An Intrusion Detection Based on Bayesian Game Theory for UAV Network

Jianguo Sun, Wenshan Wang, Qingan Da, Liang Kou, Guodong Zhao, Liguo Zhang, Qilong Han
{sunjianguo, wangwenshan, da_qing_an}@hrbeu.edu.cn

College of Computer Science and Technology, Harbin Engineering University, Harbin 150001

Abstract. Unmanned aerial vehicles (UAVs) have enormous potential in public, civil and military fields, so the security of UAV networks is attracting increasing people's attention. The existing schemes to network intrusion detection have two main limitations: a high false alarm rate and computational overhead. In this paper, aiming at the problem of UAV network security, an intrusion detection scheme based on Bayesian game theory is proposed. Bayesian game means that game participants do not have complete information on the profit function of the opponent. In this paper, incomplete information means that the IDS agent is not sure of the type of attacker and the attacker is not sure whether its neighbor node is an IDS agent or not. The simulation and experimental comparison show that the proposed scheme achieves a high detection rate of intrusion. In addition, the communication cost of the network is the lowest.

Keywords: Unmanned Aerial Vehicles (UAVs), UAV networks, intrusion detection system (IDS), Bayesian game, Bayesian Nash equilibrium.

1 Introduction

The development of wireless communication technology and microelectronic technology has made the unmanned aerial vehicle (UAV) remarkable achievements in a short period of time. Because of the strengthened payload capacity and the improved hover stability, UAVs have been gradually used in modern military applications, social security and economic construction, such as military reconnaissance, urban wars [1], disaster relief, agriculture Irrigation, aided by urban transport. In particular, small UAVs have the advantages of low energy consumption, low cost, ease of operation and deployment, so that the groups of these aircraft are capable of performing more complex tasks. A group of small UAVs is called a UAV network, which has good scalability, flexible topological structure, and low communication costs.

The UAV network realizes the communication between the UAV group and the ground or the aerial base station through the unstable wireless link. And it is generally deployed in the harsh field or the sensitive area, which is easy to suffer black hole attacks, Sybil attacks and denial of service (DoS) attacks [2] [3]. As UAV technology infiltrates every aspect of society, some organizations or individuals exploit this new technology to make a series of malicious incidents, such as intercepting drones, tapping network data, consuming drones, guiding flight routes and even interfering with military strategies [4]. These malicious acts can bring about huge economic losses, casualties and strategic risks. For example, when a UAV received a fake

MOBIMEDIA 2018, June 21-22, Qingdao, People's Republic of China

DOI 10.4108/eai.21-6-2018.2277054

GPS signal which is sent by an attacker, it will change course to collide with other UAVs in the network or fly to dangerous locations [5] [6]. To this end, some researchers [7] devised regional division-based UAV network screen coverage systems to defend against various types of intrusion initiated by intruders.

An effective means of detecting intrusion in a UAV network is to develop an intrusion detection system (IDS). Due to the similarities between the vehicular ad-hoc network (VANET) and the UAV network, we investigated existing intrusion detection systems designed for UAV networks or VANET, and classified these research results into three categories: the classifier-based IDS, the behavioral prediction-based IDS and the statistics and cryptography-based IDS.

(1) Classifier-based IDS:

Brust *et al.* [8] proposed a UAV defense system based on the self-balancing clustering method. When an intrusion is detected, the rogue UAVs or maliciously-targeted aircraft can be tracked by the UAV group used for defense, which effectively reduce the communication losses. However, this solution increases the burden on the drone node. Sedjelmaci *et al.* [9] proposed a kind of IDS which can support VANET node's high-speed moving and fast topology by using the algorithm of secure clustering. They overcome the mobility and network vulnerability of cluster member nodes during the initialization phase of distributed ad hoc networks, and select the appropriate cluster head node according to the mobility state and trust level of nodes, which effectively reduce the communication overhead. In addition, based on the existing dynamic link routing protocol, Wahab *et al.* [10] reduced the size of training dataset by restricting data collection and storage, and adopted the classification technology of support vector machine (SVM) to implement collaborative monitoring between vehicles in online and incremental manner, and reduced the cost of exchanging results between nodes by transporting the final decision in some data clusters. This scheme improves the accuracy of intrusion detection to a certain extent. Similarly, in order to ensure the privacy and sensitivity of the health data of Telemedicine monitoring system, Ahmad *et al.* [11] used random forest algorithm for benchmark datasets to detect the DoS and DDoS attacks on VANET-assisted telemedicine monitoring systems, and improved the systematic security and intrusion detection accuracy. This scheme allows users to successfully access the complete network of data.

(2) Behavioral prediction-based IDS:

VANET or UAV networks use open wireless media with no fixed security infrastructure or sophisticated dynamic topologies, which gives attackers the opportunity to take advantage of. Alheeti *et al.* [12] proposed an intrusion detection model for VANET using artificial neural network (ANN) technology. Using the behavior of nodes in the network as training data, this scheme can accurately detect DoS and selective forwarding attacks. However, there are too many features extracted from the tracking files of VANET behavior, which can affect the efficiency of the classifier. In order to solve this problem, they used Proportional Overlapping Scores (POS) method to reduce the number of features used for classification, and then combined with ANN and fuzzy clustering techniques to design an IDS, which can effectively detect the node attacked by black holes attacks [13]. Similarly, in order to solve the problem of black hole attacks on multi-point relays in ad-hoc network, Baiad *et al.* [14] proposed an optimized link state routing protocol to improve the existing watchdog intrusion detection model. They took into account the test results from MAC layer and the network layer of VANET to avoid the high false alarm rate due to channel conflicts. However, the high-speed moving UAV network differs from VANET, so the routing protocol is not perfect for UAV networks. Misra *et al.* [15] applied the concept of learning automaton (LA) to IDS for VANET, which can detect the malicious data in the network with high accuracy. However, the detection of malicious data can only guarantee the reliability of data collected by UAV, but cannot detect attacks on nodes inside the network. These attacks pose a more serious threat to the life cycle, energy consumption and communication behavior of the entire network. Later, Bouali *et al*. [16] pointed out that certified nodes with certificates can attack under the premise of complying with the implemented protocols. Therefore, they used Kalman filter to predict the upcoming behavior of network nodes, and divided them into three kinds (normal nodes, abnormal nodes and the nodes to be observed) according to the expected trust. This scheme can detect and prevent DoS attacks, Sybil attacks and false alarm attacks, and exclude the malicious nodes.

(3) Statistics and cryptography-based IDS:

An intrusion detection system for VANET application layer was proposed by Zaidi *et al*. [17], which used a method of exchanging collaborative information and a statistical method to demonstrate good intrusion detection effect in dynamic topologies and high-speed moving networks. This scheme can significantly reduce the packet loss rate and deal with known types of network attacks. But in complex wireless network environments, the identification of attacks should have ambiguous characteristics. Mitchell *et al*. [18] designed a behavior rule-based IDS that demonstrated the impact of violent, random and opportunistic attackers on the system. By auditing UAVs in the distributed network architecture, this system can test and evaluate the working status. It shows superior performance under complex network environment and attack, greatly reduces the false alarm rate and false alarm rate. In addition, a packet-key authentication and malicious behavior detection model is designed [19]. Handshakes and the message signatures are preformed among nodes within a certain transmission range. What's more, a group key is generated at the end of each period, which is used to authenticate the identity of nodes in that group. In addition, they use the vehicle's location information and time stamp to determine the malicious behavior in the network. This scheme can effectively reduce the transmission delay, communication overhead and packet loss rate.

In this paper, a Bayesian game theory model is proposed to solve the UAV network security problem. IDS agents and attackers maximize their respective profits, achieving a balance between high detection rate and low overhead. Bayesian game means that game participants do not have complete information on the profit function of the opponent. In this paper, incomplete information means that the IDS agent is not sure of the type of attacker and the attacker is not sure whether its neighbor node is an IDS agent or not. And we prove that the proposed intrusion detection system (BGM) using Bayesian game theory has good performance through simulation.

The remainder of this paper is organized in the following manner: Section 2 presents the network monitoring architecture and describes our intrusion monitoring based on Bayesian games. Section 3 discusses the security analysis and simulation results. Finally, conclusions are presented in Section 4.

2 The UAV Network Architecture and Intrusion Monitoring Based on Bayesian Game

In this section, we present the UAV network architecture, and discuss the design of intrusion detection system based on Bayesian game.

2.1 The UAV Network Architecture

Assuming that the UAV network is deployed over an area, we use the LEACH routing protocol to achieve clustering hierarchical organization, as shown in **Figure 1**. In order to reduce the broadcast storm and achieve a better transmission rate, UAV network is divided into a certain number of clusters. And each cluster has a cluster head node which collects the data regularly collected by the common UAV nodes and then forward the aggregated data to the Sink node in a multi-hop manner. What’s more, the Sink node is relatively safe and cannot be easily compromised.

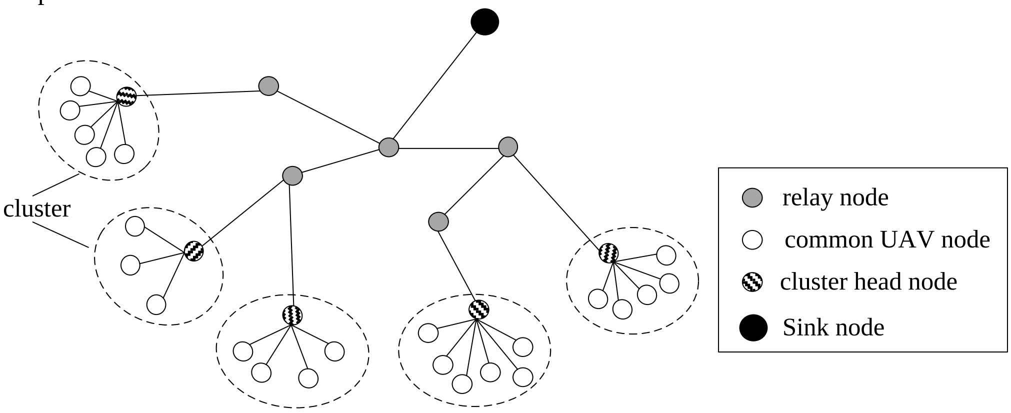


Fig. 1. Distributed Network Architecture

In a security-oriented application, once a UAV node discovers a suspicious event, it broadcast an alarm message to its neighbor nodes. The UAV nodes that receive the alarm message will also continue to transmit the message to their neighboring nodes until the destination (for example, the base station) receives the alert message and triggers further actions (such as reporting to the police / fire department, etc.) to avoid irreparable events. In this paper, our goal is to protect the UAV network and detect malicious actions initiated by attackers, such as DoS attacks, false alarms and Sybil attacks.

2.2 The Design of Intrusion Detection System

In this research effort, our goal is to monitor the behavior of the UAV to ensure the safety of the UAV network. And node monitoring tasks are performed by an intrusion detection system (IDS) agent. Not only the relay node and the cluster head node but also the cluster head node and the common UAV node monitor each other. Each node in the network can act as an IDS agent. However, there is a problem worth considering that If each node performs IDS from the beginning to the end of the execution of a task, a large amount of overhead is added, thereby the network performance will be degraded. How to minimize the overhead under the premise of high detection rate is the focus of this paper.

Only the best number of nodes perform monitoring procedures to monitor the node with the highest probability of causing malicious behavior, thus we can reduce the overhead while ensuring UAV network security. Therefore, it should be fairly accurate when to implement IDS. In this paper, the execution of IDS is determined by Bayesian Nash equilibrium game theory by studying the past behavior of UAV nodes, that is, IDS will be launched before or during an attacker's malicious behavior.

As shown in **Figure 1**, it is assumed that an IDS embedded in the sink node monitors the relay nodes, an IDS embedded in the relay node monitors cluster head node, and an IDS embedded in a cluster head node monitors a common UAV node, and an attacker can attack any node. In this paper we set up two players IDS agent (I_{IDS}) and attacker ($I_{attacker}$) for the purpose that the IDS Agent should be activated to monitor the neighbor nodes that are expected to perform malicious behaviors. I_{IDS} and $I_{attacker}$ have a set of strategies $\delta_{IDS} = \left\{ \alpha_i^1 \middle| i = 1, 2, ..., m \right\}$ and

$\delta_{attacker} = \{\beta_j^2 \mid j = 1, 2, ..., n\}$, respectively, where m, n respectively represent the maximum number of strategies that I_{IDS} and $I_{attacker}$ can enforce.

I_{IDS} and $I_{attacker}$ can randomly adopt any strategy (α_i^1, β_j^2), but the profit obtained by each strategy is different, as shown in Table 1, where P_{ij} and $P_{ji}^{'}$ respectively represent the profits obtained by I_{IDS} and $I_{attacker}$, that is, a set of profits obtained by these two players can be defined according to the α_i^1 and β_j^2 strategy that are performed by each of them.

Table 1. The strategies and profits of IDS agent and attacker.

$I_{attacker}$ \ I_{IDS}	β_1^2	β_2^2	$\cdots$	β_n^2
α_1^1	$(P_{11}, P_{11}^{'})$	$(P_{12}, P_{12}^{'})$	$\cdots$	$(P_{1n}, P_{1n}^{'})$
$\cdots$	$\cdots.$	$\cdots$	$\cdots.$	$\cdots\cdots.$
α_m^1	$(P_{m1}, P_{m1}^{'})$	$(P_{m2}, P_{m2}^{'})$	$\cdots$	$(P_{mn}, P_{mn}^{'})$

The UAV network intrusion detection system can be divided into the following four situations:

(1) When the node does not perform intrusion detection but the attacker initiates a malicious behavior, the profits $(P_{ij}, P_{ij}^{'})$ obtained by the players I_{IDS} and $I_{attacker}$ are respectively as follows:

$$P_{ij} = \text{-FNDR} * \text{D}, \tag{1}$$

$$P_{ij}^{'} = \text{FNDR} * \text{D-OVERH}, \tag{2}$$

where $\text{FNDR}(0 \le \text{FNDR} \le 1)$ represents the probability that a node is classified as a normal node in the execution of malicious behavior, that is, the rate of false negative detection, $\text{D}(0 \le \text{D} \le 1)$ represents the damage caused by the attacker in performing malicious behavior, $\text{OVERH}(0 \le \text{OVERH} \le 1)$ represents the overhead caused by the attacker in performing malicious behavior, including the overhead of message exchange and computational processing.

(2) When the node performs intrusion detection and the attacker initiates a malicious behavior, the profits $(P_{ij}, P_{ij}^{'})$ obtained by the players I_{IDS} and $I_{attacker}$ are respectively as follows:

$$P_{ij} = D^{'} * EDR, \tag{3}$$

$$P_{ij}^{'} = -\left(D^{'} * EDR + OVERH\right), \tag{4}$$

where $D^{'}$=1-$D\left(0 \le D^{'} \le 1\right)$ represents the damage caused to the IDS caused by the malicious behavior of the attacker; $EDR\left(0 \le EDR \le 1\right)$ represents the IDS expected detection rate when the detected node happens to have malicious behavior. $D^{'} * EDR$ is equal to the overhead $OVERH^{'}\left(0 \le OVERH^{'} \le 1\right)$ incurred by the IDS agent in performing the detection process, which includes the overhead of message exchange and computational processing. In addition, since I_{IDS} monitors the number of messages sent and received by $I_{attac\mathrm{ker}}$ and its behavior, we default to this fact that the IDS knows the attacker's $OVERH^{'}$.

(3) When a node performs intrusion detection but the attacker did not initiate any malicious behavior, the profits $\left(P_{ij}, P_{ij}^{'}\right)$ obtained by the players I_{IDS} and $I_{attac\mathrm{ker}}$ are respectively:

$$P_{ij}\text{=-}\left(FPDR + OVERH^{'}\right), \tag{5}$$

$$P_{ij}^{'}\text{=}FPDR, \tag{6}$$

Where $FPDR\left(0 \le FPDR \le 1\right)$ is the probability of a node being classified as a malicious node when it performs normal behavior, that is, a false positive detection rate.

(4) When the node does not perform IDS detection and the attacker did not initiate any malicious behavior, the profits $\left(P_{ij}, P_{ij}^{'}\right)$ obtained by players I_{IDS} and $I_{attac\mathrm{ker}}$ are respectively:

$$P_{ij}\text{=-}FPDR, \tag{7}$$

$$P_{ij}^{'}\text{=}FPDR. \tag{8}$$

In the following we describe the best balance between IDS high detection and low overhead using Bayesian Nash equilibrium game theory.

Let ω_i be the probability that I_{IDS} accept α_i^1, υ_i be the probability that $I_{attac\mathrm{ker}}$ accept β_{j}^2. To achieve the best balance, the benefits that IDS agents and attackers can gain are first calculated:

$$R_{IDS}\left(W,V\right)\text{=}\sum_{i=1}^{m}\sum_{j=1}^{n} P_{ij} \bullet \omega_i \bullet \upsilon_j \tag{9}$$

$$R_{attac\mathrm{ker}}\left(W,V\right)\text{=}\sum_{i=1}^{m}\sum_{j=1}^{n} P_{ij}^{'} \bullet \omega_i \bullet \upsilon_j \tag{10}$$

Where $W = \left\{w_1, w_2, ..., w_m\right\}$ and $V = \left\{\upsilon_1, \upsilon_2, ..., \upsilon_m\right\}$ represent the probability distributions of strategies adopted by IDS agents and attackers respectively. During the game, both sides maximize and minimize the value by selecting the appropriate the value ω_i and υ_i. Now consider the best balance between the two parties:

$$\overline{E_{IDS}} = \min_{W} \max_{V} R_{IDS}\left(W,V\right) = \max_{W} \min_{V} R_{IDS}\left(W,V\right) = \underline{E_{IDS}} \tag{11}$$

$$\overline{E_{attac\ker}} = \min_{W} \max_{V} R_{attac\ker}\left(W,V\right) = \max_{W} \min_{V} R_{IDS}\left(W,V\right) = \underline{E_{attac\ker}} \tag{12}$$

$\left(\overline{E_{IDS}}, \overline{E_{attac\ker}}\right)$ and $\left(\underline{E_{IDS}}, \underline{E_{attac\ker}}\right)$ respectively represent the upper and lower bounds of the game, so when the maximum return and the minimum return obtained by the strategy of IDS agent and attacker are equal, the optimal equilibrium state of the game is reached:

$$\begin{cases} \overline{E_{IDS}} = \underline{E_{IDS}} \\ \overline{E_{attac\ker}} = \underline{E_{attac\ker}} \end{cases} \tag{13}$$

It is assumed here that the probability of each node performing malicious behavior is MAR, and when the node's MAR reaches the threshold, IDS is started. The definition of MAR is as follows:

$$\begin{gathered} MAR_1 = x_1 \cdot T_{DoS} + y_2 \\ MAR_2 = x_2 \cdot e^{T_{FI}} + y_1 \\ MAR = \frac{T_{DoS} + T_{FI}}{MAR_1 + MAR_2} \end{gathered} \tag{14}$$

Where $0 \le MAR \le 1$, MAR_1 (linear function) denotes the probability of malicious behavior of nodes propagating false information (FI), MAR_2 (exponential function) indicates the probability of malicious behavior of a node attacked by DoS, T_{DoS} indicates the times of DoS malicious events, T_{FI} indicates the number of false information events, and x_1, x_2, y_1, y_2 represent weight factors which are limited to [0,1].

$$MAR \ge \overline{E_{attac\ker}} \tag{15}$$

When the above conditions are met, the node preforms the IDS to monitor malicious nodes where $0 \le \overline{E_{attac\ker}} \le 1$.

Each node in the UAV network determines whether to start IDS by calculating MAR and $R_{IDS}\left(W,V\right)$, and players I_{IDS} and I_{attacker} gain the maximum profit by choosing different strategies. The nodes satisfying condition (15) start IDS monitoring in time period λ_1, shut down the IDS within the time period λ_2 and no longer monitor their neighbor nodes. Then these nodes repeat the process and proceeds to compute MAR and $R_{IDS}\left(W,V\right)$ to decide whether to start IDS.

Thus, the choice of time periods λ_1 and λ_2 is important, so they are related to the performance of the system and the security of the network. When λ_1 is too long and λ_2 is too short, the execution of IDS takes too long, which increases the system overhead. When λ_1 is too short and λ_2 is too long, the IDS is performed for a short time, and it may happen that when an attacker performs malicious behavior but IDS is turned off, which reduces the expected detection rate.

3 Experiments and Results

In this paper, we used NS-3 network simulator to implement our method. In order to simulate the high reliability of the UAV network, the UAV will fly in a clear trajectory. In the process of experiment simulation, we used three attack models: DoS attacks, false alarms and Sybil attacks. DoS attacks include: black holes, selective forwarding, and the attacks on communication media in the network that are blocked by attackers which cause exhaustion of network resources. False alarms are considered as the most dangerous attacks. Attackers attempt to change the direction of UAV flight by spreading false messages which in turn leads to irreparable consequences. Sybil attack refers to the behaviors which use the malicious nodes to create a number of false nodes causing network congestion and affecting the normal operation of the system.

3.1 Experiments Settings

We set the simulation area to $3000*3000m^2$. The type of attack on each node was randomly selected. The attacked nodes accounted for 10% -40% of all the nodes in the network and cannot exceed 40%, otherwise the network is not reliable network.

The settings of simulation parameters are shown in Table 2:

Table 2. The settings of simulation parameters

parameters	values
Simulation area	$3000*3000m^2$
Simulation time	420s
Number of UAVs	300
Speed	80-120km/h
Radio range	250m
Malicious UAVs	10%-40%

From the analysis in the previous section, we can see that the values of λ_1 and λ_2 is very important to the result. Therefore, in this section we first choose an optimal value through calculation, which makes IDS have a higher expected detection rate and lower overhead. λ_1 and λ_2 are expressed as:

$$\lambda_1 = a_1 \cdot EDR + b_1 \cdot OVERH' , \tag{16}$$

$$\lambda_2 = a_2 \cdot EDR + b_2 \cdot OVERH' , \tag{17}$$

where a_1, a_2 $\left(0 \le a_1, a_2 \le 1\right)$ denote weighting parameters for the expected detection rate of IDS, b_1, b_2 $\left(0 \le b_1, b_2 \le 1\right)$ denote weighting parameters for the cost required for IDS to perform the detection. What's more, $0 \le a_1, a_2, b_1, b_2 \le 1$. When $a_1 = 1$, $a_2 = 1$, $b_1 = 0$, $b_2 = 0$, it means that the system is only concerned with the detection, does not care about the overhead. When $a_1 = 0$, $a_2 = 0$, $b_1 = 1$, $b_2 = 1$, this means that the system is more concerned with the overhead, and what we need to consider is the value of a_1, a_2, b_1, b_2 for which the expected detection rate and overhead are optimal.

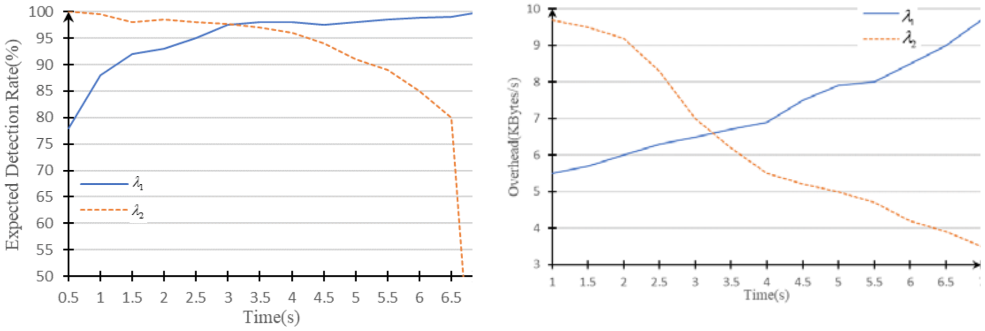


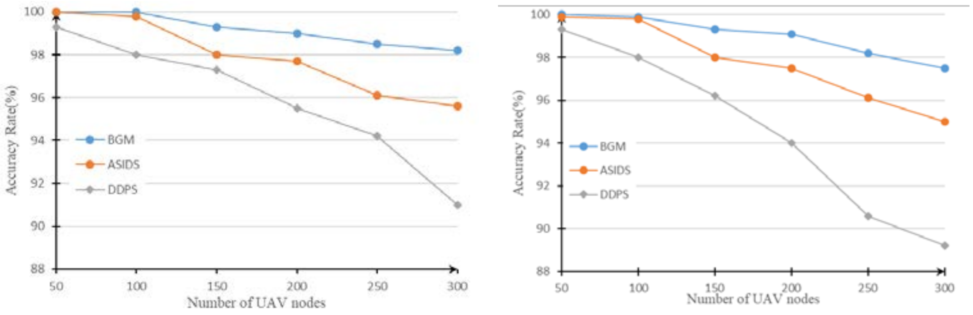
Fig. 2. (a) Expected detection rate (b) Communication overhead

It can be seen from **Figure 2** that when $\lambda_1 = 3\,\mathrm{s}$, $\lambda_2 = 3.5\,\mathrm{s}$, the expected detection rate is close to 98%, and the communication overhead at this time is close to 6.3 Kbytes / s. Therefore, we compare the accuracy and the overhead between the expected detection system with others in the case of $\lambda_1 = 3\,\mathrm{s}$, $\lambda_2 = 3.5\,\mathrm{s}$.

3.2 Experimental Results

3.2.1 Comparison of accuracy

We compared the proposed detection method BGM with the adaptive specification-based intrusion detection system (ASIDS) described in [18] and the distributed detection and prevention scheme (DDPS) mentioned in [16]. As shown in **Figure 3**, regardless of whether a malicious node accounts for 10%, 20%, 30%, or 40% of the entire network, the detection accuracy of the BGM is much higher than that of ASIDS and DDPS, up to 91%, which is especially clear when the network's summary nodes increase and malicious nodes increase. This is because the approach in BGM is to start the optimal number of IDS agents to protect the neighboring nodes that may be targets of attacks. While the network distributions of both ASIDS and DDPS are not optimal and cannot properly start IDS mode and turn off IDS mode, it will have a higher false alarm rate.



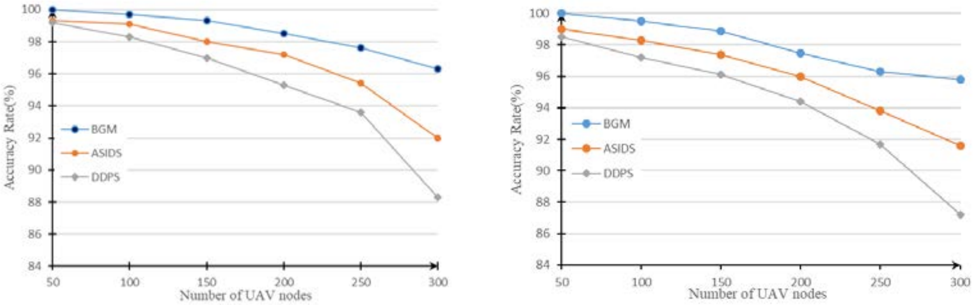


Fig. 3. Comparison of Accuracy: The ratio of the number of attackers to the total number of network nodes (a) 10% (b) 20% (c) 30% (d) 40%

3.2.1 Comparison of overhead

As shown in **Figure 4**, the overhead of the security detection method BGM proposed in this paper is still compared with that of ASIDS and DDPS. We adjust the number of malicious nodes to the maximum, which accounts for 40% of the network nodes.

For the ASIDS scheme, when the number of attacker reaches 40% of the network nodes, the IDS agent will continue to handle the OPEN state, so a large number of messages will be generated to detect whether the node being detected is a malicious node, resulting in a large amount of overhead. Therefore, among the three detection schemes, the DDPS scheme and the BGM scheme are better than the ASIDS scheme. In addition, the BGM scheme calculates the optimal number of nodes to start IDS and appropriately adjusts the time to start and shut down the IDS during detection process, thereby greatly reducing the overhead of the network.

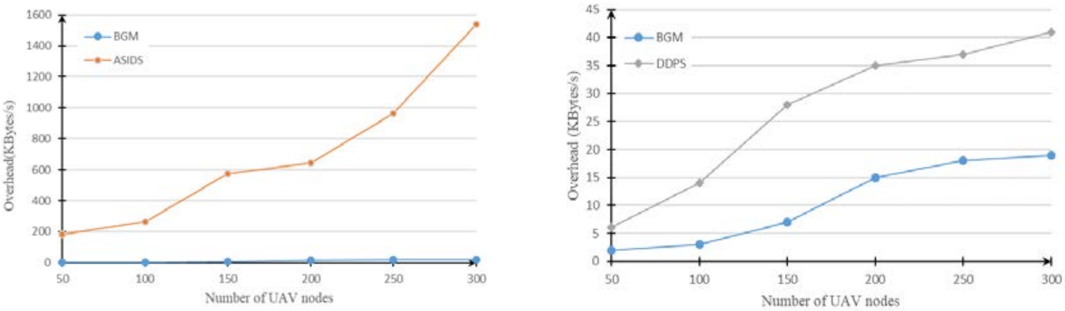


Fig. 4. The comparison of overhead (a) BGM and ASIDS (b) BGM and DDPS

3 Conclusions

With the rapid development of UAV technology, UAVs have played an important role in various fields such as agricultural irrigation, transportation of goods, traffic detection, wind power estimation, disaster area rescue and so on. Therefore, the security of UAV network has also been increasingly people's attention. In this paper, we use Bayesian game theory to propose an intrusion detection model to effectively detect malicious nodes in the network. The game problem is defined between the IDS agent and the attacker. These two players choose different strategies to maximize their profits. Through the Bayesian Nash equilibrium theory, we prove that the proposed intrusion detection scheme has the advantage of low overhead with high detection rate. Simulation results show that the intrusion detection method based on Bayesian game theory has better performance than other methods.

Acknowledgments. This work was supported by project of NSFC of China (61472096, 61202455, 61501132, 61370084, 61301095).

References

[1] Grumazescu, C, Vlăduţă, VA, Subaşu, G.: WSN solutions for communication challenges in military live simulation environments. International Conference on Communications. pp. 319-322 (2016)

[2] He, D, Chan, S, Guizani, M.: Communication Security of Unmanned Aerial Vehicles. Vol. 99, pp. 2-7. IEEE Wireless Communications (2016)

[3] Erritali, M, Ouahidi, BE.: A review and classification of various VANET Intrusion Detection Systems. Security Days. pp. 1-6 (2013)

[4] Nijim, M, Mantrawadi, N.: Drone classification and identification system by phenome analysis using data mining techniques. Technologies for Homeland Security. pp. 1-5 (2016)

[5] Sedjelmaci, H, Senouci, SM, Ansari, N.: Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology. Vol. 99, pp. 1-11. IEEE Transactions on Intelligent Transportation Systems (2017)

[6] Anouar, B, Mohammed, B, Abderrahim, G, et al.: Vehicular navigation spoofing detection based on V2I calibration. IEEE International Colloquium on Information Science and Technology (2017)

[7] Kim, H, Ben-Othman, J, Bellavista, P.: Collision-free Reinforced Barriers in UAV Networks. Vol. 22, pp. 289-300. Journal of Computational Science (2017)

[8] Brust, MR, Danoy, G, Bouvry, P, *et al*.: Defending Against Intrusion of Malicious UAVs with Networked UAV Defense Swarms. IEEE, Conference on Local Computer Networks Workshops. pp. 103-111 (2017)

[9] Sedjelmaci, H, Senouci, SM.: An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. Vol. 43, pp. 33-47. Computers & Electrical Engineering (2015)

[10] Wahab, OA, Mourad, A, Otrok, H, *et al*.: CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. Vol. 50, pp. 40-54. Expert Systems with Applications (2016)

[11] Ahmad, I, Fazal-e-Amin, *et al*.: Towards Intrusion Detection to Secure VANET-Assisted Healthcare Monitoring System. Vol. 7, pp. 1391-1398. Journal of Medical Imaging & Health Informatics (2017)

[12] Alheeti, KMA, Gruebler, A, Mcdonald-Maier, KD.: An intrusion detection system against malicious attacks on the communication network of driverless cars. Consumer Communications and NETWORKING Conference. pp. 916-921 (2015)

[13] Alheeti, KMA, Gruebler, A, Mcdonaldmaier, KD.: An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars. International Conference on Emerging Security Technologies. pp. 86-91 (2015)

[14] Baiad, R, Otrok, H, Muhaidat, S, *et al*.: Cooperative cross layer detection for blackhole attack in VANET-OLSR. Wireless Communications and Mobile Computing Conference. pp. 863-868 (2014)

[15] Misra, S, Krishna, PV, Abraham, KI.: A stochastic learning automata-based solution for intrusion detection in vehicular ad hoc, networks. Vol. 4, pp. 666-677. Security & Communication Networks (2011)

[16] Bouali, T, Senouci, S, Sedjelmaci, H.: A distributed detection and prevention scheme from malicious nodes in vehicular networks. Vol. 29, pp. 1683-1704. International Journal of Communication Systems (2016)

[17] Zaidi, K, Milojevic, MB, Rakocevic, V, *et al*.: Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection. Vol. 65, pp. 6703-6714. IEEE Transactions on Vehicular Technology (2016)

[18] Mitchell, R, Chen, IR.: Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications. Vol. 44, pp. 593-604. IEEE Transactions on Systems Man & Cybernetics Systems (2014)

[19] Kumaresan, G, Macriga, TA.: Group Key Authentication scheme for Vanet INtrusion detection (GKAVIN). Vol.1, pp. 1-11. Wireless Networks (2016)