The Analysis of Improved Network Security Model Based on Dynamic Wireless Networks

Lifang Lu [1, a]

[1]Yunnan Physical Education College of Qujing Normal University, china

[a] molifangfei@126.com

Keywords: Dynamic wireless networks, Network security model, Dynamic self-adjusting.

Abstract. Nowadays, dynamic wireless network security model flawed in terms of initiative defense, risk assessment and security policy generation and others. To solve this problem, we proposes an improved model of network security model based on dynamic wireless networks. This network security model is mainly characterized by the data flow through the match, responsible for detecting and filtering traffic; is detected and analyzed data packets flowing based on a security policy ; increases the corresponding new security policy based on logging, to achieve a response control and interaction by AP interactive connections. The improved model can achieve a good dynamic security policy self-regulating, be effective to solve the coordination and policy updates about wireless network outside the mobile terminal and the access point. Based on this, the research mainy analyzes network security model based on improved dynamic wireless networks.

Introduction

Dynamic wireless network is proposed based on the popularity of network applications and network-dependent people to gradually increase, but the limitations of traditional networks to increase. Dynamic wireless networks have high flexibility, low cost networking, easy operation, and so on, so it gets more customers. But nowadays, dynamic wireless network security model flawed in terms of initiative defense, risk assessment and security policy generation and others. To solve this problem, we proposes an improved model of network security model based on dynamic wireless networks. This network security model is mainly characterized by the data flow through the match, responsible for detecting and filtering traffic; is detected and analyzed data packets flowing based on a security policy ; increases the corresponding new security policy based on logging, to achieve a response control and interaction by AP interactive connections. The improved model can achieve a good dynamic security policy self-regulating, be effective to solve the coordination and policy updates about wireless network outside the mobile terminal and the access point.

Dynamic wireless network security model

Dynamic wireless network security model consists of four major components: security policy; protection; testing; response. It is single-line type of protection based on a static open-loop control mechanism. When the dynamic wireless network security model runs, firstly it saves the security policy to the corresponding strategy warehouse. A wireless network entity may beautomatically run based on policy task .Dynamic wireless network security model's mathematical description:

$$P_t > D_t + R_t \tag{1}$$

P_t represents the required time protection after a network security policy settings. D_t represents a time network intrusion detection of illegal acts needed. R_t represents the network by the impact of the illegal invasion, then the time required to adjust the network normalization[1].Equation (1) shows that, if the detection time plus the adjustment time is less than the guard time, it can be considered that the wireless network is in a safe condition. Dynamic wireless network security model is focused on the dynamic nature of network security, emphasizing positioning and regulatory capacity, and can achieve real-time monitoring and effective assessment, timely detect

threats to improve security of the system. But the dynamic wireless network security model flawed in terms of defense initiative, risk assessment and security policy generation. Thus proposes an improved model of network security model based on dynamic wireless networks.

Improved model of dynamic wireless networks security model

Dynamic wireless network security model flawes in terms of initiative defense, risk assessment and security policy generation and others. Thus requiring dynamic wireless network security model must be distributed strategy to achieve self-regulating dynamic security policies to effectively address coordination and policy updates wireless network outside the mobile terminal and the access point.

Improved model's architecture.

The improved model's architecture is shown as Figure 1:

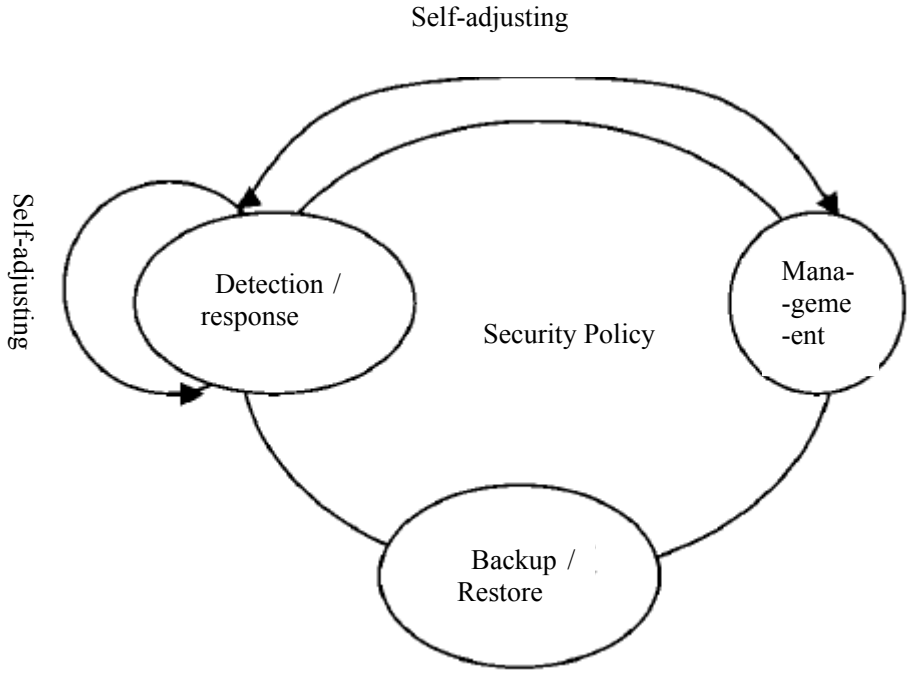

Fig. 1 Architecture in dynamic wireless network security model based on improved

In Figure 1, Detection / response section is made up of several different functions, unified architecture with self-adjusting filters and the adapters with interaction coordination, management, safety testing, and other responses. Security policy part by policy management tools and security controller, can be considered as an administrator by policy management tools related network management regulations into understandable and suitable for global wireless network security policy; Backup / Restore section is mainly based on the database server policies and rules for storage and recovery security policy and data sources.

Self-adjusting filter architectural of model improvements. In the dynamic wireless network, self-adjusting filter is mainly characterized in the data flow through the matching is responsible for detecting and filtering the flow. In addition, self-adjusting filter also implement data traffic Comparative analysis, and view it as a data source for mining, digging out the wireless network feature new threats, and generate the corresponding security policies. Self-adjusting filter architecture is shown as Figure 2.

Figure 2 shows that self-adjusting filter includes a policy enforcement, protected application, parameter measurement, intelligent assessment and policy generation module.

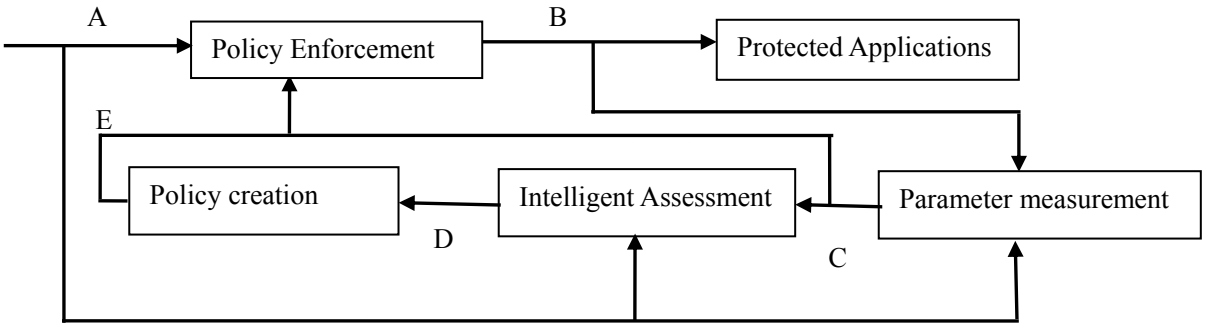

Figure 2 Self adjusting filter architecture

Policy enforcement module of model improvement. Strategy execution model is mainly for mobile devices and servers proxy related processes, is the core component of the entire wireless network security model, usually embodied in the wireless router, access point (AP), mainly responsible for detecting the presence of wireless network security risks[2].Wireless network policy enforcement mainly acquires transmitted data packets in real-time , detectes data packets and generates security policy , make feedback response through interaction with the AP and other equipment .In this paper, policy enforcement module based on dynamic wireless networks improved model mainly composes of self-adjusting filters, communication management unit, a feedback response interactive adapters and other accessories. Self-adjusting filters is in series, parallel or series-parallel combination of ways to set up, to detect and analyze flowing data packets based on the security policy, for the risk of packet to intercept and log . Meanwhile, according to a corresponding logging increases new security policy.

Operational process of model improvement. When a new security policy is in creation, in order to be able to enhance the security of dynamic wireless network security model, it should be useful to policy controller updated in real time to generate a new suit local wireless network security strategy, and concurrent to the policy enforcement module. In other words, the dynamic model of wireless network security improvements after detecting network threats, must be able to achieve real-time security response [3]. This function mainly based on self-adjusting filters generates updated security policy rules, connects via AP interactive response, control and interaction.

Wireless network traffic is dynamic, so the improvement of safety management model is a dynamic process, and there should be continuous monitoring of wireless networks, security issues to find protection and timely response [4] . The problem should be noted : Each sub-process improvement model dynamic wireless network security is likely to generate feedback, not only through these regular feedback information in order to make the security model to achieve the best state, but the process itself that is a continuous cycle of spiraling process.

Conclusion

Simulation of network security model based on dynamic wireless network is to use SWARM software to emulate. simulation model is based on Agent to model. Each Agent on behalf of a dynamic wireless network attacks and analogs transmission network traffic. The simulation results of the initial attack is shown as Fig. 3:

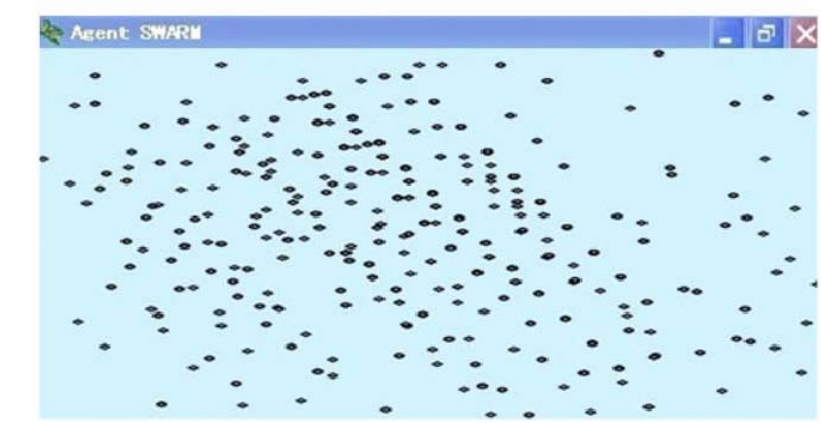

Fig. 3 The simulation results of the initial attack

Fig. 3 shows that in the initial attack simulation process, the data for each Agent is disorderly distributed. Through improved dynamic wireless network security model simulation results is shown as Figure 4. It shows that the attack data into normal data, reaches a relatively stable wireless network status.

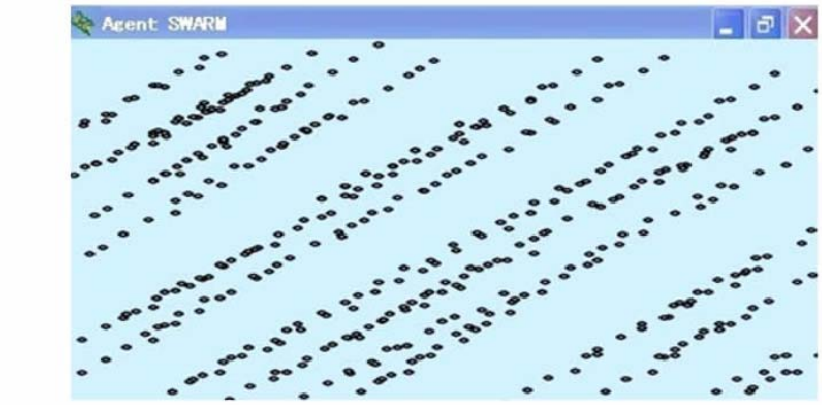

Fig. 4 The simulation results of dynamic wireless network security model based on the improved filter

To sum up: Improved dynamic wireless network security model uses a distributed strategy, through self-adjusting filters, policy enforcement module to be effective realization of the self-regulating dynamic security policy to solve the wireless network between the mobile terminal and the external access point coordination and policy updates.

Reference

[1] Jamalipour A, Wada T, Yamazato T. Atutorial on multiple acess techonologies for beyond mobile networks. Communications Magazine, IEEE, 2005, 43(2): 110-117.

[2] K.Z. Huang，X.J. He, P. Zhang, ect. Heterogeneous Wireless Networks dynamic trust model based on fuzzy sets. Computer Applications, 2010(8): 2111-2113.

[3] K.Z. Huang, J.X. Wu. The fourth generation of mobile wireless network management protocol analysis. Computer Engineering and Design, 2007(19): 4645-4648.

[4] Y.Y. Cheng, Knowledge of wireless network optimization model for automatic acquisition. Telecommunication Technolog, 2010 (12): 9-13.