A Bayesian Game Approach for Security Defense Strategy in WSN

Liang Yu
Computer Science and Engineering Department
Xiangsi Lake College
Guangxi University for Nationalities
Nanning,China

Qin Donghua
Teaching Resources and Technology Centre
GuangXi Radio & TV University
Nanning,China

***Abstract*—Wireless sensor networks (WSN) are a new self-organizing network as a kind of military applications by RF wireless communications, so its security is very important. Intrusion detection system always be deployed at each node in previous research in defense mechanism in WSN, and it will produce great energy consumption. According to the characteristics of WSN, this paper puts forward a defense model based on the Bayesian game theory in WSN and analyses the game between the attacker and defenders. This model can improve detection rate and show higher energy efficiency.We study the achievable Nash equilibrium for the attacker and defender game in both static and dynamic scenarios.**

Keywords- Bayesian game, wireless sensor networks, security defense strategy

I. INTRODUCTION

Wireless sensor network (WSN) is a distribution system with no center. Many nodes are integrated a sensor, data processing unit and communication module, they form a network through wireless channel [1].Wireless sensor network almost can not maintenance, and radio communication are not equilibrium. As a result of the wireless channel, distributed control technology, network is vulnerable to passive eavesdropping and active invasions attack. WSN is a new self-organizing network as a kind of military applications by RF wireless communications, so its security is very important. Therefore wireless sensor networks need to have the ability to defend attacks [2-3].

Generally, each node is configured IDS (Intrusion detection system) as a good defense model, and each IDS should always be activated. But the sensor nodes are energy limited, it is impossible that IDS is always on. How to adjust the strategy against the attack of malicious node? Game theory has many advantages in solving the cooperation problem between individuals [4-5].

Game theory applications in network security dates back to 1997, Syverson proposed the way of using rational stochastic game theory to analyze the normal network nodes and malicious nodes [6]. Lye and Wing and implemented the formal definition of the idea of Syverson in 2002 [8]. In 2003, Xu and Lee proposed a DDoS defense system, which is based on the complete information static game theory, and that the introduction of game theory makes the performance of DDoS defense system optimized [10]. Alpcan use the game theory to analyze intrusion detection in wireless network [11] [12]. Most of their researches were under complete information game for analysis, but in the wireless sensor network applications, it has not given incomplete information game model [13]. This paper on the basis of previous research presented a Bayesian game model of security and defense, and the simulation experiments in wireless sensor network platform prove the validity of the model and provide new ideas for the wireless sensor network security research

II. DEFENSE MODEL BASED ON BAYESIAN GAME

Definition 1 Game model

(1) Players: There are two players. One is a node in WSN，denoted by i . Its type space is $N_i\{N_i^m, N_i^r\}$ (N_i^m represents a malicious node which can cause certain threats, a normal node denoted by N_i^r which is safe). The other player is IDS, denoted by j , its type space is $N_j\{N_j^d\}$ (N_j^d represents IDS which can detect the attack by malicious nodes). Each player do not know anything about the type of the other player, but they know the prior belief, action space, and payoff about other players. So, each player knows how the action space and payoff rely on their type of other players.

(2) Action space: it is what actions the players can take. Player i has two identities, if it is a normal node, then its action space is not attack, that is denoted by $A_i(N_i^r) = \{not\ attack\}$, and if it is a malicious node, its action space is attack or not attack, that is denoted by $A_i(N_i^m) = \{attack, not\ attack\}$. Player j is IDS, its action space is defend or not defend, that is denoted by $A_j(N_j^d) = \{defend, not\ defend\}$.

(3) Prior belief: it is prior probability that the type of the other player the one thinks it is. We define the probability that a node is a malicious one is μ , denoted $p(N_i^m) = \mu$, so if a node is a normal one, the probability is $1-\mu$, denoted $p(N_i^r) = 1-\mu$, because of $p(N_j^d) = 1$.

© the authors

(4) Payoff: it is players earning from taking actions. Payoff of a malicious node is denoted by $E_i(N_i^m)$, payoff of a normal node is $E_i(N_i^r)$, payoff of defender is $E_j(N_j^d)$.

III. Analysis based on Bayesian Nash equilibrium

Payoff of players is given in table 1.

ω means the system loss caused by aggression, it is also the malicious node earnings when it successfully attack the system; α means the probability of defender issued a correct alarm; β means under no attack, the probability of defender issued a false alarm; γ means further damage to the system caused by false alarm; C_d means the cost of nodes take intrusion detection; C_a means the cost of attacker launch attacks.

We suppose that the probability of defender detection is p and the probability of attacker attack is q, then the payoff of defender is

$$E_j = \mu pq(\alpha\omega + \beta\gamma) - p(\beta\gamma + C_d) - \mu q\alpha(1-p) \quad (1)$$

The payoff of attacker is

$$E_i = \mu q(\omega - p\omega\alpha - C_a) \quad (2)$$

Based on Rules offinding derivative, we can get $p^* = \frac{\omega - C_a}{\omega\alpha}$ $q^* = \frac{\beta\gamma + C_d}{\mu(\alpha\omega + \beta\gamma + \omega)}$, so there is a mixed-strategy BNE

$$(a_i(N_i^m, N_i^r), a_j(N_j^d)) = ((q^* attack, not\ attack), p^* defend)$$

When $p=1, q=1$, $(a_i(N_i^m, N_i^r), a_j(N_j^d)) = ((attack, not\ attack), defend)$, then payoff of the player j is

$$E_j(defend) = \mu(\alpha\omega + \beta\gamma) - (\beta\gamma + C_d) \quad (3)$$

$p=0, q=1$, $(a_i(N_i^m, N_i^r), a_j(N_j^d)) = ((attack, not\ attack), not\ defend)$, then payoff of the player j is

$$E_j(not\ defend) = -\mu\omega \quad (4)$$

If $E_j(not\ defend) = E_j(defend)$, it is $\mu = \frac{C_d + \beta\gamma}{\alpha\omega + \beta\gamma + \omega}$

If $\mu \geq \frac{C_d + \beta\gamma}{\alpha\omega + \beta\gamma + \omega}$, then $a_j(N_j^d) = defend$ is the best strategy to player j .Under this case, player i choose $a_i(N_i^m, N_i^r) = (not\ attack, not\ attack)$, so $(a_i(N_i^m, N_i^r), a_j(N_j^d)) = ((attack, not\ attack), defend)$ is not a pure strategy BNE.

If $\mu < \frac{C_d + \beta\gamma}{\alpha\omega + \beta\gamma + \omega}$, then $a_j(N_j^d) = not\ defend$ is player j 's best strategy, and player i should choose $a_i(N_i^m, N_i^r) = (attack, not\ attack)$, so $(a_i(N_i^m, N_i^r), a_j(N_j^d)) = ((attack, not\ attack), not\ defend)$ is a pure strategy BNE.

$p=1, q=0$, If player i 's strategy is $a_i(N_i^m, N_i^r) = (not\ attack, not\ attack)$, player j 's best strategy is $a_j(N_j^d) = not\ defend$, so $(a_i(N_i^m, N_i^r), a_j(N_j^d)) = ((not\ attack, not\ attack), defend)$ is not a pure strategy BNE.

When $p=0, q=0$. If player j 's strategy is $a_j(N_j^d) = not\ defend$, player i 's best strategy is $a_i(N_i^m, N_i^r) = (attack, not\ attack)$, so $(a_i(N_i^m, N_i^r), a_j(N_j^d)) = ((not\ attack, not\ attack), not\ defend)$ is not a pure strategy BNE.

IV. Performance evaluation

We have simulated our proposed model on GAMBIT [14].

Figure 1 shows the probability of defender issued a correct alarm α to the probability of player i choose attack strategy. $\alpha \in [0.3,1]$, β =0.01, C_d =100, ω =200, γ =150, μ ={0.4， 0.7}.Along with α bigger, the probability of malicious node taking aggression is smaller, and different values of prior probability μ make different experiment results. How to determine the μ 's initial value, it have a major influence to the whole game process. And as the intrusion detection should strive to improve their detection rate, thereby reducing malicious node invasion.

Figure 2 shows the probability of defender issued a false alarm under no attack β to the probability of player i choose attack strategy. $\beta \in [0, 0.1]$, α =0.7, C_d =100, ω =1000, γ =200, μ ={0.1， 0.4,0.7}.Along with β increasing, malicious node taking an attack strategy is more possible, and different values of prior probability μ make different experiment results. In addition, when μ = 0.7, as the prior probability is quite high, the probability of malicious node taking attack strategy is lower, and as the β keeps getting bigger, the probability of malicious node aggression strategy has little change.

© the authors

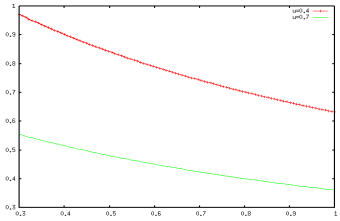

Figure 1. α to the probability of player i choose attack strategy.

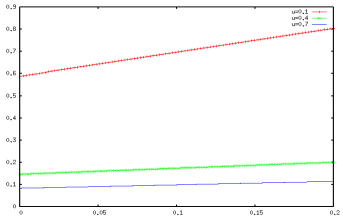

Figure 2. β to the probability of player i choose attack strategy.

V. CONCLUSION

In this paper, we proposed a Bayesian game defense model which can defense many types of attack in wireless sensor network. The defender takes effective strategy maximization of their profits according to the Bayesian Nash equilibrium. IDS should improve the probability of defender issued a correct alarm and reduce the probability of defender issued a false alarm to make a rapid response of the system. In practical application, defenders determine the value of μ according to the cognition of network environment. For example, if a sensor node in a hostile environment, we can set up a larger value. In the game, we assumed the behavior of each node would not be affected by other nodes, so when simultaneously multiple attack, the Bayesian game model can not make good performance, so this is a direction for future research.

REFERENCES

[1]

[2] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[3] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[4] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[5] K. Elissa, “Title of paper if known,” unpublished.

[6] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[7] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[8] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[9] Electronic Publication: Digital Object Identifiers (DOIs):

Article in a journal:

[10] D. Kornack and P. Rakic, “Cell Proliferation without Neurogenesis in Adult Primate Neocortex,” Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

Article in a conference proceedings:

[11] H. Goto, Y. Hasegawa, and M. Tanaka, “Efficient Scheduling Focusing on the Duality of MPL Representatives,” Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.

TABLE I. PAYOFF MATRIX OF THE GAME

Player i	**Action space**	**Player** j **(IDS** N_j^d **)**			
		defend		*not defend*	
		Payoff of IDS	***Payoff of node***	***Payoff of IDS***	***Payoff of node***
Malicious node N_i^m	*attack*	$\alpha\omega - C_d$	$(1-\alpha)\omega - C_a$	$-\omega$	$\omega - C_a$
	not attack	$-\beta\gamma - C_d$	0	0	0
Normal node N_i^r	*not attack*	$-\beta\gamma - C_d$	0	0	0

© the authors