker attacking out of inquisitiveness is likely to be less dangerous than one for financial gain.

5.2 Probability of Attack

This parameter denotes if an attack is desirable based on two factors – *cost of an attack* and the *severity factor* of the attack. We define *cost of attack* as a combination of time, the hardware needed and the general strategy required for an attack. Severity factor is defined as the effect an attack has on a network. It is evident that the probability of an attack is likely to increase as the cost decreases and the severity increases. Thus we can quantify the probability of attack as

$$\Pr(Attack) = f(Severity_{Attack}, Cost_{Attack}) \quad (1)$$

5.3 Easier Alternative

This parameter relates the risk of an attack to another attack which is at a higher probability due to either increased severity or lower cost for a given network.

5.4 Target Network Characteristics

This parameter describes the features and characteristics of the target network. It encompasses other features such as system level misconfiguration [9], the unexpected side effect of operations [10] and platform specific attacks which can be exploited. Another factor that would be considered by an attacker is the type of traffic flowing through the network.

5.5 Cost of Attack

This parameter quantifies what it would cost an attacker to launch an attack. The three factors that make up this parameter are *Time*, *Strategy* and *Hardware*. It is evident that the first two factors are directly dependent on each other and it is the prerogative of an attacker to decide which factor is more important to him. These two factors affect the third factor – as the attacker has to invest in the appropriate hardware depending on which of the above two factors he gives more importance to.

5.5.1 Time

This parameter denotes the time taken for an attack which includes the time for gathering information and implementation.

5.5.2 Hardware Constraints

This parameter specifies the constraints that an attacker has to both work with or face when launching an attack. Suppose an attacker takes over a node in a Wireless Sensor Network. The energy constraint as well as the memory constraint would be a factor that would prevent him from making more complex attacks. On the other hand the same constraints (as the characteristic of the target network) also allow him in implementing a denial of service attack. Similarly the uncertainty of radio ranges [11] and radio hardware could affect the severity of his attack.

5.5.3 Strategy

This parameter features in the cost of an attack and is an important parameter. We further subcategorize it into:
1) Practical Difficulties: This factor considers the remaining aspect of difficulties while dealing with network hardware such as synchronization [12] and basic cryptography in networks. We also use this factor to represent the unpredictable behavior of the wireless medium which equally affects the attacker as the target network such as radio ranges.
2) Implementation: This refers to implementation difficulties of attacks due to built-in defenses in the target network or hardware constraints.
3) Identification of Network Protocols: The correct functioning of a network protocol relies on specifications and implementations [13]. However implementations are inherently more complicated and could introduce discrepancies and vulnerabilities, even though the analysis for soundness

validation may not discuss it [14]. It has been shown that most Internet protocols such as ICMP, TCP are subject to these discrepancies [15]. The universal presence of these discrepancies is due to the fact that network protocols cannot be completely and deterministically specified; instead opportunities are provided for implementations to distinguish itself [16]. The author of [17] states that the identifying protocols employs the following two methods:

Network Protocol Fingerprinting: This is the process of identifying a protocol by analyzing its output characteristics and traces based on the user input using tools like NMAP [18] or TBIT [19]. This method is called active fingerprinting since one can change the input to get different outputs. However it is also prone to alerting system administrators. Passive fingerprinting, where one does not provide inputs but only observes the output is a time intensive process. Further, it is extremely difficult to conduct rigorous proof about the validity of fingerprinting experiments [20]. It has been shown that the complexity and time required for fingerprinting make it infeasible in practice [16].

Network Protocol Fuzz Testing: This is the process of mutating the normal traffic to reveal unwanted behavior such as crashing or confidentiality violation [21]. However the authors also states that due to various factors this method is also mostly infeasible and inaccurate.

4) Selection: This denotes the methodology of the attacker including factors such as gaining information content by gathering and storing data, analyzing it to obtain target network characteristics, and verifying the results. Too aggressive methods of gathering data, could unintentionally alert a system administrator about the attacker's intention. The information content includes operating system, hardware, type of data, network protocols, purpose of network, size of network, topology, etc. We are specifically interested in identifying a network protocol which contrary to intuition, is much more complex. For instance, the author of [22] suggests that the difference among NewReno and Reno (TCP) can be discovered only when multiple packets are dropped within the same congestion window. This suggests that the time and resources required by an attacker to accurately assess a network protocol are important.

Figure 1 summarizes our risk model along with the underlying factors and their relationships. In the following section we use a qualitative approach to validate our risk model and highlight the novelty of our approach by evaluating the risk of a jamming attack against a network. We first present the risk analysis of the attack by evaluating it only from the defender's perspetive. We then show how our model, by incorporating the attacker's perspective, evaluates the same "highly" probable attack as a "low" probability attack.

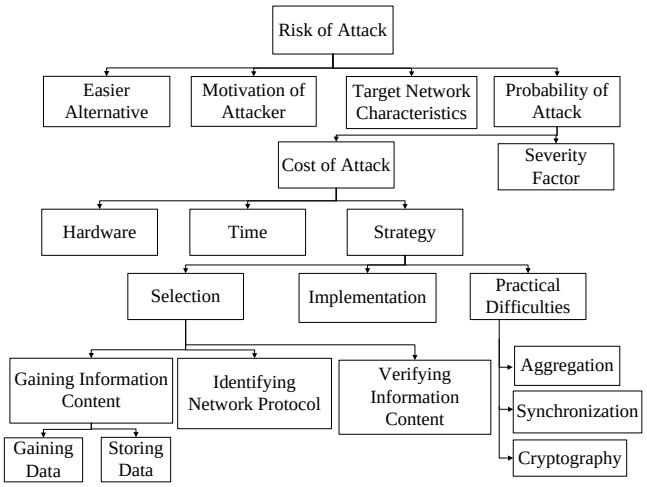

Fig. 1
RELATION BETWEEN FACTORS AFFECTING RISK ASSESSMENT IN OUR MODEL

6. Case Study-Jamming attacks

6.1 Overview

Jamming attacks target the Medium Access Control Layer (MAC) or the Physical (PHY) Layer of the OSI stack. This attack involves a jammer causing interference by emitting a RF signal continuously, disrupting the operations of a target network. However, the authors of [23], [24] state that a broader range of behaviors can be adopted by a jammer and a common characteristic of jamming attacks is that their communications are not compliant with the MAC protocols. They define a jammer as any entity interfering with the transmission or reception of wireless communications by either preventing a source from sending out a packet or reception of legitimate packets, leveraging mostly on the shortcomings of the MAC or PHY protocols. Any attack based on this idea is classified as a jamming attack.

6.1.1 Profiles of a Jammer

The success of a jamming attack like most attacks is dependent on the strategy chosen by the jammer. It must be noted that the strategy in this kind of attack includes both the layer of choice, i.e., either PHY or MAC and the model used to *jam* it. There are four different models or profiles of jammers – Reactive, Constant, Random and Deceptive [24].

6.1.2 Severity of Jamming Attack

Jamming attacks at the MAC level are effective due to the simple strategy and the difficulties in detection [23], [25]. Further since these attacks specifically target the protocols there are no effective means of circumventing the problem. Particularly, the problem lies in the inability of the

network devices to distinguish between *malicious* jamming and *unintentional* interference. The only effective solutions are changes to the MAC protocol or using expensive radio level technologies at the PHY level such as Direct-Sequence Spread Spectrum (DSSS) techniques [26].

6.2 Effectiveness of Jamming Attack

From a network perspective the effectiveness of jamming attacks is dependent on the following two necessary features of the network.

1) Target Network Characteristics: WSNs or Ad-Hoc Neqtworks are attractive targets due to their resource constrained nature since jamming attacks aim at depleting the energy of the devices by reducing their sleep times, increasing either the number or time of re-transmissions. Another characteristic of jamming is that it directly affects the data flow in a network making it effective against networks where data freshness is critical.

2) Hiding in Plain Sight: The success and effectiveness of the attack also depends on the jammer's ability to remain unidentifiable in the network. While a part lies in the implementation of the attack, a major part is the network's inability to differentiate between jamming and congestion. In addition to this it is also necessary that the network cannot identify the misbehaving devices. This implies that any kind of scheduled access to the medium is ruled out, as in such cases the jammer(s) can be easily identified and the network can differentiate if it is under attack.

6.3 Consideration of Jammer's Perspective

As explained in Section 6.1.2, the effectiveness and strategy of a jamming attack makes it hard for a network administrator to defend without investing in expensive countermeasures. Further, current countermeasures require an elaborate protocol of secret sharing for the scheme to be viable and effective. Since the defense strategies against these attacks are expensive, they are unlikely to be widely deployed. Considering this one would assume that such attacks would be nearly impossible to prevent or protect and should be widespread. However, the lack of evidence of such attacks in real-world [27] implies that while theoretically plausible there are some caveats that make them unpopular. This indicates that traditional threat modeling which considers only the defender's perspective does not encapsulate the risk convincingly. Further, it has to be noted that these attacks are unpopular from an $attacker's$ perspective which means that one has to consider an attacker's perspective. A reasonable explanation as to why such an attack is unattractive to an attacker could be that the effort required for successful initiation of the attack is large with diminishing returns or that the attack does not comply with the motivations of most attackers. For an attacker, the effort required for initiation is the effort (time and cost) to gain the information content that convinces him that the attack can be successful. Further, in DoS attacks an attacker's motivation is likely to be low since there is nothing tangible to gain. Since we are incorporating the attacker's perspective we have to also present some of the concerns in planning such an attack. In the following subsection we first present these concerns and try to analyze if one of the two factors mentioned above or a combination of them is the reason for the unpopularity of such attacks.

6.4 Attacker's Perspective and Concerns

To begin with an attacker has to spend considerable resources to ascertain that the network complies to the two necessary conditions described in Section 6.2. This includes finding the answers to the following questions:

1) What is the type of network? This critical question has to be addressed for the attacker to know what target network he is attacking.

2) Is the concern of the network energy or data freshness? This question would tell an attacker if a jamming attack is going to be effective or not.

3) What is the type of data flow in the network – Periodic, Query based or Event driven?

4) If the concern is data freshness, what are the standard packet sizes that flow in the network? Are there other features in the network such as aggregation or network coding? Answers to the above questions help in choosing the kind of jammer profile. Methods such as aggregation/network coding will reduce the effectiveness of the attack or require deploying/taking over more resources.

5) Identifying the *exact* protocol of the network. This is another critical dependency for an attacker. A motivating example for this is that the implementation of the attack is completely different in case of a CSMA MAC protocol from a preamble based MAC protocol. If the target network is running a schedule based MAC protocol, the attack will be ineffective.

6) Identifying physical access to the channel. What is the power required to jam? For example, if the devices transmit using BPSK or AM [28], due to the robustness of the signals the jamming attack may not be viable.

These are some of the concerns an attacker has to address to guarantee success to even an extent. However the following are also some additional practical concerns which an attacker needs to address.

1) What is the size of the network? What is its topology?

2) How to implement his attack? Does an attacker have physical access to the network? Where to place the jamming nodes?

Figure 2 presents the cookbook steps of an attacker's preparation for a jamming attack based on our analysis. The figure shows that there are 3 main steps for an attacker, namely, *Identifying Network Characteristics, Identifying Exact Protocols and Implementation Concerns*.

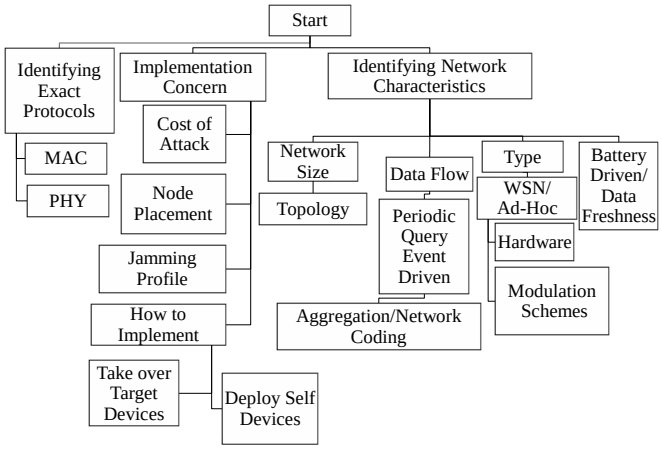

Fig. 2

STEPS AN ATTACKER HAS TO TAKE FOR A JAMMING ATTACK

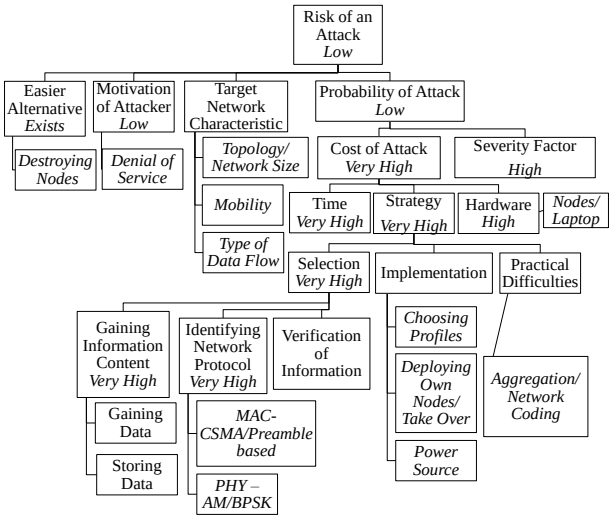

Fig. 3

RISK MODEL APPLIED TO JAMMING ATTACKS

6.5 Attack Implementation Concerns

Section 5.5.3 describes the concerns and analysis of identifying network characteristics and exact protocols. We now focus on the implementation concerns for the practical aspects of the attack. The implementation of the attack requires us to consider two scenarios as shown in Figure 2 – Takeover Target Devices or Deploy Own Devices. We present an analysis below:

1) Takeover Target Devices: In this scenario, the attacker has to take over the nodes of the target devices and use them in his attack. Since we do not consider human interaction, an attacker has to get within transmission range or have physical access to the devices. In cases of WSN or Ad-Hoc networks tamper proof (TPD) devices [29] could easily circumvent this problem. Further, if physical access is possible, then the attacker has easier options such as destroying them - a feasible alternative in a DoS attack.

2) Deploy Own Devices: Here, the attacker deploys his own devices. While this scenario is feasible and is likely to improve the success rate, the cost of attack also increases. The attacker has to invest in the devices just for denying service or interfering with the performance. Again easier alternatives such as destroying devices exists. The scenario of a more powerful device (such as a laptop) against sensors does exist, however the effect of jamming would be localized to a small region. Further, even in such cases the attacker too is restricted with the same energy constraints. Deploying more than one laptop will increase his cost of attack manifold.

The next aspect of implementation is choosing an optimum jammer profile since all the profiles are orthogonal to each other in terms of effect, cost and target networks.

1) Constant: This profile is effective on all kinds of protocols. However, the type of data flow also directly affects its efficiency. If the data flow is periodic, event driven or query based, constant jamming is going to be wasteful and will also affect the life of the jammer nodes as they need to transmit all the time.

2) Deceptive: This profile is very effective on a very small subset of preamble based protocol. However, it requires the jammer to be able to exactly ascertain the protocol as it has to send the exact preamble or the packet.

3) Random: This profile is the most efficient profile, provided that the jammer is able to configure the exact time/distribution of sleeping and jamming. Its efficiency reduces significantly in Event Driven networks and would not be effective at all in query based networks. It is again important to note that this profile attacks data freshness more than energy consumption.

4) Reactive: This profile is the most effective but also the least efficient since the jammer node has to be "ON" all the time. While it circumvents the amount of information content required by an attacker, networks with aggregation or small packet sizes would not be really affected. Further, considering that the energy consumption for reception is nearly equal to transmission, this profile would lead to wastage of energy.

The most important factor in this attack after observing the steps of a jamming attack is the cost of attack. This attack aims at a small subset of networks and requires too many necessary conditions for the attack to be successful. Simply put, this kind of attack extracts a huge cost in terms

of time and resources from the attacker, due to the amount of reconnaissance required. The description above leads to a risk model for jamming attacks as shown by Figure 3. This is an instance of the generic model from Figure 1 where the boxes represent the factors we have identified, with their respective values shown in italics.

7. Discussions

We have presented a new risk model that incorporates factors from the attacker's perspective. We believe this is a new approach that can be used for creating new proactive security and privacy schemes by including features such as obfuscation/confusion to provide efficient and practical measures. We have demonstrated the effectiveness of our model using jamming attacks as an illustration and also highlighted the novelty of our approach as compared to the generic approach in the literature that takes into account only the defender's perspective. Specifically we show how some of the assumptions made in the literature are questionable. While we have studied the attacks using a systematic qualitative analysis, our next step will be a more formal mathematical analysis for deeper insights into the complexity of attacks.

Acknowledgments

This research is supported in part by NSF Grant No. IIS-0916612. Usual disclaimers apply.

References

[1] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Computer Security Foundations Workshop, 2002. Proceedings. 15th IEEE*, 2002, pp. 49 – 63.

[2] P. Manadhata and J. Wing, "An attack surface metric," *Software Engineering, IEEE Transactions on*, vol. PP, no. 99, p. 1, 2010.

[3] M. Howard, J. Pincus, and J. Wing, "Measuring relative attack surfaces," *Computer Security in the 21st Century*, 2003.

[4] M. Barbeau, J. Hall, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks," in *In Proceedings of MADNES 2005 Workshop on Secure Mobile Ad-hoc Networks and Sensors - Held in conjunction with ISC2005*. SVLNCS, 2005.

[5] D. Geer and J. Harthorne, "Penetration testing: A duet," in *ACSAC*, 2002, pp. 185–198.

[6] S. Gupta and J. Winstead, "Using attack graphs to design systems," *IEEE Security & Privacy*, vol. 5, no. 4, pp. 80–83, 2007.

[7] Q. Duan, M. Virendra, and S. J. Upadhyaya, "On the hardness of minimum cost blocking attacks on multi-path wireless routing protocols," in *ICC*, 2007, pp. 4925–4930.

[8] C. Peikari and S. Fogie, *Maximum Wireless Security*. Indianapolis, IN, USA: Sams, 2002.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," *Security and Privacy, IEEE Symposium on*, vol. 0, p. 273, 2002.

[10] S. Chen, Z. Kalbarczyk, J. Xu, and R. K. Iyer, "A data-driven finite state machine model for analyzing security vulnerabilities," in *In IEEE International Conference on Dependable Systems and Networks*, 2003, pp. 605–614.

[11] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Impact of radio irregularity on wireless sensor networks," in *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*. New York, NY, USA: ACM, 2004, pp. 125–138.

[12] S. Dolev, S. Gilbert, R. Guerraoui, F. Kuhn, and C. Newport, "The Wireless Synchronization Problem," in *Proceedings of the 28th Annual Symposium on Principles of Distributed Computing*, 2009.

[13] D. Lee, D. Chen, R. Hao, R. E. Miller, J. Wu, and X. Yin, "A formal approach for passive testing of protocol data portions," in *ICNP '02: Proceedings of the 10th IEEE International Conference on Network Protocols*. Washington, DC, USA: IEEE Computer Society, 2002, pp. 122–131.

[14] G. Lowe and B. Roscoe, "Using csp to detect errors in the tmn protocol," *IEEE Trans. Softw. Eng.*, vol. 23, no. 10, pp. 659–669, 1997.

[15] R. Beverly, "A robust classifier for passive tcp/ip fingerprinting," in *PAM*, 2004, pp. 158–167.

[16] G. Shu and D. Lee, "Network protocol system fingerprinting – a formal approach," in *Proceedings of IEEE Infocom*, 2006.

[17] G. Shu, "Formal methods and tools for testing communication protocol system security," Ph.D. dissertation, Ohio State University, 2008.

[18] F. Yarochkin., "Remote os detection via tcp/ip stack fingerprinting." 1998, http://www.insecure.org.

[19] J. Padhye and S. Floyd, "On inferring tcp behavior," in *In the proceeding of SIGCOMM*, 2001, pp. 287–Ű298.

[20] D. Lee and K. Sabnani, "Reverse-engineering of communication protocols," in *Network Protocols, 1993. Proceedings., 1993 International Conference on*, 1993, pp. 208–216.

[21] O. Arkin and F. Yarochkin, "Xprobe2 - a 'fuzzy' approach to remote active operating system fingerprinting." 2002, http://www.sys-security.com.

[22] K. Fall and S. Floyd, "Simulation-based comparisons of tahoe, reno and sack tcp," *SIGCOMM Comput. Commun. Rev.*, vol. 26, no. 3, pp. 5–21, 1996.

[23] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *Network, IEEE*, vol. 20, no. 3, pp. 41–47, 2006.

[24] Y. Chen, W. Xu, W. Trappe, and Y. Zhang, *Securing Emerging Wireless Systems: Lower-layer Approaches*, 1st ed. Springer Publishing Company, Incorporated, 2008.

[25] A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[26] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*. Artech House Publishers, 2006.

[27] S. Peters, *2010 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute, December 2009.

[28] J. G. Proakis and D. K. Manolakis, *Digital Signal Processing (4th Edition)*. Prentice Hall, Mar. 2006.

[29] P. Ning and W. Du, "Journal of computer security," January 2007.