Model the Flow Control Attack in Wireless Networks

Wei Wang *
Science and Technology on Communication Information Security Control Laboratory
Jiaxing, China, 314001
wwzwh@163.com
* Corresponding Author

Wenhong Zhao
Nanhu College
Jiaxing University
Jiaxing, China, 314001

Abstract—To analyze the attack on mechanisms of confliction in wireless networks, a new method based on the system stability is introduced. Firstly, the theoretic basis for flow control attacks is discussed, which shows that the flow control attack may destroy data stream and network system at a low speed. Then, the procedure of flow control attack is analyzed and the basic attack method and double speed attack method is presented. At last, the efficiency of flow control attack is discussed from two aspects: link throughput and link utilization. The results show that the flow control attack may cause great harm to wireless networks.

Keywords-System Stability; Flow Control Attack; Confliction Tetransmition; Window adjustment; Network Security

I. INTRODUCTION

Attack to wireless communication networks is of great significance for the research of network security. Many researchers have made a lot of relevant researches [1-9]. Tao Yuan et al established network attack situation model based on factors neural network theory, defined the relevant factors of network attacks, extracted network attack situation factor vine through attack situation, analyzed according to the given time window and displayed corresponding attack situation of the overall effect of network attacks [1]. Wang Qian et al constructed a multidimensional classification model and established attack ontology model by making use of the logic relationship and hierarchy structure among the concepts of attack ontology so as to attack the target system by making use of the attack scenario of attack atomic ontology structure [2]. Zhang Junyi discussed the intelligent lamming attack and deception jamming in single-node and multi-node collaborative methods to Ad Hoc networks based on MAC protocol and compared the interference effects of different ways [5]. Yu Ling et al proposed the algebraic method for the victim host to reconstruct the attack path based on the address information in the marked message by marking the address of the router with message at a certain probability by making use of the option field in IP message [8]. Zhang Yuegong et al analyzed the security enhancement due to IPv6 and new network attack and intrusion methods introduced by IPv6, especially the network intrusion during the transition from IPv4 to IPv6 [9].

However, the above methods need the precondition of decryption so that it is difficult to realize information attack on the encrypted wireless network in the short term. Thus, it is necessary to carry out effective research on wireless communication network attack techniques against this situation. Aiming at these problems, the feasibility analysis is made into the flow control attack of confliction retransmission-window re-adjustment mechanism based on the system stability, then a specific attack method is proposed, and finally the attack effect is analyzed.

II. THEORETICAL BASIS FOR FLOW CONTROL ATTACKS

In case of attacks on wireless networks, it is often the case that it is unable to master network protocol field and details but can only grasp some network protocol operation mechanisms (for example, only protocol operation mechanism can be got from network signal time-domain graph. It can be seen from Fig. 1 that confliction retransmission mechanism is adopted in this network protocol, and it can be seen from Fig. 2 that window flow control mechanism is adopted in this network protocol)[10-13]. This paper aims to research effective attack methods for the wireless network protocol in case of only master of the confliction retransmission-window re-adjustment function and mechanisms.

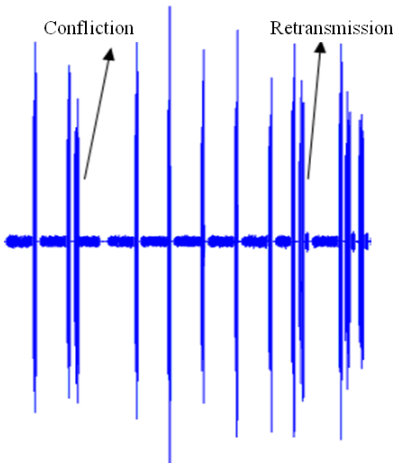

Figure 1. Confliction-retransmission mechanism

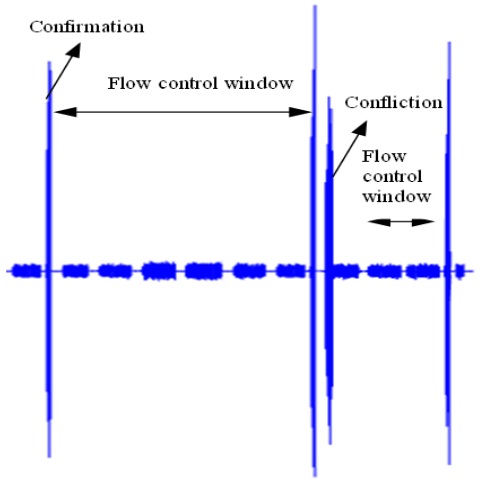

Figure 2. Window flow control mechanism

First, the possibility of flow control attack is described through theoretical analysis. Π is defined as the ratio of the loss caused by the attack method and the attacker's resource consumption: $\Pi = \frac{Damage}{Cost^{\frac{1}{\Omega}}}$, wherein the parameter Ω is used to describe the attacker's aggression. The greater the Ω is, the more resource will be used by the attacker to achieve the expected destructive effect. Storm deny of service attack is the reflection of high Ω value. For wireless network, traffic model is available:

$$\frac{d}{dt}x_r(t) = \kappa\left(w_r - x_r(t)\sum_{l\in r} p_l(\sum_{l\in s} x_s(t))\right) \quad (1)$$

Wherein, κ represents the link gain, wr represents additional increase of the speed rate, $x_r(t)\sum_{l\in r} p_l(\sum_{l\in s} s_x(t))$ represents the multiplicative reduction of the speed rate, and $p_l(\cdot)$ reflects the resource consumption caused by the feedback of the input load changes on the link to the source terminal. The system Lyapunov function is as follows:

$$U(x) = \sum_{r\in R} w_r \log x_r - \sum_{l\in L}\int_{y=0}^{\sum_{l\in s} x_s} p_l(y)dy \quad (2)$$

Wherein, $U(x)$ represents the network gain, $\sum_{r\in R} w_r \log x_r$ represents the gain of the transmission rate, and $\sum_{l\in L}\int_{y=0}^{\sum_{l\in s} x_s} p_l(y)dy$ represents the sum of loss on the relevant link L, and s is the speed rate set on a particular link $l \in L$. Lyapunov function stability analysis indicates that the system will converge to a steady state x^*r to realize the maximum $U(x)$. Namely, for all r, in case of $x_r(t) \neq x^*_t$, then $\frac{d}{dt}U(x(t)) > 0$. In case of $xr(t) = x^*r$, then $\frac{d}{dt}U(x(t)) = 0$.

Steady-state rate x^*t can be obtained by solving the following partial differential equation:

$$\frac{\partial}{\partial t}U(x(t)) = \frac{w_r}{x_r} - \sum_{l\in r} p_l(\sum_{l\in s} x_s) \quad (3)$$

Assuming that the system can converge from any initial state $x_r(0)$, if the system fluctuates around the stable state, by introducing the linear model $x_r(t) = x_r^* + \sqrt{x_r^*}\,y_r(t)$ of the variable $y_r(t)$, the following can be obtained:

$$\frac{d}{dt}y(t) = -\kappa(WX^{-1} + X^{1/2}A^T P'AX^{1/2}) = -\kappa\Gamma^T\Phi\Gamma y(t) \quad (4)$$

Wherein W, X and P' are diagonal matrix, and the diagonal elements are the differential of w_r, x^*_r and $p_l(\sum_{l\in s} x_s^*)$ respectively. Matrix A is of L^*R dimension. In case of connection of r by making use of the link l, $a_{1r}=1$. The diagonal of the diagonal matrix Φ gives the eigenvalues of the system. Extremely minimal eigenvalue is λ, wherein the higher λ is, the faster the fading of the system is and the faster the convergence is.

Assuming the network system has been stable at x^*r state, since the link is accustomed to the maximized capacity, the increased attack load will result in high feedback cost, making the link close to saturation. The flow control attack introduces the data with sustained rate of δ and time units of τ, the new stable point of the system is denoted as $(x')^*r$, and λ' is the new minimum eigenvalue, which means the rate in case of convergence to a new stable point. After time τ, the capacity of the attacked link is effectively reduced. With the stability of the system on the new $(x')^*r$, flow control attack stops, and the system will return to the state x^*r, repeat the above attack modes again and switch among different states.

For a given value of Ω, there is a peak attack rate, which enables the greatest attack power, namely that the flow control attacker can inject appropriate attack data stream at the appropriate time to guide the system to an unstable state, resulting in higher attack cost-efficiency.

As can be seen from the above theoretical analysis, the flow control attack can attack data stream and network system at a low speed, which is featured in improving network attack cost-efficiency and reducing the probability of its being found by IDS so that it is more suitable for network attacks on wireless networks.

III. FLOW CONTROL ATTACK METHOD FOR CONFLICTION RETRANSMISSION-WINDOW RE-ADJUSTMENT MECHANISM

The flow control function of wireless networks adopts a lot of confliction retransmission-window re-adjustment

mechanism (such as the packet confirmation mechanism for link layer and transport layer), and this mechanism is easy to be found by network reconnaissance system. Therefore, appropriate flow control attack methods are introduced in the condition of assuming that the wireless network is only provided with this mechanism.

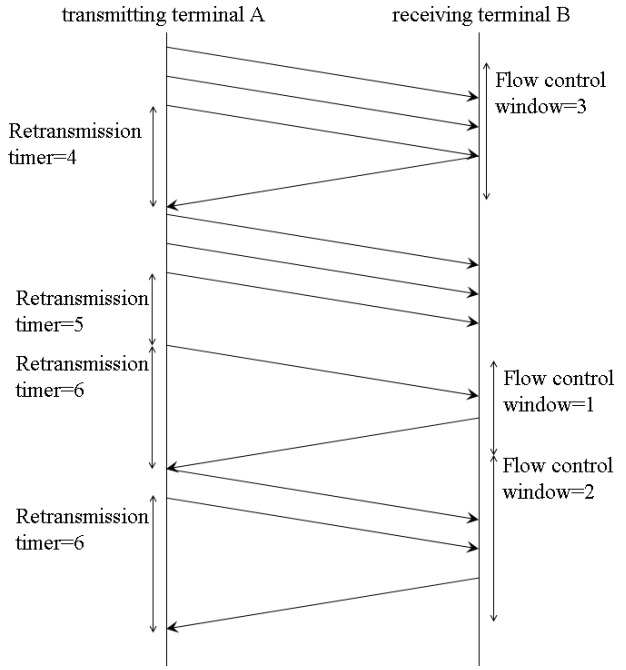

Figure 3. Confliction retransmission-window re-adjustment mechanism

In confliction retransmission-window re-adjustment mechanism, the information transmitting terminal will wait the timeout of retransmission timer after each confliction. Window re-adjustment will be performed after each retransmission timeout. If information transmitting terminal repeatedly enters into timeout retransmission process, it will cause great impact on the performance of the network. Fig. 3 shows the schematic of confliction retransmission- window re-adjustment mechanism. In the figure, the information transmitting terminal A receives the response of the information receiving terminal B after transmitting three frame data. At this time, the flow control window is 3, and the retransmission timer is 4. Then, confliction occurs in the fifth frame. A begins retransmission from the fourth frame and sets retransmission timer to 5. The flow control window is set to 1. However, after timeout of retransmission timer, A does not receive the response from B so that A retransmits the fourth frame and sets the retransmission timer to 6, then A receives the response of B before timeout of retransmission timer, and at this time the flow control window is 1. After receiving the response data, A sets the flow control window to 2 and starts sending the fifth and sixth frame data, and B returns response data before timeout of retransmission timer, and at this time the retransmission timer is 6.

The attacker sends attack packets to the target to implement flow control attack by making used of vulnerabilities in the process of confliction retransmission and re-adjustment window of wireless network protocol. In the course of the attack, the attacker can adjust the transmission rate to cause conflict between attack data stream and communication flow on the link, resulting in link congestion so that all wireless data stream sharing this link will be in confliction retransmission-re-adjustment window phase. At this point, the performance of the network system will be reduced to a low level, and then the network system will gradually adjust the flow control window to a large value, and then the attacker attacks again to make the value of flow control window of the sending terminal small again. Repetition of this attack process will greatly reduce network performance. Under this attack, the attacked network can only provide low quality of service, and the attacker is difficult to be found by IDS systems since only a small number of attack packets are sent. This attack can also be generalized to distributed attack. The uncertain attack source makes detection more difficult.

The flow control attack on retransmission timeout-re-adjustment window mechanism is described as follows:

A burst attack data stream sent by the attacker is called a pulse, with consideration into a single network data stream and a single flow control attack source, as shown in Fig. 4. Assuming that the information flow transmitting terminal will double the value of the confliction retransmission timer with the lower limit of 1 second after the confliction and that the attacker launches the first attack at the 16th second, the network communication mechanism will adjust the flow control window and the timeout timer (1 for window and 2 for timer); and if the attacker launches a second pulse at the 23rd second, the information flow transmitting terminal will wait for the value of current confliction retransmission timer-4 seconds, and the attacker can achieve the purpose of making the information flow transmitting terminal substantially unable to send data and transmitting attack data at a very low rate by generating pulse at the 27th , 35th ..... second.

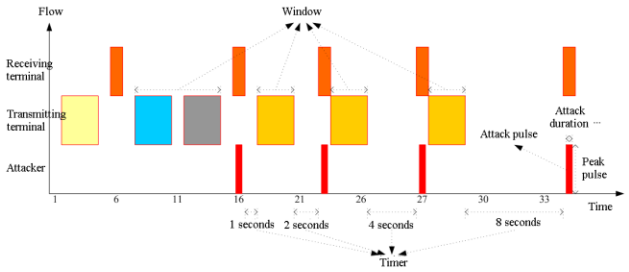

Figure 4. Schematic of traffic of flow control attack

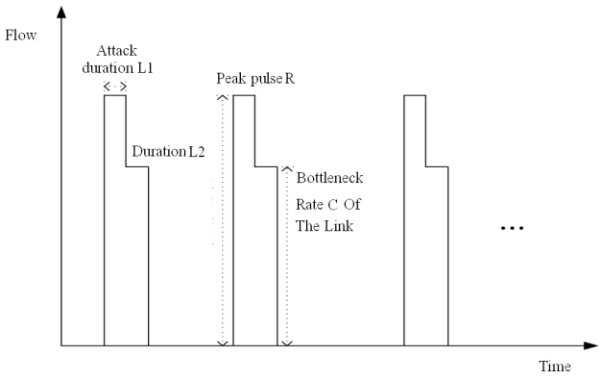

Figure 5. Schematic of traffic of dual-rate attack

Under the above attack, the attack flow is not always in the form of square wave. In order to avoid discovery by

the high rate data detection mechanism on the router, the attacker should minimize the transmitted data flow. To reduce the transmitted data, the attacker should use the double-rate pulse as shown in Fig. 5 for flow control attack. In this way, the data link is quickly occupied at a high rate. After the full load of the data link, the transmission rate is reduced to the bottleneck rate of the link to ensure continuous network packet loss at the lowest rate.

IV. PERFORMANCE ANALYSIS

According to the theoretical analysis and introduction of attack methods, the flow control attack method can enable the attack data stream to be featured in low average rate but high peak rate in a short time. Accurate detection of this attack in traffic monitoring method requires long duration of the attack. However, in fact each flow control attack lasts for a short time. In case that the data characteristics in a short time is used for detecting network flow control attacks, many normal applications will be wrongly reported as attack traffic, such as the instantaneous burst traffic generated by video, voice and other services. In case of detection by the packet features, the attacker can use forged legitimate data packets for attack to avoid being found by IDS. Some spoofing techniques of other deny of service attacks can also be applied to flow control attacks, such as forged source IP address and so on. In this case, it will make detection more difficult. It is also difficult to protect the network by filtering data stream on the router because the attacker can also forge legitimate packets.

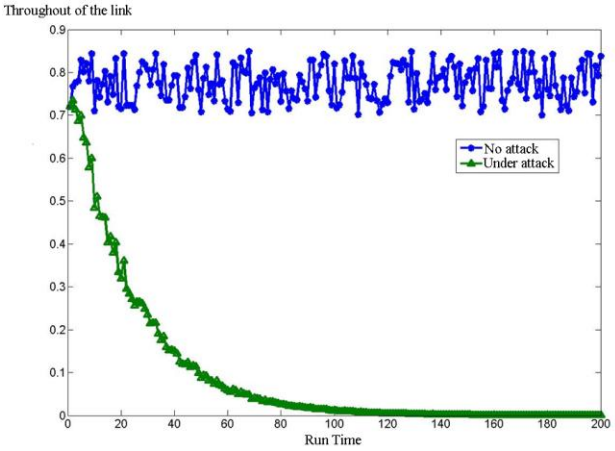

Figure 6. Throughout of the link

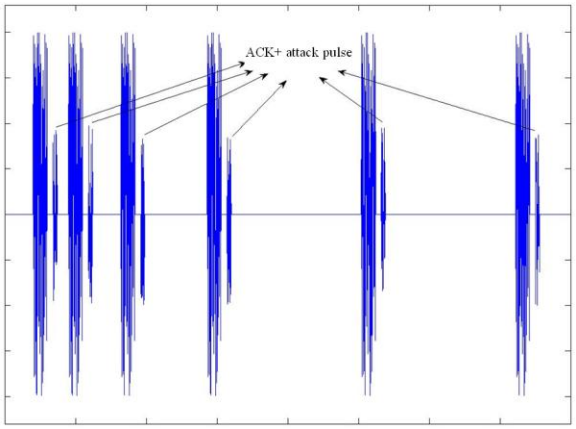

Figure 7. Link utilization

Fig. 6 shows the link throughput of the network in case of flow control attack and no attack. As can be seen from the figure, in case of more than 40 of running time, flow control attacks can greatly reduce the link throughput. Fig. 7 shows the network link utilization in case of flow control attacks. As can be seen from the figure, with the increase of the number of attacks, the duty cycle of the link is smaller and smaller and network link utilization is gradually reduced. In addition, it is unable to detect the attack pulses from the power and duty cycle.

V. CONCLUSIONS

Firstly, the feasibility analysis is made into the flow control attack of confliction retransmission-window re-adjustment mechanism based on the system stability. Then, the basic attack method and double speed attack method is presented by analysis of the confliction retransmission-window re-adjustment mechanism. At last, the efficiency of flow control attack is validated from two aspects: link throughput and link utilization. However, the flow control attack method is more suitable for the wireless network protocol where the network flow control mechanism can suffer multiple iteration adjustment. In case that there is an upper limit to the number of times for adjustment of the flow control mechanism of wireless networks, the attacker needs to increase the number of attacks to achieve better results, which results in that the attack is easy to be found by intrusion detection system. In the future, this paper will focus on the research of flow control attack technology which is not limited by the number of adjustment of the flow control mechanism targeting at the wireless network of which the number of adjustment of the flow control mechanism is limited through expansion of the above flow control attack method.

REFERENCES

[1] Y. Tao, Z.L. Liu, Z.N. Zhang and C.X. Guo, "Research on Network Attack Situation Niching Model Based on FNN Theory," High Technology Letters, vol 7, pp. 680-684, 2010.

[2] Q. Wang, Y.J. Feng and L. Yao, "Network Attack Model Based on Ontology and its Application," Computer Science, vol 37, pp. 114 - 117, 2010.

[3] G.Y. Wang, H.M. Wang and Z.J. Chen, "Research on Computer Network Attack Modeling Based on Attack Graph," Journal of National University of Defense Technology, vol 31, pp.74- 80 , 2009.

[4] F.F. Zhao, X.Z. Chen and J.H.Li, "Generation Methods of Network Attack Graphs Based on Privilege Escalation," Computer Engineering, vol 34, pp. 158-160, 2008.

[5] J.Y. Zhang, "Ad Hoc Network Attack Based MAC Protocol," Radio Engineering, vol 7, pp. 4 -6, 2008.

[6] F. Chen, Y.X. Luo and X.Q. Gong, "Progress of Research of Network Attack Technology," Journal of Northwestern University: Natural Science, vol 37, pp. 208-212, 2007.

[7] J.W. Zhuge, X.H. Han and W. Zou, "Network Attack Plan Recognition Algorithm Based on Extended Goal Graph," Chinese Journal of Computers, vol 29, pp. 1356 -1366, 2006.

[8] L. Yu, B. Chen and J.M. Xiao, "A Network Attack Path Reconstruction Program," Journal of University of Electronic Science and Technology of China, vol 35, pp. 392 -395, 2006.

[9] Y.G. Zhang and D.X Li, "Analysis of Network Attack and Intrusion under IPv6," Computer Science, vol 7, pp. 100- 102, 2006.

[10] S. Tursunova and Y. Kim, "Realistic IEEE 802.11e EDCA model for QoS-aware mobile cloud service provisioning," IEEE Trans. on Consumer Electronics, vol 58, No 1, pp.60−68, 2012.

[11] S. Rashwand, J. Misic and H. Khazaei, "Performance analysis of IEEE 802.15.6 under saturation condition and error-prone channel," In: Proc. of the IEEE Wireless Communications and Networking Conf. (WCNC), Cancun, IEEE, pp. 1167−1172, 2011.

[12] S. Rashwand, J. Misic and H. Khazaei, "IEEE 802.15. 6 under saturation: Some problems to be expected," Journal of Communications and Networks, vol 13, No 2, pp.142−148, 2011.

[13] S. Rashwand and J. Misic, "Effects of access phases lengths on performance of IEEE 802.15.6 CSMA/CA," Computer Networks, vol 56, No 12, pp.2832−2846, 2012.