# Threat Model Based Security for Wireless Mesh Networks

Freshta Popalyar(✉)

Department of Telecommunication Systems, Communication and Operating Systems, Technische Universität Berlin, Berlin, Germany
Popalyar@win.tu-berlin.de

**Abstract.** Wireless Mesh Network (WMN) is a technology, which has gained popularity due to its cost effective design, robustness, and reliable service coverage. Despite the advantages, WMNs are considered vulnerable to security breaches. Thereby, it is important to consider security in the early design phase in WMNs. Identifying security threats helps the system designer in developing rational security requirements. In this paper we propose threat modeling as a systematic approach to pinpoint the security threats for WMNs as basis for developing security requirements. We identify assets, value them and categorize possible attacks that target the assets in a layer-wise manner. We further elucidate our threat model by use of Attack Trees to clearly define vulnerabilities in the system during early design phase. We take the example of Schools' WMN in a district of Kabul City in Afghanistan as our scenario. We briefly discuss how to assess the risks that are associated with the specified WMN based on the information that is derived from the threat model.

**Keywords:** Wireless Mesh Networks · Security · Threat model · Attack Tree

## 1 Introduction

Wireless Mesh Network (WMN) is a promising technology which is characterized as a robust, scalable, resilient, cost effective and easily maintainable and manageable network technology [1]. As WMN owns such qualities it is considered a good network solution for developing countries and organizations/institutions with low budget. In contrast, with the advantages of WMNs there are a number of problems associated with general performance of WMNs. One of the main concerns regarding WMNs is security [1–3,8,9]. The vulnerabilities existing in every layer of wireless mesh network stack pose threats and risks that need to be mitigated. There are many intrusion detection systems available and a number of security mechanisms and techniques have been proposed. But it is important to realize whether the features included in the security systems are required and whether they can fulfill the security requirements of the WMN. It is the responsibility of the system designer to resolve such doubts regarding security of the


S. Sigg et al. (Eds.): MobiCASE 2015, LNICST 162, pp. 325–332, 2015.
DOI: 10.1007/978-3-319-29003-4_20

system in the design phase of WMN during elicitation of the security requirements of the system. Generally considering security requirements of the system in the early design phase can save time and financial resources [4]. Therefore, before incorporating the security measures, the system designer should utilize a systematic approach that involves identifying risks, requirements, risk mitigation strategies and looking at the system from the adversary's perspective.

Threat modeling helps in rationalizing the chosen security measures for a system and verifying the security decisions of system designer [4]. Previously threat modeling was used for application security modeling [12], but recently it has been adopted by researchers in the areas of Mobile Ad hoc Networks and Wireless Sensor Networks [13–16]. There is still a lack of literature on threat modeling and attack tree definition for WMNs.

In this paper we propose Threat Modeling as a systematic approach to pinpoint the security threats for WMNs as basis for security requirements in the initial design stage of developing a WMN. We identify assets, value them and identify threats to assets. To elucidate the threat model we use Attack Tree to view the system from the attacker's perspective and develop attack trees to clearly define vulnerabilities in the system during early design phase. Moreover, the proposed approach considers a layer-wise classification of threats in WMNs, since attacks can happen in every layer of WMN network stack. The proposed approach can also be used in existing WMNs where security measures need to be reimplemented.

Obtaining spatio-temporal attack information in WMNs can help in understanding which kinds of attacks are targeting WMNs. According to [22], adapting the definition of Situation, it is implied that an attack on the WMN is an actionable event and can be observed in time. Furthermore, situation modeling is used to derive information about an occurrence, sequence of events and set of events [23]. Thereby, we use the concept of situation modeling (attack/threat modeling) to obtain information about attacks in WMNs. We take the example of Schools' WMN in a district of Kabul City in Afghanistan as our scenario. We briefly discuss how to assess the risks that are associated with the specified WMN based on the information that is derived from the threat model.

The rest of the document is structured as follows: The threat model is described in Sect. 2. Risk assessment is presented in Sect. 3 and the conclusion is presented in Sect. 4.

## 2 Threat Model

A threat is a goal of an adversary that if achieved can harm the system. Protecting a system from threats is one of the most important aspects in a system's security. Securing a system against threats and risks is a process that carries out identification of the risks and threats, figuring out the ways to mitigate the risks and developing security strategies to omit them [11].

WMNs are generally considered not secure enough and there are various research being conducted on security of WMNs [1–3,8,9]. There has been less

attention devoted on embodying security in WMNs in the design phase and threat modeling for WMNs. On the contrary several research in the same area have been accomplished for other similar network types such as Mobile Ad hoc Networks and Wireless Sensor Networks [13–16]. For this reason we proposes a threat model based approach to secure WMNs in the early design phase. According to [4], to create a threat model for a system it is crucial to accomplish the following sub processes; (i) characterizing the system, (ii) identifying assets and (iii) identifying threats. Our work differs from the existing bodies of work because we tailor the threat modeling steps to suit WMNs and focus on layer-wise derivation of attack information in WMN. The necessary steps taken towards threat model in this paper are described as follows.

- To understand the system a network model needs to be created for the network scenario which is shown in Fig. 1.
- The assets of the intended network are identified based on the scenario.
- Possible attacks that target the identified assets are listed and categorized based on the network layer in which a certain attack can occur. To elaborate the threat model and obtain clear attack information for the WMN, Attack Tree modeling method is used.

### 2.1 Scenario

As the first step in threat modeling is to understand and realize the intended network, the network model of the scenario used in this work is described and illustrated in this section.

The environment of a network of schools in a district of Kabul, Afghanistan is used as the scenario for this work. The network considered is based on the administrative structure of schools and their relation to the Education Directorate of the City (EDC) in Afghanistan. The Education Directorate in every city is a representative of Ministry of Education and is responsible for collecting data from all schools in a city. At the end of every semester and school year, data is transfered from the school to Education Directorate of City. Thus the schools need to be connected to the EDC.

The structure of wireless mesh networks considered is based on three tiers which is depicted in Fig. 1. The bottom most tier is where the mesh clients (MCs) are. These are the nodes that belong to the users of the services provided by the school's network. The mesh routers (MRs) that provide connectivity to mesh clients are located in the intermediate tier. These routers are stationary nodes that are responsible to connect the schools to the gateways. And in the topmost tier the gateways are located.

### 2.2 Assets

Identifying assets of the network is a critical step in threat modeling [4]. Assets are the target of attackers in a network. If there were no assets there would be no attacks.

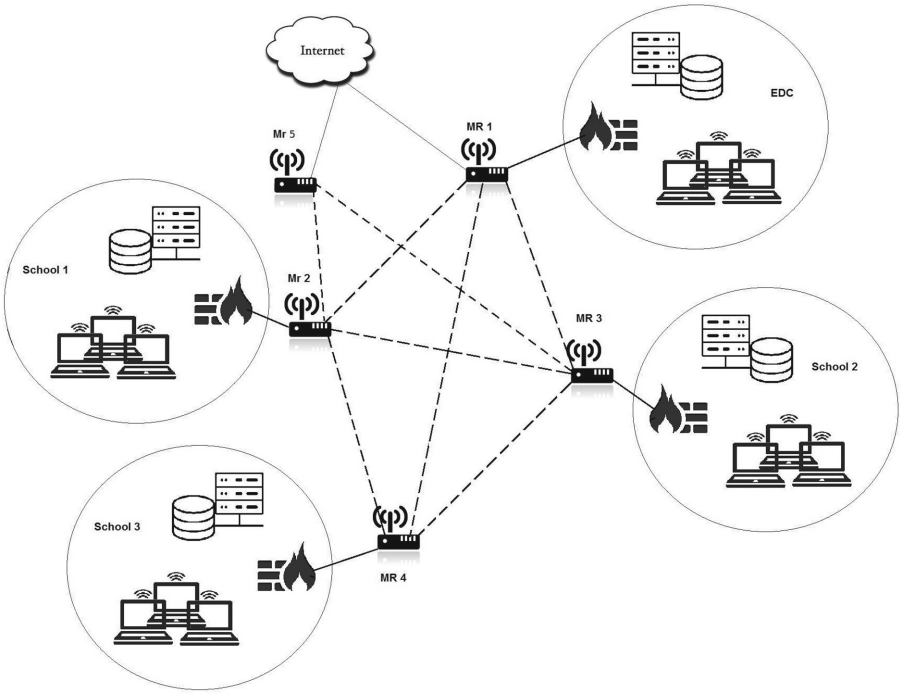


**Fig. 1.** The Wireless Mesh Network of Schwools

According to the illustrated scenario (Fig. 1), there are a number of services that run on the servers of the school and the education directorate. Each of the services are considered as assets. These services include; DHCP, DNS, Web Service, Email, authentication, user's database, employee information database, student information database. Additionally, availability of the network is one of the most important assets. The assets identified for the intended network are described as follows.

- Availability of the network
- Integrity of the school's data
- Confidentiality of the school's data
- The Software installed in user nodes and servers
- Hardware of all network components

**Asset Valuation.** Since assets can be tangible or intangible [10], in the network considered in this work the tangible assets are software systems and hardware and the intangible assets include; availability of the network and services, data integrity and confidentiality. It is assumed that the hardware and software assets are kept safe against attacks in the scenario used in this work and only the Availability, Integrity and Confidentiality of data are taken in consideration that have relatively high value of importance.

### 2.3 Possible Attacks

The best way to list possible attacks for a system is to identify threats based on every asset on the network. Threats/attacks aim towards one or more assets [4]. The assets for the scenario are identified in the previous section. The following table (Table 1) pinpoints the attacks that can happen on every identified asset on the intended WMN according to [9,24] and the attacks are categorized layer-wise. The layer-wise categorization of threats on assets helps the system designer in decision making on employing and developing security countermeasures.

**Table 1.** Layer based categorization of possible attacks on identified assets

| Assets | Possible attacks | Layers |
|---|---|---|
| Availability | Signal jamming Intentional collision of frames, virtual jamming UDP flood, ICMP flood DoS attacks, DDoS DNS spoofing, TCP SYN flood, de-synchronization | Physical data-link network transport |
| Data integrity | Mac spoofing session hijacking | Data-link transport |
| Confidentiality | Replay attack, eavesdropping and man-in-the-middle, mac spoofing, pre-computation and partial matching | Data-link |
| Software | Worms and viruses | Application |
| Hardware | Device tampering and physical damage | Physical |

**Attack Tree.** Threat-logic trees were first introduced by Weiss [17] which were used for analyzing failure conditions of complex systems [19]. Later the idea of "Attack trees" was popularized by Bruce Schenier [5,18,19] which was based on the original fault tree idea. Attack trees are defined as a systematic approach for characterizing system security based on different types of attacks that can be launched on the system [6]. In an attack tree, the root of the tree represents the threat, in other words the root of the tree is the main goal of the adversary. Considering that, to reach the goal, the adversary has to achieve the subgoals that are presented by each child node in the attack tree. Thus the leaf nodes show the starting points of the attack. Subgoals in the attack tree can be either conjunctive (AND decompositions) or disjunctive (OR decompositions) [7]. As a result each path on the tree shows a distinct attack on the system [6].

Attack trees are considered one of the most popular methods of graphical security modeling [17].In this approach it is proposed to model the WMN threats using Attack Trees. Because Attack Tree presents a visual way of depicting security holes and help in better understanding the underlying security threats and vulnerabilities in a system.

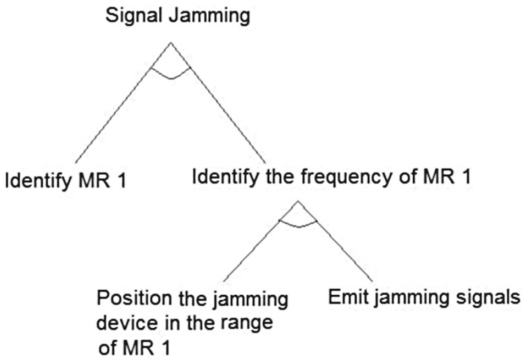


**Fig. 2.** Attack tree for signal jamming attack

In order to complete the threat model it is necessary to develop attack trees for each possible attack and create a forest of attack trees [6]. Furthermore, by using the attack trees specification of other attributes of the threats to the system such as cost, possibility and impossibility, ease and difficulty can be determined [7].

An attack tree for Signal Jamming attack is presented as an example which is depicted in Fig. 2 which is based on the network model illustrated in Fig. 1. The result of an In-order traversal of the attack tree gives the method the attacker should use to jam the intended network, which in the given example would be; *Identify MR 1 (see Figure 1.) AND Identify its frequency range, Position the jamming device in the range of MR 1 AND emit jamming signals.*

Similar to the presented example it is necessary to create attack trees for each identified attack and develop the attack forest for the network. Once the attack tree for every possible attack is depicted and vulnerabilities of the network are known, it is relatively important to analyze the risks associated with each threat. Risk assessment helps us to rank threats based on the level of their risk and based on the level of the risks, they can be prioritized and risk mitigation strategies can be applied accordingly.

## 3 Risk Assessment

Threat modeling and risk management are related processes [21]. In order to manage risks by applying risk mitigation strategies it is crucial to asses risks in this stage.

The relationship between threat, risk and vulnerability is explained in [20], which can be summarized in the following sentence. Threat exploits vulnerability and both threat and vulnerability increase risk. Thus defining the probability of threat and the level of vulnerability for every asset defines the risk associated with the asset and the impact that the risk can have depends on the value of the asset under threat. Considering this explanation the following formula is acquired [21] that we use for calculating risk of attacks in WMN:

Risk = Vulnerability Level x Threat Probability x Asset Value

At this point the systematic approach for securing WMNs at the early stage of design is finalized. Based on the identified assets, their evaluated threats and known layers of vulnerabilities, risk of attacks in WMN can be calculated and decisions can be made on risk mitigation strategies that need to be applied to secure the intended WMN.

## 4 Conclusion

Distinct characteristics of a Wireless Mesh Network such as its broadcast nature and use of shared wireless media make it vulnerable to security threats. This paper proposes a threat model based approach for securing WMNs during early design phase where threat modeling is used as the basis of WMN security requirements. Throughout the paper, assets of the network are identified based on the scenario, threats for every asset are pointed and categorized in a layer-wise manner. The attack tree is used to elaborate the threat model and an example attack tree is developed. Lastly, risk assessment methods for possible attacks are discussed.

Once the threat model is created the WMN's threats and security requirements are identified. Based on the information derived from our threat model proper ways to mitigate the risks can be figured out and security mechanisms for the WMN can be developed. These two steps are considered as future work.

## References

1. Akyildiz, I., Wang, X.: Wireless Mesh Networks, vol .1. John Wiley and Sons Inc., UK (2009)
2. Khan, S., Pathan, A.S.K.: Wireless networks and security: issues, challenges and research trends. In: SCT, pp. 189–272 (2013)
3. Sen, J.: Security and Privacy Issues in Wireless Mesh Networks: A Survey, Innovation Labs. Tata Consultancy Services Ltd., Kolkata (2013)
4. Myagmar, S., Lee, A.J., Yurcik, W.: Threat modeling as a basis for security requirements. In: Symposium on Requirements Engineering for Information Security (2005)
5. Schneier, B.: Attack trees: modeling security threats. Dr. Dobbs J. **24**(12), 21–29 (1999)
6. Moore, A.P., Ellison, R.J., Linger, R.C.: Attack Modeling for Information Security and Survivability. Software Engineering Institute, Pittsburgh (2001)
7. Mauw, S., Oostdijk, M.: Foundations of attack trees. In: Won, D.H., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 186–198. Springer, Heidelberg (2006)
8. Siddiqui, M.S., Hong, C.S.: Security issues in wireless mesh networks. In: The Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07), Seoul, Korea, pp. 717–722 (2007)
9. Sen, J.: Security and privacy issues in wireless mesh networks: a survey. In: Khan, S., Pathan, Al-SK. (eds.) Wireless Networks and Security. SCT, vol. 2, pp. 189–272. Springer, Heidelberg (2013)
10. Allee, V.: Value network analysis and value conversion of tangible and intangible assets. J. Intell. Capital **9**(1), 5–24 (2008)

11. McGraw, G., Allen, J.H., Mead, N., Ellison, R.J., Barnum, S.: Software Security Engineering: A Guide for Project Managers. Addison-Wesley Professional, Boston (2008)
12. Johansson, J.M., Riley, S.: Protect Your Windows Network From Perimeter to Data. Pearson Education Inc., USA (2005)
13. Spiewak, D., Engel, T., Fusenig, V.: Towards a threat model for mobile ad-hoc networks. In: Proceedings of the 5th WSEAS International Conference on Information Security and Privacy, Venice, Italy, 20–22 November 2006
14. Clark, J.A., Murdoch, J., McDermid, J.A., Sen, S., Chivers, H., Worthington, O., Rohatgi, P.: Threat modelling for mobile ad hoc and sensor networks. In: Annual Conference of ITA (2007)
15. Hasan, R., Myagmar, S., Lee, A.J., Yurcik, W.: Toward a threat model for storage systems. In: Proceedings of the 2005 ACM Workshop on Storage Security and Survivability, pp. 94–102. ACM, New York (2005)
16. Zalewski, J., Drager, S., McKeever, W., Kornecki, A.J.: Threat modeling for security assessment in cyberphysical systems. In: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop. ACM, New York (2013). Article No. 10
17. Kordy, B., Mauw, S., Radomirovi, S., Schweitzer, P.: DAG-based attack and defense modeling: dont miss the forest for the attack trees. Comput. Sci. Rev. **13**(14), 1–38 (2014)
18. Kordy, B., Mauw, S., Radomirovi, S., Schweitzer, P.: Attack Defense Trees. Oxford University Press, New York (2012)
19. Steffan, J., Schumacher, M.: Collaborative attack modeling. In: Proceedings of the 2002 ACM Symposium on Applied Computing, pp. 253–259. ACM, New York (2002)
20. Arnes, A.: Risk, Privacy, and Security in Computer Networks, Ph.D. thesis (2006)
21. UcedaVelez, T., Morana, M.M.: Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Wiley, Hoboken (2015)
22. Singh, V.K.: From multimedia data to situation detection. ACM, Scottsdale (2011)
23. James, L.: Crowley, patrick reignier and remi barranquand, situation models: a tool for observing and understanding activity. In: Proceedings of IEEE ICRA, Workshop of People Detecting and Tracking, Kobe, Japan, May 2009
24. Glass, S., Portmann, M., Muthukkumarasamy, V.: Securing wireless mesh networking. IEEE Internet Comput. **12**, 30–36 (2008)