This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

EDJam: Effective Dynamic Jamming Against IEEE 802.15.4-Compliant Wireless Personal Area Networks

Guobin Liu, Jiaqing Luo, Qingjun Xiao, Bin Xiao
Department of Computing, The Hong Kong Polytechnic University, Hong Kong
Emails: {csgliu, csjluo, csqjxiao, csbxiao}@comp.polyu.edu.hk

Abstract—**Jamming is one of the most important methods of attack to deprive or reduce the communication service of wireless personal area networks *WPANs*. Most existing jamming attacks can cause negative interference, but the attack strategies are usually not adjusted against the countermeasures that are currently taken. This paper proposes an effective dynamic jamming attack *(EDJam)* in an 802.15.4-compliant WPAN. In this attack, a jammer can choose a better strategy to make more damage to the network with less cost according to the the change of the network defense strategy. Similarly, a well-protected network can change its defense strategy against the *EDJam*. This procedure of competition between the *EDJam* attacker and defending networks is modeled as a Stackelberg game. We prove the existence of a unique Nash Equilibrium point. Based on an equilibrium analysis, we discuss the condition under which a defense strategy will increase the utility of the network and a dynamic retransmission mechanism defense strategy is proposed accordingly. The simulation results show that *EDjam* can be more cost-efficient than continuous, random and fixed-period jamming.**

I. Introduction

With widespread commercial implementation of the 802.15.4-compliant Wireless Personal Area Network (*WPAN*) in recent years, the demand for security has grown rapidly. The jamming attack is one of the security threats that can lead to great damage in the real world. Nowadays, however, with the help of a wireless sniffer, jammers can easily obtain transmitting packets in the open wireless communication environment that will allow them to analyze changes in critical parameters and jam the channel more smart. These parameters can reveal some configuration information (e.g. transmission and countermeasure) the network is using. Therefore, Jammers can dynamically adjust their strategy of attack after detecting the kind of environment that will make it possible for them to maximize their damage to the network, e.g. by the reduction of network throughput. Similarly, in order to fully utilize the channel bandwidth, legitimate users can dynamically change their defense strategies in response to the detection.

Most existing works on jamming attacks fall into one of the following two categories according to whether the network configuration is known by attackers. In the first category, jammers are unaware of the network configuration. This category includes continuous, random, and deceptive jamming [1]. The random jamming is energy-efficient but less effective. Both of continuous and deceptive jamming are effective but consume a great deal of energy.

The second category assumes that jammers are aware of the network configuration so that a jammer can adopt a relevant strategy of attack. Under this category, a typical method of jamming is reactive jamming [1]. It can cause the network throughput to fall to zero or almost zero. However it is not an energy-efficient method of attack because the jammer consumes energy sooner than the victims, given comparable energy budgets. A more efficient jamming attack is proposed in [2], in which the jammer controls the probability of jamming and the transmission range to cause maximal damage to the network in terms of corrupted communication links. However, the jamming transmission range can be difficult to control because the range depends on the circumstances.

In this paper, we propose an effective dynamic jamming attack (*EDJam*) to efficiently corrupt the legitimate communication. The jammer adjusts the jamming period in order to achieve maximal attack utility, with more damage done to network at less cost to launch the jam. Likewise, as a defender, the network would dynamically select a retransmission mechanism to maximize its utility of high throughput and reliability. In order for the jammer to maximize its utility, it needs to know the current value of the network retransmission timer (the longest waiting time for the ACK frame). Accordingly, the network would need to know the current period of jamming. Therefore, we use a dynamic competition model to describe the procedure of attacker jamming and the network defending.

In our model, we assume that both the network and attackers are rational and selfish, in that they are interested in maximizing their own utilities. The model of attack that is being considered can be analyzed by game theory, characterized by a competition involving two players. One player (network) optimizes its strategy based on the knowledge of the effect of its decision on the behavior of another player (attacker). To study this competition procedure, we use an analytical model named the Stackelberg game [3]. We prove that there is a unique equilibrium point for this Stackelberg game under the following several constraints: the length of the jamming signal, the jamming period, and the power of the jamming signal.

The main contributions of our work are as follows. 1). A novel, effective dynamic jamming attack (*EDJam*) and defense model is proposed to describe the procedure of jamming and defending. Different from previous work, our model can describe the procedure of the attacker jamming and attackers and the network defending. In this procedure, they can revise their

This work was partly supported by HK RGC PolyU 5314/10E.

978-1-61284-233-2/11/$26.00 ©2011 IEEE

respective strategies when they detect the strategy that their rival is using. 2). We formulate the above model as a Stackelberg game, with the network acting as the leader and the attacker acting as the follower. We prove that there exists a unique Nash Equilibrium for the game. From the analytical results, we modify the retransmission mechanism for IEEE 802.15.4 [4] to defend *EDJam*. 3). The simulation results show that the network can achieve good performance in terms of throughput and high reliability, when using the dynamic retransmission mechanism.

The rest of this paper is organized as follows. Section II describes related work on jamming attacks in wireless networks. Section III gives a detailed description of the network retransmission mechanisms and attack model, which focuses on the exploitation of the vulnerability of the 802.15.4 retransmission mechanism. Section IV uses the Stackelberg game to formulate the model and presents the equilibrium analysis. Completing the analysis of the performance of the model, we simulate our model in Section V. Section VI contains the conclusion.

II. Related Work

Jamming is a typical attack in wireless networks, which can disrupt wireless communication by emitting interference signals. IEEE 802.15.4-compliant wireless networks are susceptible to jamming attacks since such networks are composed of small energy-constrained devices to execute some tasks without a central powerful monitoring node.

Various jamming attacks and defending strategies [5], [6], [7], [8] are proposed. Attackers launch jamming attacks at the access layer by either corrupting control packets or occupying the channel for the maximum allowable time, so that the network throughput will decrease [5]. By observing the channel and learning protocols' semantics, various jamming attacks aimed at different *MAC* protocols in sensor networks are proposed in [6] to attack the network effectively. However, they are either static or not energy-efficient.

Some efficient strategies are proposed in [9], [2]. The work in [9] discusses a low-energy attack that destroys a packet by jamming only a few bits, such that the code error correction functionality will take on an excessive load. To save energy, a jammer controls the probability of jamming and the transmission range to cause maximal damage to the network in terms of corrupted communication links [2]. However, the access probability is difficult to get hold of and the transmission range is greatly affect by the surroundings.

Game theory is considered to describe the procedure of jamming and defending. A malicious node corrupts broadcasts from a base station (*BS*) to a sensor network by depriving other nodes from receiving a broadcast message. The procedure of attacking and *BS* defending is formulated as a zero-sum game in [10]. A one-way time-slotted packet radio communication link can be attacked by a jammer that works in an on-off mode. This process is modeled as a a two-person zero-sum noncooperative dynamic game [11]. However, a more precise model to reflect the dynamic procedure of jamming and defending is Stackelberg game. In this paper, we use Stackelberg game to analyze the behavior of the jammer and the network. Based on the analysis, we proposed a dynamic jamming strategy and finally provide an efficient countermeasure.

III. Attack Model

In this section, we first simply introduce the retransmission mechanism used in 802.15.4 and demonstrate how an attacker can exploit this retransmission mechanism to launch an *EDJam* attack. Then, we present a model to describe the attack.

In the open wireless circumstance, there are many factors that would lead to the loss of data. Therefore, a retransmission mechanism is necessary for *WPANs*. In the retransmission-enable 802.15.4, if the destination receives the frame correctly, it will generate and send back an acknowledgement. In this paper, device and sender, coordinator and receiver, are exchangeable. *macAckWaitDuration* is the maximum number of symbols (default value is 16 *microseconds*.) to wait for an acknowledgment frame to arrive following a transmitted data frame. In this paper, we denote the value of *macAckWaitDuration* as t_{r_0} and name it retransmission timer. If the expected acknowledgement is received within t_{r_0} symbols after the original data frame, the sender will believe that the transmission is successful. If the sender does not receive the acknowledgement within t_{r_0} symbols or receive a wrong acknowledgement, the sender will conclude that the transmission has failed. In that case, the sender will initiate a retransmission.

This retransmission mechanism, while essential for robust communication, provides an opportunity for our *EDJam* attack. The purpose of an *EDJam* attack is to force the sender to continuously enter the retransmission state by jamming signals with dynamic period. The jamming period is decided by observing the value of the network current retransmission timer. A jammer can calculate the value of the retransmission timer by blocking a packet sent by a legitimate node in the network. First, using a sniffer, a jammer detects a sender sending out a packet at time *x* and block the packet or its ACK frame by jamming signals. Then, the sender will retransmit the same packet again and the jammer would detect it at time *y*. Therefore, the value of the current retransmission timer is *y*-*x*.

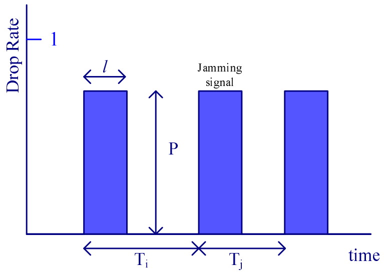


Fig. 1. In the attack model, l is the duration of the jamming signal. T_i and T_j are the optimal *jamming periods (T)* at different time under an *EDJam* attack. P is the packet drop rate, which is affected by the strength of jamming signals.

Our attack model is visualized in Fig. 1. T denotes the attack period, which means the interval between two continuous jamming signals. The jammer will adjust its jamming period (T_i, T_j) according the current observation of the network. We use the parameter P to measure the jamming signal strength. P is defined as the ratio of the number of packets that have arrived to the number of packets that were sent out.

There are two main factors in a successful launch of an *EDJam* attack: the duration of each jamming (l) and the jamming period (T). Although a short jamming signal is less detectable, it must still be long enough to effectively block packets. For this purpose, we generate a periodically repeating short jamming having a time-scale length of t_2 [12]. Simultaneously, the *EDJam* attack is to avoid detection by sending a low average volume of traffic. Thus, the value of l should be smaller than T. T should be larger than t_{r_0} so that the jammer can work as a legitimate member in the network. T is a critical parameter to launch our attack efficiently.

IV. Game Between Jammers and the Network

In this section, we first define utility functions for both the attacker and the network to formulate the attacking and defending procedure as a Stackelberg game. Then, we study the existence of the equilibrium of the game by maximizing utilities and propose a dynamic network defense strategy.

The Stackelberg game can be used to formulate a dynamic process of competition between two players, which can precisely reflect the procedure of a dynamic jamming attack and network defence. The attacker and network choose their strategy after they observe a competitor's operation. π_a and π_d are the utilities of the attackers and the network respectively. A device uses the standard IEEE 802.15.4 and presents in the network first. Therefore, it has the right to decide its retransmission mechanism by changing the value of the retransmission timer, so as to maximize its own utility in terms of both performance and reliability. We use t_r to denote the value of the current modified retransmission timer. Hence, the network can modify the retransmission mechanism by changing t_r. Attackers in the network choose its jamming period (T), duration (l) and packet drop rate (P) in the predefined network to optimize its utility in terms of the reduction of throughput minus the cost of jamming the network. Therefore, it is a typical two-stage leader-follower game which can be analyzed under the Stackelberg game framework.

A. Utility Functions

The attacker's utility (π_a) is defined as the revenue (damage to the network) minus the cost it incurred in making the attack. The utility of the network is defined to be the performance plus reliability. Performance is measured by the normalized throughput and reliability is measured by the satisfaction function of the retransmission timer. Based on the model illustrated in Section III, we calculate these two utilities in the following manner.

Damage is defined to be the reduction in network normalized throughput, which is used to measure the performance of the network, under an *EDJam* attack. $Cost$ (Eq. 1) is proportional to l and P, but in inverse proportion to T.

$$Cost = \frac{l \cdot P}{T} \tag{1}$$

We derive the normalized throughput on the time domain. In this paper, the normalized throughput is defined to be the ratio of the channel available time to total time.

$$\rho = \rho(t_r, T) = P\frac{\lceil \frac{t_r}{T} \rceil T - t_r}{\lceil \frac{t_r}{T} \rceil T} + (1-P) = 1 - P\frac{t_r}{\lceil \frac{t_r}{T} \rceil T}$$

Therefore, damage (Eq. 2) and utility (Eq. 3) of the attacker are calculated as follows:

$$Damage = 1 - \rho = 1 - P\frac{\lceil \frac{t_r}{T} \rceil T - t_r}{\lceil \frac{t_r}{T} \rceil T} \tag{2}$$

$$\pi_a = (1-\rho) - \frac{l \cdot P}{T} = \frac{P}{T}\left(\frac{t_r}{\lceil \frac{t_r}{T} \rceil} - l\right) \tag{3}$$

The network utility (Eq. 5) is calculated as normalized throughput plus the network satisfaction index of current modified retransmission mechanism. Although changing the retransmission mechanism could help the network defend against the attack and raise the throughput under the attack, there are some side effects to this approach. Therefore, when we change the default value of the retransmission timer, the performance of the retransmission mechanism will change at the same time, and we have to consider how this change impacts the utility of devices. In order to keep the same metric with normalized throughput, we normalize the factor, which is measured by a satisfactory function (Eq. 4). Sigmoid function [13] has been widely used to approximate the users satisfaction with respect to service qualities. a is the steepness of the satisfaction curve. The meaning of this function is that when the value of the retransmission timer becomes larger, the device will be more satisfied with the retransmission mechanism because more reliable communication is promised. And we know that when t_r is larger than a constant, such as the default value suggested in 802.15.4, the satisfaction of device will increase more and more slowly.

$$S(t_r) = \frac{1}{1 + e^{-a(t_r - t_{r_0})}} \tag{4}$$

$$\pi_d = \rho + S(t_r) = 1 - P\frac{t_r}{\lceil \frac{t_r}{T} \rceil T} + \frac{1}{1 + e^{-a(t_r - t_{r_0})}} \tag{5}$$

B. Maximizing the Attacker's Utility

When the value of l closes T, our *EDJam* attack will degenerate into continuous jamming. Therefore, we assume that $l \le \frac{1}{2}T$. We have obtained the formula of attacker utility as Eq. 3, which will be maximized in the following.

Theorem 1: $\pi_a(T, t_r)$, with respect to T, is maximized at $T = t_r$ when $l < t_r$.

Proof: When $\frac{t_r}{k} \le T < \frac{t_r}{k-1}$ (k is an integer and $k > 0$), $\lceil \frac{t_r}{T} \rceil$ equals to k. In particular, the inequality is simplified to $T \ge t_r$ when $k = 1$. Substituting it to Eq. 3,

$$\pi_a = \frac{P}{T}\left(\frac{t_r}{k} - l\right) \qquad where \quad \frac{t_r}{k} \le T < \frac{t_r}{k-1} \tag{6}$$

The function of π_a, with respect to t_r, is decreasing in each slot $[\frac{t_r}{k}, \frac{t_r}{k-1})$ (k is an integer and $k > 0$) since $\frac{t_r}{k} > l$. Therefore, the local maximum point in each slot is $(\frac{t_r}{k}, P \cdot (1 - \frac{l \cdot k}{t_r}))$. Moreover, the global maximum point should be $(t_r, P \cdot (1 - \frac{l}{t_r}))$ when $k = 1$.

When T equals to the global maximum point (Eq. 7), the utility function of the attacker is maximized (Eq. 8).

$$T^* = \frac{t_r}{k} = t_r \tag{7}$$

$$\pi_a^* = \pi_a(T^*) \tag{8}$$

■

According to the analytical results (Eq. 7 and 8), we design an attack scheme to jam the network by dynamically maximizing the jammer's utility. First, a jammer senses the wireless environment periodically, to catch any changes in the network retransmission mechanism. Second, once the retransmission mechanism changes, this means that there is a new retransmission timer. To calculate the new timer, a jammer can use the method presented in Section III. Finally, according to the value of the new retransmission timer and our analytical result, the jammer can choose an optimal strategy by setting the jamming period to the same value as that of the new retransmission timer.

C. Network Defense Strategy

The utility of network is calculated as Eq. 5. Devices can also figure out the best response and use it to defend against an attack. According to the jammer's optimal period, $T = t_r$, we can simplify the utility devices as Eq. 9.

$$\pi_d = 1 - P + \frac{1}{1 + e^{-a(t_r - t_{r_0})}} \tag{9}$$

Theorem 2: When the following condition, $a \cdot T > 4P$, is satisfied, a device maximizes its utility function if and only if the retransmission timer t_r is set to the following optimal value, $t_r = t_{r_0} - \frac{1}{a} \cdot \ln(\frac{a \cdot T + \sqrt{a \cdot T(a \cdot T - 4P)}}{2P} - 1)$.

Proof: Calculating the first order derivative of π_d with respect to t_r, we have,

$$\frac{\partial \pi_d}{\partial t_r} = -\frac{P}{T} + \frac{a \cdot x}{(1+x)^2} \tag{10}$$

where x is given by $x = e^{-a(t_r - t_{r_0})}$.

When $a \cdot T \leq 4P$, the first order derivative of π_d with respect to t_r is always nonpositive,

$$\frac{\partial \pi_d}{\partial t_r} = -\frac{P}{T} + \frac{a \cdot x}{(1+x)^2} \leq -\frac{P}{T} + \frac{a}{4} \leq 0$$

Therefore, the network utility is a monotonically decreasing function. Because $t_r \geq 0$, π_d achieves its maximum at $t_r = 0$ when $a \cdot T \leq 4P$.

When $a \cdot T > 4P$, with the increase of t_r, π_d decreases first, then increases, and at last decreases. There is a local minimum point t_{r_1} and a local maximum point t_{r_2} when π_d is defined in the whole positive real number field. Both t_{r_1} and t_{r_2} can be derived by assigning the first order derivative of π_d (Eq. 10) to be 0.

When t_r is equal to the local maximum point, which is also the global maximum point (Eq. 11), the utility function of the device is maximized (Eq. 12).

$$t_r^* = t_{r_0} - \frac{1}{a} \ln \frac{-2P + a \cdot T + \sqrt{a \cdot T(a \cdot T - 4P)}}{2P} \tag{11}$$

$$\pi_d^* = \pi_d(t_r^*) \tag{12}$$

■

According to the analytical result in Eq. 11, we propose an adaptive countermeasure against *EDJam* in the IEEE 802.15.4 compliant network by dynamically selecting the retransmission timer. As illustrated in Eq. 11, a and t_{r_0} are predefined parameters for the attacker and network. The optimal retransmission timer (t_r) is a function of the jamming period (T) and packet drop rate (P), which may change with real channel conditions and is decided by the jammer. In order to study the real time packet drop rate in various environments, we have implemented the jamming signal by exploiting the *CSMA-CA* mechanism used in 802.15.4. In order to calculate the current jamming period, legitimate nodes periodically detect channel conditions to find jamming signals appearing from the jammer and record their intervals. Some legitimate nodes that detect the jamming signal will send their intervals to the coordinator. Then, the coordinator will calculate the optimal retransmission timer according to the new jamming period.

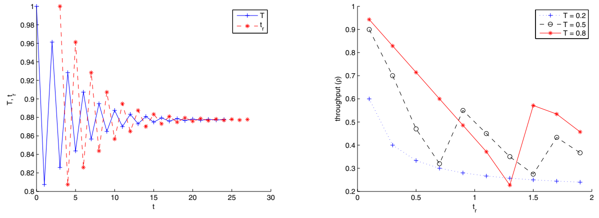
After the calculation, the coordinator will broadcast the optimal timer to the legitimate nodes in the next beacon frame. Therefore, in order to implement this dynamic retransmission, the timer value has to be added to the beacon frame for notifying all legitimate nodes to synchronize the network retransmission mechanism. In this game, a unique Nash Equilibrium exists if and only if $t_{r_0} > \frac{4 \cdot P}{a}$. Due to the space limit, we omit the existence proof of the unique Nash Equilibrium point.

V. Performance and Evaluation

In this section, we show simulation results to illustrate the impact of the jamming period for attacking and retransmission mechanism for defending the jammer. Moreover, we compare our *EDJam* with continuous and random jamming, which are classic jamming attacks in wireless networks. In the simulation, we consider a simple transfer model where devices transfer data to a coordinator using beacon-enabled IEEE 802.15.4.

A. Impact of the Jamming Period and the Retransmission Timer

We used a homemade simulator programmed by C++ to simulate the *EDJam* schedule. We have implemented the generation of jamming signals in the network composed by MicaZ motes that use 802.15.4 as their communication standard. Therefore, our simulator focused on how the jammer controls the jamming period (T) and how the network adjusts its retransmission timer (t_r) to maximize their respective utilities.



(a) The attacker and network respectively adjust the jamming period (T) and the retransmission timer (t_r) to maximize their utilities.

(b) Network normalized throughput versus the network retransmission timer (t_r) when the attacker uses various jamming periods.

Fig. 2. Game process and the normalized throughput.

Figure 2 (a) shows the temporarily optimal T and t_r, versus time t. With the increase of time, T and t_r converge to an equilibrium point. Finally, the retransmission timer t_r will be equal to the jamming period T because the condition of an attacker maximizing its utility is $T = t_r$. In the figure, we can see that these two parameters converge to the same point.

Figure 2 (b) illustrates how the network defense (t_r) impacts the normalized throughput (ρ). In the simulation, we fix the value of the jamming period T, e.g. t_{r_0}, which is the default retransmission timer in 802.15.4. In Fig. 2 (b), when the network uses a static strategy, a constant retransmission timer (t_r), to defend itself against the jamming, an attacker dynamically adjust its jamming period (T) to decrease the network throughput. For example, when $t_r = 0.5$, the attacker choose $T = 0.5$. Then, in order to defend itself against this dynamic jamming schedule, the network should adjust its defense strategy correspondingly, e.g. by choosing $t_r = 1.5$. We have proposed this kind of defense in Section IV.

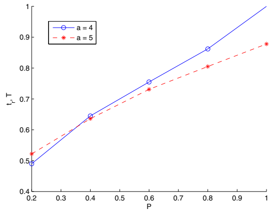
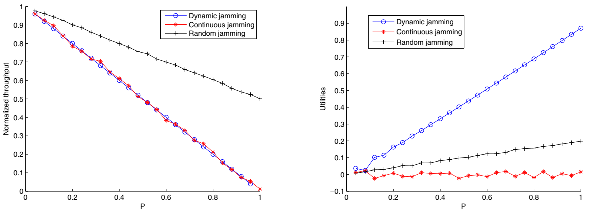


Fig. 3. The optimal network retransmission timer (t_r) and jamming period (T) versus the drop rate during jamming P.

Figure 3 illustrates how the drop rate (P) impacts the optimal jamming period T and retransmission timer t_r. There is a point at which the two curves intersect. When P is larger than the value of the intersection point, the values of the optimal T and t_r are larger. This means that the more quickly the satisfaction of the retransmission mechanism increases, the larger the optimal values of T and t_r are. This reveals that a larger reaction sensitivity of the network leads to an increase in the equilibrium point and a decreased in the normalized throughput.

B. Comparison

Now we turn to compare the performance of our *EDJam* attack with continuous, random, and fixed-period jamming in terms of utility and normalized throughput. We will also study the difference between dynamic and static defense strategies. From the following result, we can conclude that *EDJam* obviously has a higher utility than continuous and random jamming.



(a) Normalized throughput of EDJam, random jamming, and continuous jamming versus the jamming power (P).

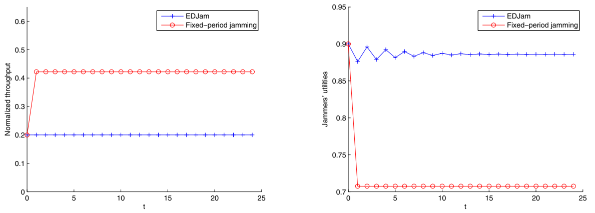
(b) Utilities of EDJam, random jamming, and continuous jamming versus the jamming power (P).

Fig. 4. Comparison among EDJam, continuous jamming and random jamming.

Fig. 4 (a) shows that the network normalized throughput under continuous jamming is equal to under EDJam, which is lower than under random jamming. This means that the continuous jamming can make the same damage with EDJam to the network, then EDJam, then random jamming. EDJam can force a sender to enter the retransmission state repeatly, so EDJam can cause the similar damage to a continuous jamming which emits jamming signals continuously.

Although continuous jamming produce the same damage with EDJam, it obviously costs more energy than EDJam. Fig. 4 (b) shows that no matter what jamming signals strength (P) is used, the utility of an EDJam attack is higher than those of both continuous and random jamming attacks.

Figs. 5 illustrates that EDJam has higher utility and damage than fixed-period jamming. Fixed-period jamming differs from EDJam in that the jamming periods are dynamically adjusted to optimize the utility or are decided right at the beginning. Under both attacks, the network uses retransmission mechanism to defend against them. It reveals that dynamic period has higher utility than the fixed-period jamming because of the flexible strategy and optimizing process of EDJam.



(a) Normalized throughput of EDJam and fixed-period jamming using dynamic countermeasure versus the time.

(b) Utilities of EDJam and fixed-period jamming using dynamic countermeasure versus the time.

Fig. 5. Comparison between EDJam and fixed-period jamming.

VI. Conclusion

In this paper, we proposed an effective dynamic jamming strategy to attack IEEE 802.15.4-compliant wireless personal area networks. The attacker dynamically adjusts the jamming period to maximize its utility, while the network will change its retransmission mechanism correspondingly to defend the jamming. The dynamic procedure of jamming and defending can be modeled as a Stackelberg game and we derived the Nash Equilibrium for the game by maximizing the utilities of network and attacker respectively. In the simulation, the numerical results showed that the attacker and network can achieve optimal utility in the procedure of jamming and defending and will finally converge to a point of equilibrium.

References

[1] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, pp. 41–47, 2006.

[2] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," *IEEE INFOCOM*, pp. 1307–1315, 2007.

[3] D. Fudenberg and J. Tirole, "Game theory," *MIT Press*, 1993.

[4] "Wireless medium access control(mac) and physical layer(phy) specifications for low-rate wireless personal area networks(lr-wpans).," *IEEE Standard, 802.15.4-2003*, October 2003.

[5] R. Negi and A. Perrig, "Jamming analysis of mac protocols," *Carnegie Mellon Technical Memo*, 2003.

[6] Y. Law, L. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols," *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, pp. 76–88, November 2005.

[7] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," *In Proceedings of 20th International Parallel and Distributed Processing Symposium IPDPS 2006 (SSN2006)*, pp. 1–8, 2006.

[8] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify suspect nodes in selective forwarding attacks," *Journal of Parallel and Distributed Computing (JPDC - Elsevier)*, pp. 1218–1230, 2007.

[9] G. Lin and G. Noubir, "On link-layer denial of service in data wireless lans," *Journal on Wireless Comm. and Mob. Computing*, pp. 273–284, 2004.

[10] J. McCune, E. Shi, A. perrig, and M. K. Reiter, "Detection of denial-of-message attack on sensor network broadcasts," *In Proceedings of IEEE Symposium on Security and privacy*, pp. 64–78, 2005.

[11] R. Mallik, R. Scholtz, and G. Papavassilopoulos, "Analysis of an on-off jamming situation as a dynamic game," *IEEE Transactions of Communications*, pp. 1360–1373, 2000.

[12] A. Kuzmanovic and E. Knightly, "Low-Rate TCP-targeted denial of service attacks and counter strategies," *IEEE/ACM Trans. Netw.*, pp. 683–696, 2006.

[13] D. H. von Seggern, "CRC standard curves and surfaces with mathematica, second edition (chapman & hall/crc applied mathematics and nonlinear science)," *Chapman & Hall/CRC*, 2006.