doi:10.3772/j.issn.1006-6748.2020.03.011

Detecting and adaptive responding mechanism for mobile WSN①

Zhao Min(赵 敏), Qin Danyang②, Guo Ruolin, Xu Guangchao
(Key Laboratory of Electronic and Communication Engineering, Heilongjiang University, Harbin 150080, P. R. China)

Abstract

Mobile wireless sensor network (WSN) composed by mobile terminals has a dynamic topology and can be widely used in various fields. However, the lack of centralized control, dynamic topology and limited energy supply make the network layer of mobile WSN be vulnerable to multiple attacks, such as black hole (BH), gray hole (GH), flooding attacks (FA) and rushing attacks (RU). Existing researches on intrusion attacks against mobile WSN, currently, tend to focus on targeted detection of certain types of attacks. The defense methods also have clear directionality and is unable to deal with indeterminate intrusion attacks. Therefore, this work will design an indeterminate intrusion attack oriented detecting and adaptive responding mechanism for mobile WSN. The proposed mechanism first uses a test sliding window (TSW) to improve the detecting accuracy, then constructs parameter models of confidence on attack (COA), network performance degradation (NPD) and adaptive responding behaviors list, finally adaptively responds according to the decision table, so as to improve the universality and flexibility of the detecting and adaptive responding mechanism. The simulation results show that the proposed mechanism can achieve multiple types of intrusion detecting in multiple attack scenarios, and can achieve effective response under low network consumption.

Key words: mobile wireless sensor network (WSN), network security, intrusion detection, adaptive response

0 Introduction

The inherent mobility, complexity, and variability make mobile wireless sensor network (WSN) vulnerable to attacks and damage, while bringing potential safety hazard to sensitive information in the military field and private information in the civilian domain[1,2]. In the process of communication, it is difficult to achieve complete protection of information by relying only on encryption technology and authentication technology[3-5]. Thus, in order to ensure higher security, it is essential to deploy a defense system on key nodes of the network system. Compared with firewalls, intrusion detection system is an active defense technology, which can make up for the deficiencies of the firewall technology. Such a detection system can actively collect information in network or system in real time to analyze and estimate. If the information is against the relevant security rules, there will be an alarm and relative response to protect the whole system. Most of the current intrusion detection methods[6,7] seldom consider the attack response, which has great limitations in the practical application of dealing with unknown attacks. Refs [8-10] showed how the isolated nodes operate to defense predetermined attacks, but the defense effect is not ideal when dealing with uncertainties and various types of intrusion attacks, and the blind isolation attacks have a great negative impact on the network. Ref. [11] proposed an effective intrusion responding mechanism based on agents' collaboration. Ref. [12] proposed a protection mechanism based on neighbor trust for mobile WSN.

Aiming at the security problem of mobile WSN, the typical intrusion attacks will be analyzed deeply. Considering the one-sidedness and separation of the existing detection and intrusion responding method, a novel intrusion detection and adaptive responding mechanism will be proposed for mobile WSN, combining knowledge-based intrusion detection (KBID) with anomaly-based intrusion detection (ABID), so as to protect mobile sensor networks from various practical attacks. In addition, a cluster method[13] will be adopted to improve scalability and alleviate the over-

① Support by the National Natural Science Foundation of China (No. 61771186), University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province (No. UNPYSCT-2017125), Outstanding Youth Project of Provincial Natural Science Foundation of China (No. YQ2020F012) and Graduate Innovative Research Project of Heilongjiang University (No. YJSCX2020-061HLJU).

② To whom correspondence should be addressed. E-mail: qindanyang@hlju.edu.cn

Received on Mar. 6, 2019

head.

The subsequent sections are organized as follows: typical intrusion attacks and intrusion detection methods for mobile WSN is analyzed comprehensively in Section 1. Section 2 presents an effective intrusion detecting method for multiple types of mobile WSN, and an adaptive responding mechanism model is established. Section 3 simulations the proposed intrusion detecting and adaptive responding mechanism are performed in terms of the success delivery rate, false alarm rate, rationality of response behavior and the network performance degradation. Section 4 summarizes the paper and presents the conclusions.

1 Related work

The limited energy, the mobility of nodes, the large scale of distribution, and the dynamic topology make mobile WSN be vulnerable to various attacks[14]. In this regard, the protection mechanisms of 2 typical mobile WSNs[15,16] will be described briefly as follows. This work will compare the proposed mechanism with these 2 existing mechanisms for performance in the Section 3.

(1) Cost-sensitive intrusion responding: cost-sensitive intrusion responding model will estimate the topology dependent index (TDI), which indicates the times of the routing service of the nodes being interrupted when a intruder is isolated. After estimating the attack damage index (ADI), the loss attack will be calculated according to the number of affected nodes so as to indicate the damage caused by the attack to the mobile sensor network. When ADI is greater than TDI, the node will respond to the intrusion by complete isolation; when ADI is less than TDI, the node will respond to the intrusion by relocation; when ADI is close to TDI, the attack will be temporarily isolated when ADI is twice greater than TDI. The intrusion responding types adopted in such model can be normal, recovery, complete isolation, temporary isolation, and relocation.

The cost-sensitive model is applicable to active routing protocols such as optimized link state routing (OLSR), which requires the complete network topology rather than reactive routing protocols such as ad hoc on-demand distance vector routing (AODV) based on partial topology information.

(2) Generalized intrusion detecting and responding mechanism: generalized intrusion detecting and responding method mainly adopts the combination of anomaly-based and knowledge-based intrusion detection to ensure the mobile WSN lying in safe state facing to various attacks. The architecture of the mechanism consists of a data collection module, a training module, a test module, an attack identification and inference module, and an attack recognition module. In the case of an intrusion, the cluster head will invoke the attack identification and inference module to obtain the rules from the knowledge base to defend against intrusion. If an unknown attacker occurs, the interpreter will keep the rule path and look for a match for the rule path in the current test sliding window. If a match is found, a new rule will be established and a set of additional new rules will be stored in the knowledge base to confirm the new rule detection.

Though some unknown attacks can be detected and mobile WSN will be protected against typical attacks in some degree, the attacker being isolated, as the primary defensing method, will affect the network performance much more seriously.

2 Intrusion detecting and adaptive responding

2.1 Key assumption

Detecting anomalies in the network will ask for a training model based on anomaly-based intrusion detection. Such model depends on the data tracking and traffic patterns of normal events. However, data resources reflecting normal activities or events are not available for mobile sensor networks currently. Thus, assume that there is no abnormal behavior in network initialization. Moreover, in order to improve the scalability of the adaptive responding mechanism, a clustered mobile network organizing model is introduced, where the network nodes are divided into management nodes (MNs), cluster heads (CHs) and cluster nodes (CNs) according to different functions. In addition, a security mechanism[17] is further introduced to protect the communication between MNs, CHs, and CNs. Details will not be mentioned since the intrusion detection and intrusion response are focused on in this paper.

2.2 Adaptive responding mechanism

The architecture model will be established and the adaptive responding mechanism will be presented in this part. Intrusion detecting and responding process, as shown in Fig. 1, mainly includes 3 stages: data collecting, training and testing.

2.2.1 Intrusion detecting architecture

(1) Data collecting: this stage depends on the sensors collecting the data periodically so as to monitor the whole network. In particular, CHs will collect the data from CNs in their virtual clusters every TI (time of interval), which are presented as matrix and stored in

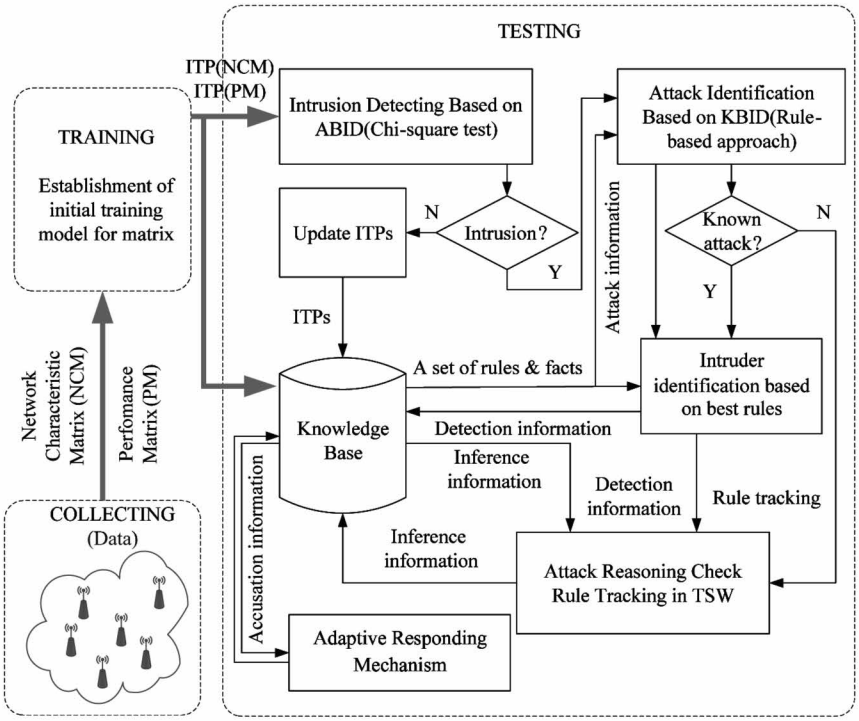


Fig. 1 Proposed intrusion detecting and adaptive responding architecture

the network characteristic matrix (NCM) and the performance matrix (PM). Then, CHs will report these matrices to MNs.

Here AODV is taken as a basic routing algorithm[18] to illustrate the principle of detecting and responding mechanism.

The network characteristic matrix NCM is

$$NCM = \{RREP,\ RREQ,\ RERR,\ TTL,\ RREQ\_scr\_seq,\ RREP\_dest\_seq,\ RREQ\_dest\_seq\}$$

which is composed of 7 parameters with the physical significance shown in Table 1.

Table 1 Parameters in NCM

Symbol	Significance
RREP	Route reply
RREQ	Route request
RERR	Route error
TTL	Time to live
RREQ _ scr _ seq	Route request source sequence
RREP _ dest _ seq	Route reply destination sequence
RREQ _ dest _ seq	Route request destination sequence

NCM is a two-dimensional matrix of $r \times c$ with the number of rows r and the number of columns c depending on matrix parameters. Its number of rows is 7, the 1st row stores the RREP sequences, the 2nd row stores the RREQ sequences, the 3rd row stores the RERR sequences, the 4th row stores the TTL sequences, the 5th row stores the RREQ _ scr _ seq sequences, the 6th row stores the RREP _ dest _ seq sequences, and the 7th row stores the RREQ _ dest _ seq sequences. Moreover, the rows represent different parameters, and the columns represent the data content contained in the parameters. The length of each column depends on the length of the different parameter data. Each row is added as an equal-length sequence by zero padding at the end of the sequence. So, the storage structure is dynamically allocated by the intrusion detecting and adaptive responding mechanism monitor. PM consists of network performance parameters derived from the parameters of NCM.

The performance matrix PM is

$$PM = \{RPO,\ PDR,\ CPD,\ throughput\}$$

which consists of 4 parameters with the physical significance shown in Table 2.

Table 2 Parameters in PM

Symbol	Significance
RPO	Routing protocol overhead: refers to the ratio of the number of packets sent to the destination node to the total required packets
PDR	Packet delivery ratio: refers to the ratio of the number of packets received by the destination to the number of packets sent by the source
CPD	Number of control packets dropped: is the number of lost packets during multi-hops
THP	Throughput: is the amount of data transmitted successfully in unit time, indicating the average throughput of the network

(2) Training: during the training phase, CH collects the information in NCM and PM continuously, and reports the collected data to an MN in a fixed time interval. Then the MN trains the data N times using the training model. The expected value of the NCM is represented by ${}_jX_k^i$, and ${}_jX_k^i = X_1, X_2, X_3, \cdots, X_M$ is a set of random variables representing NCM, where i represents the i-th time interval and j represents the j-th parameter of the NCM, k represents the number of random variables in the j-th parameter of the NCM, $1 \leqslant k \leqslant M$, where M is the maximum value of the random variable of the j-th parameter of the NCM during the i-th time interval. Similarly, the expected value of the PM is represented by ${}_jY_k^i$.

MN calculates the expected value $P({}_jX_k^i)$ of probability distribution of NCM within the time interval i, and calculates the expected value $P({}_jP_k^i)$ of probability distribution of PM at the i-th time interval. The whole process is repeated in N time intervals. MN calculates the average of NCM and PM of N time intervals, and then stores these values in an initial training file (ITP) of NCM and PM. These initial training profiles reflect the network performance and normal behavior of nodes in the network.

(3) Testing: in order to fully evaluate the performance, a comprehensive test, corresponding to the system structure in Fig. 1, will be operated in 3 phases, including the intrusion detection phase, the attack identification phase, the intruder identification phase.

Intrusion detection During the intrusion detection phase, MN utilizes the parameters in NCM as well as the chi-square test to identify intrusions in the network. Chi-square test is a ranging based method and has a lower computational cost than other tests such as the Hotelling T2. MN first calculates the probability distribution of each NCM parameter and stores the result as an observation value. Then, using the expected value above, the MN performs a hypothesis test on the zero hypothesis $H_0[j]$ for each parameter j of NCM in TI, i.e. Eq. (1).

$$X^2[j] = \forall_j \left(\sum_{k=1}^{M} \left(\frac{({}_jx_k^i - \overline{{}_jx_k^i})^2}{\overline{{}_jx_k^i}} \right) \right) \tag{1}$$

where j and $k(1 \leqslant k \leqslant M)$ have the same meaning as above. Finally, the MN performs joint hypothesis testing on all parameters of NCM.

If the joint null hypothesis H_0 (the observation of each parameter of NCM meets the expected value) is rejected, it assumes that an intrusion has occurred in the TI, and then proceeds to the attack identification phase.

The initial training model of NCM is updated mainly by exponentially weighted moving average (EWMA) as

$$\overline{{}_jX_{(q,\,k_1^M)}^i} = \beta \cdot X_{(q,\,k_1^M)}^i + (1-\beta)\,\overline{{}_jX_{(q,\,k_1^M)}^i} \tag{2}$$

where each TI is divided into q periods, $\overline{{}_jX_{(q,\,k_1^M)}^i}$ and ${}_jX_{(q,\,k_1^M)}^i$ represent the expected value and the observed value of j-th parameter of NCM, respectively when the number of updates is q. When no intrusion is detected, the q is increased in TI. And $\beta = 2/q - 1$ is a weighting factor. The updated expected profile model will reflect the current behavior of the network.

Attack identification If a network intrusion is detected, MN will enter the attack identification phase. In such phase, a rule-based approach will be adopted to identify the current attacks. The proposed adaptive responding mechanism is designed to have the knowledge base used throughout the testing phase, which consists of facts, rules, and inference engines.

A rule model for attack and intruder identification is established according to the analyses on typical attacks in mobile WSN with the knowledge base model of the adaptive protection mechanism shown in Fig. 2, where the inference engine will use forward links on the rule set and look for target conditions to represent the known attacks so as to identify the attack.

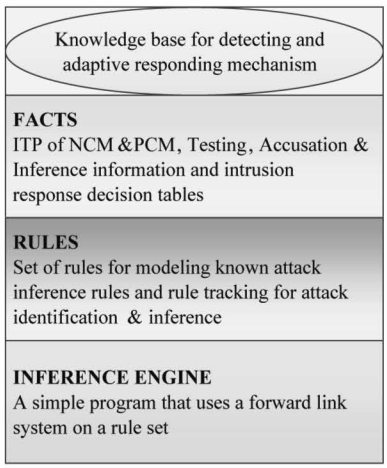


Fig. 2 The knowledge base for adaptive responding mechanism

Intruder identification The MN will initiate the intruder identification after an attack is identified. In this phase, the MN will select a known attack-oriented intruder identification rule. For example, when a black hole attack occurs, it is necessary to analyze RREP packets of all nodes in the latest time interval to find the node that has generated the false route reply packet with the highest target sequence number.

When the intruder is identified, it will be isolated, no matter what kind of the attack there is or whether the intruder isolation is the best choice or not.

Such fixed intrusion response will affect the network performance seriously. Therefore, in order to improve the overall effectiveness of the protection mechanism, an adaptive responding mechanism will be presented and described in the next section.

2.2.2 Adaptive responding mechanism

(1) Architecture: after the intrusion detection, the MN will perform the proposed adaptive responding mechanism with the architecture shown in Fig. 3.

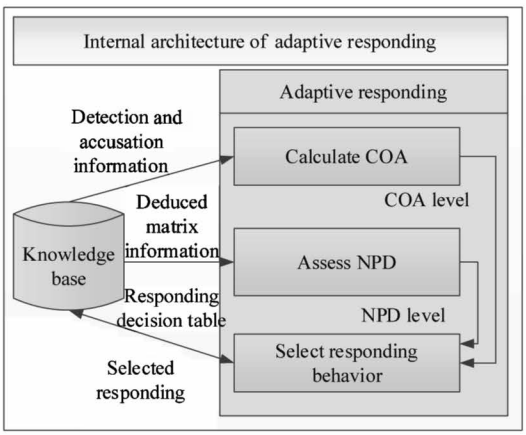


Fig. 3 Knowledge base for adaptive responding mechanisms

The general process of the proposed adaptive responding mechanism has 3 steps. Firstly, the MN will calculate the COA based on the detection information and the allegation information. Then the NPD will be evaluated using the parameters in PM to measure the severity of the attack. Finally, an appropriate responding behavior will be selected to achieve the effective security protection. Among them, the responding behavior selection is based on the decision table, which will provide the responding selection criteria according to COA, NPD and the suitability of the behavior in the current environment.

(2) Intrusion responding behavior: based on the list of intrusion responding behaviors in the literature, first, the appropriateness of the responding behavior is judged based on the magnitude of the adverse effects that the responding behavior may have on network performance. Then, further analyze the effectiveness of the responding behavior in reducing the damage caused by the intrusion and preventing further attacks from the invading nodes. Finally, based on the confidence on attacks and the impact of attacks on network performance degradation, a list of adaptive responding behavior with 3 intrusion responding behaviors is presented below.

Complete isolation Such responding behavior will be adopted when the detected attack is highly credible and the attack is severe to cause the network performance declining. The complete isolation may change the network topology or even cause global routing discovery, but the security performance of the network will be assured significantly.

Attacker bypass When the confidence of the detected attack is quite high and the network performance degradation cannot be negligible, the responding mechanism will find one or multiple nodes to replace the attack rather than initializing a new RREQ, so as to reduce the global repairing overhead as well as to prevent further attacks.

No punishment When the confidence on attack detection is not high enough or the attack is not serious, and the network performance degradation can be tolerable, the proposed adaptive responding mechanism will simply ignore the attack temporarily, so as to avoid the negative impact on network performance.

2.3 Technical model

COA and NPD are two key factors in the proposed adaptive responding mechanism.

2.3.1 Calculations of COA and NPD

The single detection based intrusion response is unreliable according to the probabilistic nature of intrusion detection. To improve the probability of identifying intruders correctly, the MN will adopt a test sliding window (TSW). Thus, the proposed adaptive responding mechanism will respond to the intrusion only when it is determined that the node is an intruder node in multiple time intervals. Specifically, the intrusion response occurs only when a node is determined to be an intruding node in multiple TSWs with a time interval p, where p is the size of the TSW, that is, the checking times, and d is the minimum times to detect when the detected node is confirmed as an attacker. Different combinations of p and d will give different results. The detection of an intrusion node in a TSW is a Bernoulli test. In other words, the tests performed in the TSW are the same and independent repeated experiments with two possible outcomes: detection or no detection. Therefore, the probability of intrusion determination in the Bernoulli test sequence is known by

$$P_c = \sum_{i=d}^{p} C_i^p \cdot (P)^i \cdot (1-P)^{(p-i)} \tag{3}$$

where, $C_i^p = p!/i!(p-1)!$ is a binomial coefficient, P is the probability of a single detection, and P_c is the probability of confirming that the node is an intruder.

The curves in Fig. 4 show how P_c varies as a function of the number of the required detections d in the condition of different values of probability of a single detection P and the TSW size $p = 5$. It can be seen

that, when $P = 80\%$ and $d = 1$, 2 or 3, the probability of identifying a node as an intruder will exceed 90%.

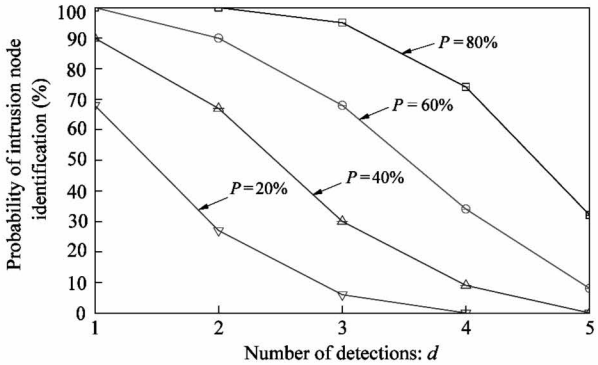


Fig. 4 Probability of correctly identifying intruders

In the current TSW, the MN will perform the proposed adaptive intrusion responding mechanism, as shown in Algorithm 1, for all nodes identified as intruders. Based on the detection information and the allegation information, the MN will estimate the confidence on attack (COA) by

$$COA = \omega_1 \cdot CI + \omega_2 \cdot P_c \tag{4}$$

where, ω_i is the weighting factor to satisfy $w_1 + w_2 = 1$; CI represents the confidence interval of the chi-square test during the intrusion detection phase; Eq. (3) will return the confidence of P_c lying in $[0,1]$. Then the MN will evaluate the network performance degradation (NPD) based on Eq. (5). This is the weighted sum of changes of parameter values (i. e. THA, RPO, PDR, CPD) in the PM from not attacked to its current. NPD is defined as

$$NPD = \omega_1 \cdot \Delta THA + \omega_2 \cdot \Delta THA + \omega_3 \cdot \Delta RPO + \omega_4 \cdot \Delta RPD \tag{5}$$

where Δ represents the change value of each parameter. Once the COA and NPD are obtained, the MN will assign a confidence level to COA and NPD. Considering the practical application of mobile WSN, 4 COA levels are defined as shown in Table 3. For NPD, similar level divisions are adopted with different mapping from NPD to degrading degree.

Table 3 Mappings of COA values and COA levels

COA level	Range of COA (%)
Low	$0 < COA \leqslant 25$
Medium	$25 < COA \leqslant 50$
High	$50 < COA \leqslant 70$
Very high	$COA > 70$

2.3.2 Establishment of decision tables

COA level and NPD level set above are adopted to establish the decision table as shown in Table 4 to select the intrusion response. The knowledge base is assumed to be built in initialization phase and the intrusion responding selection parameters can be configured and modified for different network environments.

The first 2 lines of Table 4 indicate the decision conditions (i. e. COA level and NPD level), and the last 3 lines indicate the responding operations (i. e. complete isolation, attackers bypass, and no punishment). M, L, H in Table 4 mean medium, low and high, respectively, and H + is High plus meaning the level is very high. If the selected intrusion response is complete isolation or attackers bypass, the MN will notify all nodes with intrusion responding behavior by broadcasting an allegation packet (AP).

If the relative response is no punishment, the MN will ignore the attack. When the CN receives packet AP, the broadcasting address and source address of the packet should be checked firstly to avoid duplicated APs. If the accused node V_j has been blacklisted permanently or temporarily, the CN will ignore and remove the AP to prevent unnecessary network traffic, as shown in Algorithm 2. Otherwise, the CN will check the intrusion responding behavior in the alleged packet.

Table 4 Decision table for adaptive responding mechanism

	Level and selection of responding behavior															
COA level	M	H	H +	H +	H	L	L	H	M	M	M	L	H	H +	H +	L
NPD level	H +	H +	H +	M	H	H +	H	M	H	M	L	M	L	L	H	L
Complete isolation	√	√	√	—	√	√	—	—	—	—	—	—	—	—	√	—
Attacker bypass	—	—	—	√	—	—	√	√	√	√	√	—	—	—	—	—
No punishment	—	—	—	—	—	—	—	—	—	—	√	√	√	√	—	√

If the intrusion responding behavior is complete isolation, the CN will add the intruder V_j to the blacklist and broadcast the blacklist to isolate the intruder in the whole network. After receiving the updated blacklist, the nodes will immediately delete all packets from the blacklist node, and ignore the rest relative packets, as shown in Algorithm 3 (1).

If the intrusion responding behavior is attackers bypass, the CN will add intruder V_j to the temporary blacklist table and notify the other nodes to ignore and

delete relative routing packets, including routing inquiry, routing reply, and packets generated or forwarded by intrusion nodes V_j, so as to prevent further attacks. All nodes exclude intruders V_j from the new route discoveries, that is, they choose paths that V_j are not included. However, the node will still forward the data packet received from V_j to the existing route to maintain the current data forwarding service, as shown in Algorithm 3(2). Accepting the data forwarding service from V_j can reduce the likelihood of adverse effects on network performance until the node finds a new route around V_j. This responding behavior also applies for the condition that V_j lies in the critical location or the isolated node V_j may cause a significant negative impact on network performance.

Algorithm 1 Intrusion responding mechanism

For all detected and identified nodes *Vi* in a TSW
Calculate COA value using Eq. (4).
Calculate NPD value using Eq. (5).
Assign COA level based on calculated COA value (Table 3).
Assign NPD level based on calculated NPD value.
Search decision table (Table 4) using COA and NPD levels and identify intrusion responding behavior (IRB)
If (*IRB* = = COMPLETE _ ISOLATION)
MN blacklists *Vi* and broadcasts
Accusation packet (AP) with
IRB = COMPLETE _ ISOLATION
Else If (*IRB* = = ATTACKER _ BYPASS)
MN temporarily blacklists *Vi* and broadcasts AP with IRB = ATTACKER _ BYPASS
Else: MN sets IRB to no punishment
End If
End If
End If

Algorithm 2 Accusation packet handling

Each CN *Vi* maintains its local blacklist table (BLT) and temporary blacklist (TBLT).
If CN *Vi* receives an AP for CN *Vj*.
If CN *Vi* has node *Vj* in its BLT or TBLT then ignore AP
Else: CN *Vi* checks IRB in AP.
If (*IRB* = = COMPLETE _ ISOLATION)
CN adds node *Vj* to its BLT and rebroadcasts AP.
CN isolates intruding node *Vj*
Else CN adds node *Vj* to its TBLT and rebroadcasts AP.
CN routes around intruder *Vj*
End If
End If
End If

Algorithm 3 Intrusion responding behavior

(1) Complete isolation
If node *Vi* receives packet from node *Vj*
If node *Vj* is in node *Vi* BLT ignore all packets and drop all packets queued from *Vj*
Else: handle and process packet
End If
End If
(2) Attacker bypass
If node *Vj* is in node *Vi* TBLT
If node *Vi* receives routing packet from node *Vj* Ignore and drop RREQ, RREP and RERR packets from *Vj*
End If
If node *Vi* receives data packet from node *Vj* destined for node *Vk*.
Node *Vi* forwards data packets towards node *Vk*
End If
Node *Vj* removes route entries including node *Vj* from its route table
Else: Handle and process packet
End If
End If

3 Simulating results and performance analyses

The performance of the proposed adaptive responding mechanism will be evaluated in various attack scenarios. The simulation environments are built based on GloMoSim V2.03 with the simulating parameters and configuration parameters shown in Tables 5 and 6, respectively.

Table 5 Simulation parameter

Parameter type	Parameter configuration
Number of nodes	25, 50, 100, 150, 200
Area size(m)	500×500, 707×707, 1 000×1 000, 1 225×1 225, 1 415×1 415
Node distribution	Uniform distribution
Routing protocol	AODV
Simulation duration(s)	2 000
Simulation traffic	Constant bit rate
MAC protocol	IEEE 802.11
Maximum speed(m/s)	20

Table 6 Configuration parameters

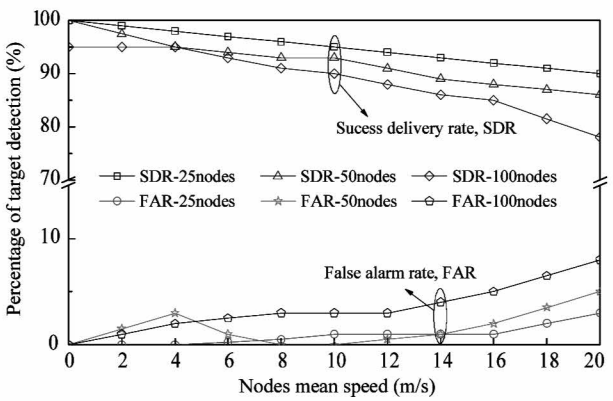
Parameter type	Parameter configuration
Time interval(TI)	100 s
Training period (*N*)	5TIs
Testing period	15TIs
Number of intruders	1, 2, 3, 4, 5
Chi-square test (α)	5% (95% confidence interval)

TSW	5TIs
Number of core parameters	PM:4, NCM:7
Intrusion responding behavior	Complete isolation, attacker bypass, no punishment
COA	Function of: *CI* and *Pc*
NPD	Function of: THA, PDR, RPO and RPD
COA&NPD level	4(L, M, H, H+)

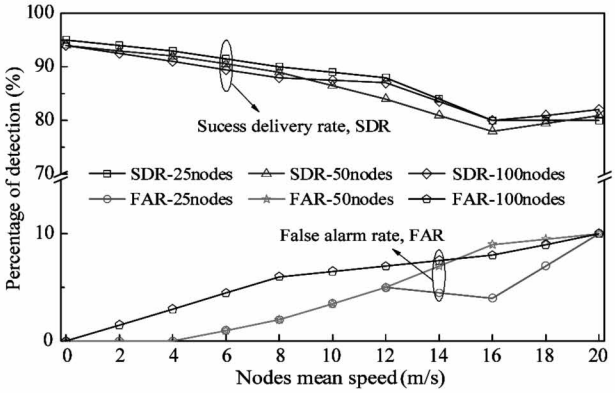
3.1 Evaluation of the attack identification

Various attack scenarios[19-22] are adopted to evaluate the successful delivery rate (SDR) and false alarm rate (FAR) for the proposed adaptive responding mechanism. SDR refers to the percentage of correctly detecting the intrusion and correctly identifying the type of attack and the number of intruder nodes. FAR refers to the percentage of the nodes with normal behavior being identified as the intruder by mistake.

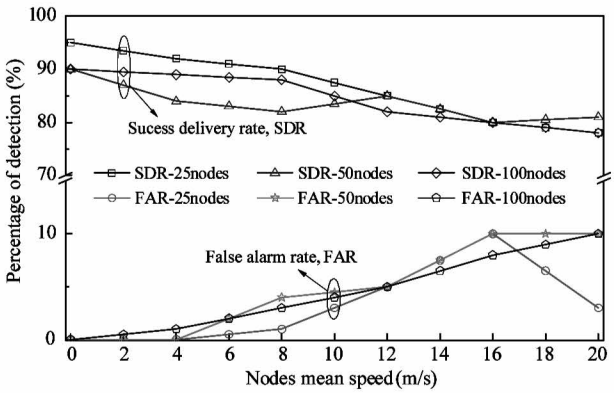
The typical attack types will be introduced to test the performance of the proposed adaptive responding mechanism. Simulations for each condition will be performed for 40 times. Simulating results of SDR and FAR at each tested mean speed under flooding attack, black hole and gray hole attack and rushing attack in different network scale are shown in Fig 5, where flooding attacks are formed by malicious RREQ broadcasting (i. e. denial of service attack) in Fig. 5(a), black hole and gray hole attacks are formed by forged RREP packets in Fig. 5(b), and rushing attacks are formed by forged RREQ packets in Fig. 5(c). As shown in Fig. 5, the detecting and adaptive responding mechanism shows high SDR and low FAR in all 3 attack scenarios. However, the performance of proposed mechanism is slightly degraded when the average tested node speed is higher than 12 m/s. This is because fast motion tends to increase the frequency of link failures, and the time required for route discovery increases.



(a) SDR and FAR under flooding attack



(b) SDR and FAR under black and gray hole



(c) SDR and FAR under rushing attack

Fig. 5 SDR and FAR under different attacks

3.2 Evaluations of the intrusion responding behavior

3.2.1 Evaluation under black hole attack

In this scenario, the performance of the proposed mechanism is evaluated by launching a black hole attack by a random intrusion node. Simulations in different network scales are performed for 20 times to obtain the statistical results. The simulation parameters, configuration parameters and COA mapping parameters shown in Table 5, Table 6, and Table 3 are adopted. The adaptive responding mechanism takes the decision table in Table 4 to select the intrusion responding behavior.

Fig. 6 shows proposed mechanism for selecting adaptive responding behavior (i. e., complete isolation, attacker bypass or no punishment) when resisting intrusions at different network sizes (25, 50, 100, 150, and 200 nodes). Simulating results show that the complete isolation is always selected to defense the black hole attack. For a large network (i. e. more than 100 nodes in the network), there is a (on average) 26% chance to choose the attacker bypass as the response by the proposed adaptive responding mechanism, on average 23% chance to choose to ignore the intrusion. For a small network (25 and 50 nodes),

there is about 90% chance for the mechanism to choose the complete isolation to respond to the intrusion, but the chance drops to 53% for the network with 100 nodes. This is because black hole attacks usually cause great damage to the network. Selecting complete isolation can minimize the negative impact on the network.

In addition, the same experiment is repeated by adjusting the NPD level settings and changing the way to launch black hole attacks in large networks to investigate the differences of selection of intrusion responding behavior in small and large networks. Fig. 7 shows the results of the improved NPD level settings. The selection of intrusion responding behavior is not much different between a small network and a large network in black hole attacks, and mainly responds to intruders by complete isolation. Inferred from Fig. 6 and Fig. 7, the intruder must adjust the way it initiates BH to produce the same side effects in a small network and a large network, in order to improve performance of large networks, so a protection mechanism must be employed.

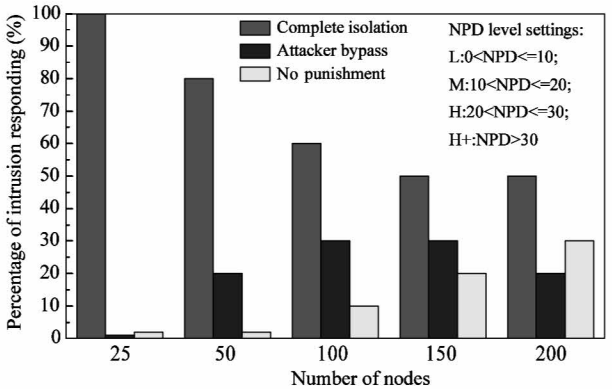


Fig. 6 Selection of intrusion responding behavior in black hole attack

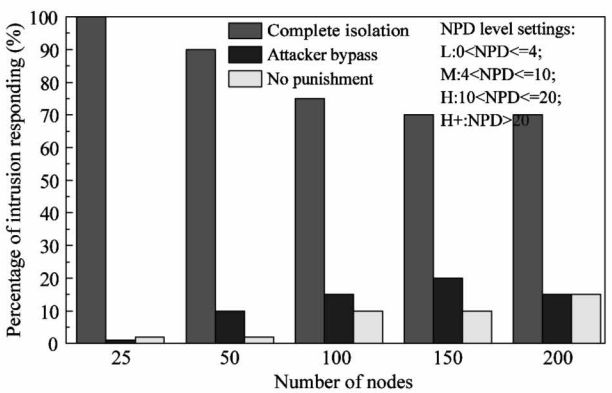


Fig. 7 Selection of intrusion responding behavior in black hole attack in improved NPD levels

3.2.2 Evaluation under flooding attack

In this scenario, the performance of the proposed mechanism is evaluated by launching a flooding attack. Experiment with the methods used in black hole attacks and the improved NPD level settings are shown in Fig. 8. There is a 78% chance to choose the complete isolation as the response by the proposed adaptive responding mechanism, on average 18% chance to choose the attacker bypass and 5% chance to choose to ignore the intrusion. Because flooding attack is a serious intrusion attack, which usually causes considerable damage to the network. It is reasonable for the proposed mechanism mostly to choose complete isolation to respond to the intrusion. In addition, it can be seen from Fig. 8 the proposed mechanism has good scalability for large networks.

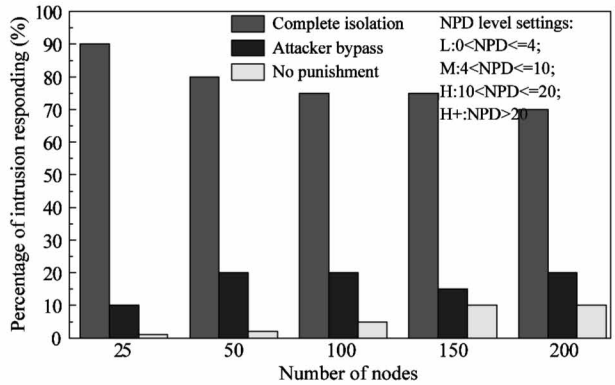


Fig. 8 Selection of intrusion responding behavior in flooding attack

3.2.3 Evaluation under rushing attack

Finally, the selection of adaptive responding behavior of proposed mechanism under rushing attack is evaluated. Fig. 9 shows that no punishment is chosen as the response by the proposed mechanism in most cases. And complete isolation or attacker bypass is chosen as the response by the proposed mechanism in a few cases. This result is basically independent of the network sizes. This is because a rushing attack is a minor attack, and the damage to the network performance is usually very small. If strict measures will be taken when the attack causes less damage to the network, this will lead to degradation of network performance. So the proposed mechanism ignores attacks in most cases to reduce the damage to the network. However, the proposed mechanism chooses complete isolation or attacker bypass to response intruders when rushing attacks greatly reduce network performance. Therefore, the proposed mechanism generally shows great flexibility and effectiveness.

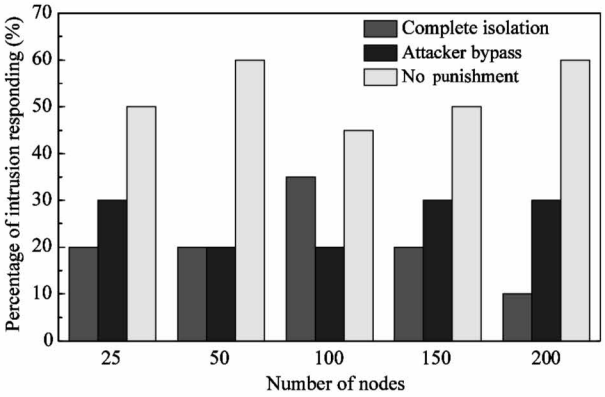


Fig. 9 Selection of intrusion responding behavior in rushing attack

3.3 Impact of adaptive responding mechanism on network performance

In this scenario, flooding attack, black hole attack, gray hole attack, rushing attack and combined attacks will be introduced to test the performance of the proposed adaptive responding mechanism, and NPD is used as a metric to analyze the effectiveness of the proposed mechanism. Simulations for a network of 25 nodes and 50 nodes will be performed for 30 times, respectively, and each responding mechanism is performed 10 times.

Fig. 10 and Fig. 11 show the effects of 3 responding mechanisms on NPD in a network of 25 nodes and 50 nodes, respectively. It can be seen that the proposed mechanism in both network sizes has the least negative impact on the (average) NPD when resisting intrusions. And the adaptive responding mechanism not only reduces the NPD in various serious attacks, but also significantly reduces the NPD when dealing with some minor attacks such as rushing attacks or gray hole attacks.

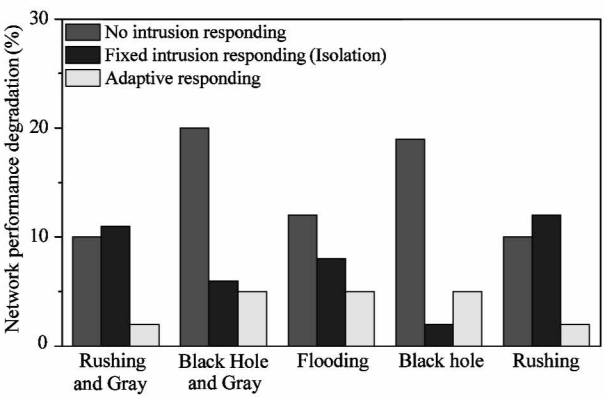


Fig. 10 Effectiveness of responding against various attacks in a 25-node network

3.4 Comparison

Now compare the proposed mechanism with cost-sensitive intrusion responding mechanism (CSIR) and generalized intrusion detecting and responding mechanism (GIDR). Fig. 10 and Fig. 11 show the comparison of the effects of the generalized intrusion detecting and responding mechanism (fixed intrusion responding (isolation) and the proposed mechanism (adaptive responding) on NPD. The results show that the fixed intrusion responding (isolation) reduces the NPD by between 2% and 12%. And the adaptive responding reduces the NPD by between 3% and 5%. It shows that the proposed mechanism is superior to that in the negative impact on network performance.

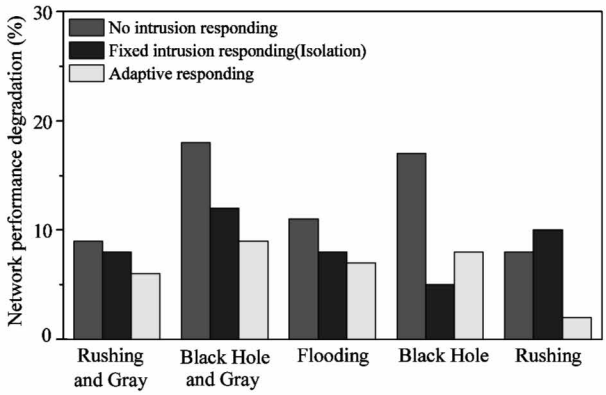


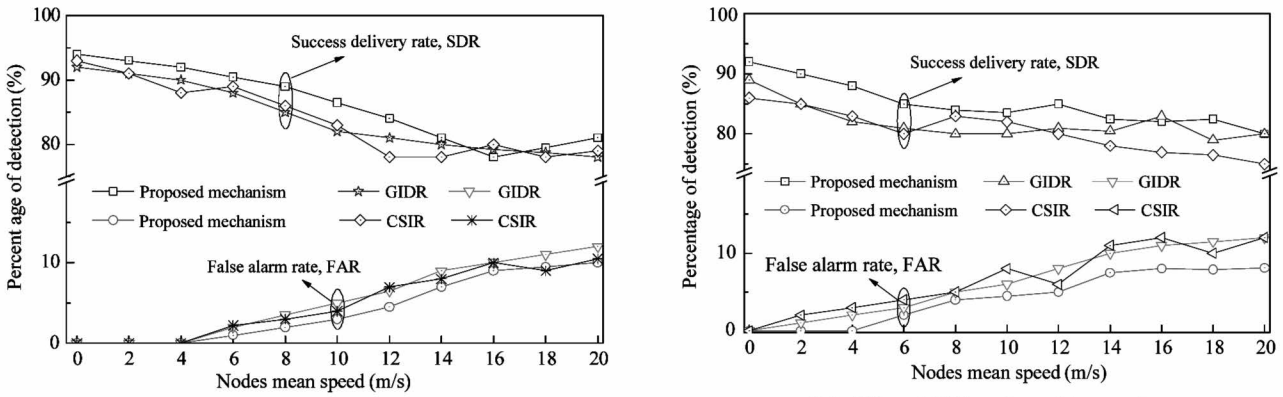
Fig. 11 Effectiveness of responding against various attacks in a 50-node network

Table 7 compares the responding selection criteria, responding behaviors, attack types, evaluation parameters, network performance impact, scalability, and network consumption of the proposed mechanism and cost-sensitive intrusion response mechanism. Both mechanisms have been implemented using GloMoSim. The comparison shows that the proposed mechanism is superior to the cost-sensitive intrusion responding mechanism in terms of network performance impact, network consumption and scalability.

In addition, the SDR and FAR of these 3 mechanisms are compared in the 50 nodes network in the black hole attack and rushing attack scenarios. As shown in Fig. 11, the 3 mechanisms can show good performance in a serious attack such as a black hole attack, because the attack is highly destructive and easy to detect. But the proposed mechanism for SDR and FAR is also superior to others. In the weak attack such asa rushing attack, the proposed mechanism has obvious advantages compared to the other two mechanisms. Not only SDR and FAR of the proposed mechanism are superior to the other two mechanisms, but also its performance is stable.

Table 7 Comparison of cost-sensitive models and the proposed responding mechanisms

Comparing parameter	Cost sensitive model	Adaptive protection mechanism
Intrusion responding selection criteria	TDI and ADI	COA and NPD
Intrusion responding behavior	Normal, recovered, complete isolation, temporary isolation, and relocation.	Complete isolation, attacker bypass, no punishment
Types of attacks considered	Authenticity, integrity and availability	Black hole, gray hole, flooding attacks, rushing attacks
Parameter for intrusion response impact assessment	PDR	NPD
Impact of intrusion response mechanism	Maximum PDR reduction = 13%	Maximum NPD = 7%
Scalability network overhead	Simulated up to 50 nodes Not considered	Simulated up to 200 nodes less than 5% of total network traffic



(a) SDR and FAR under black hole

(b) SDR and FAR under rushing attack

Fig. 12 Comparison of intrusion detection performance of 3 mechanisms

4 Conclusion

Aiming at the security requirements caused by the wide use of user information in current developing applications, an intrusion detecting and adaptive responding mechanism is proposed for mobile WSN. The mechanism first uses a test sliding window to improve the accuracy of intrusion detecting on the network, and then adoptes adaptive responding behavior lists and decision tables to select reasonable responding behavior to respond to intruders to protect the network.

The simulation results show that the proposed mechanism can achieve high SDR and low FAR in a series of attacks, and can choose reasonable responding behaviors in the face of different attacks. Compared with the other two mechanisms, the proposed mechanism has the least impact on network performance when resisting intrusion. In addition, the network overhead of the proposed mechanism is less than 5% of the total network traffic, having good performance. It can provide technical support for future network security. However, the proposed mechanism takes more time to identify and respond to intrusions for unknown attacks than known attacks. We will further improve the efficiency of dealing with unknown attacks in future research.

References

[1] Thiagarajan R, Moorthi M. Efficient routing protocols for mobile ad hoc network[C]//The 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 2017: 427-431

[2] Joseph J, Das A, Seet B, et al. CRADS: integrated cross layer approach for detecting routing attacks in MANETs [C]//IEEE Wireless Communication and Networking Conference (WCNC), Las Vegas, USA, 2008: 1525-1530

[3] Bu S R, Yu R F, Liu P, et al. Structural results for combined continuous user authentication and intrusion detection in high security mobile ad hoc networks[J]. *IEEE Transactions on Wireless Communications*, 2011, 10 (9): 3064-3073

[4] Bouhaddi M, Radjef M S, Adi K. An efficient intrusion detection in resource-constrained mobile ad-hoc networks [J]. *Computers and Security*, 2018, 76: 156-177

[5] Kalnoor G, Agarkhed J. Detection of intruder using KMP pattern matching technique in wireless sensor networks [J]. *Procedia Computer Science*, 2018, 125:187-193

[6] Liu J, Yu R F, Lung C, et al. Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks[J]. *IEEE Transac-*

tions on Wireless Communications, 2009, 8 (2):806-815

[7] Mitrokotsa A, Dimitrakakis C. Intrusion detection in MANET using classification algorithms: the effects of cost and model selection[J]. *Elsevier Journal of Ad Hoc Networks*, 2013,11 (1): 226-237

[8] Rao U H, Nayak U. Intrusion Detection and Prevention Systems[M]. The InfoSec Handbook New York: Apress, 2014

[9] Mohamed Y A, Abdullah A B. Implementation of IDS with response for securing MANETs[C]// IEEE International Symposium in Information Technology, Kuala Lumpur, Malaysia, 2010: 660-665

[10] Hasswa A, Zulkernine M, Hassanein H. Route guard: an intrusion detection and response system for mobile ad hoc network[C]// IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Montreal, Canada, 2005: 336-343

[11] Li H X, Wang G, Sun N, et al. Research on active network adaptive intrusion response system based on mobile agent[J]. *Computer Security*, 2009 (2): 49-52

[12] Vaseer G, Ghai G, Ghai D, et al. A neighbor trust-based mechanism to protect mobile networks[J]. *IEEE Potentials*, 2018, 38(1):20-25

[13] Gonzalez D O F, Hadjiantonis A M, Pavlou G, et al. Adaptable misbehaviour detection and isolation in wireless ad hoc networks using policies[C]// IFIP/IEEE International Symposium on Integrated Network Management, Long Island, USA, 2009: 242-250

[14] Oussama S, Mohamed E. Classification of mobile ad hoc networks attacks[C]// IEEE 5th International Congress on Information Science and Technology, Marrakech, Morocco, 2018: 618-624

[15] Nadeem A, Howarth M. Protection of MANETs from a range of attacks using an intrusion detection and prevention system[J]. *Telecommunications Systems Journal Springer*, 2013,52 (4): 2047-2058

[16] Wang S, Tseng C H, Levitt K, et al. Cost-sensitive intrusion response for mobile ad hoc networks[C]// The 10th International Conference on Recent Advances in Intrusion Detection, Berlin, Germany, 2007: 127-145

[17] Zhang Y, Liu W, Lio W, et al. Securing mobile ad hoc networks with certificateless public keys[J]. *IEEE Transactions on Dependable and Secure Computing*, 2006, 3 (4):386-399

[18] Tang J F. Research on energy-based AODV two-path routing algorithm in ad hoc network[J]. *Information and Communication*, 2012 (3): 5-6

[19] Hu Y, Perrig A, Johnson B. Rushing attack and defense in wireless ad hoc networks routing protocols[C]// The 2nd ACM Workshop on Wireless Security, New York, USA, 2003: 30-40

[20] Kurosawa S, Jamalipour A. Detecting black hole attacks on AODV based mobile ad hoc networks by dynamic learning method[J]. *International Journal of Network Security*, 2007, 5(3):338-346

[21] Sachan K, Lokhande M. An approach to detect gray-hole attacks on mobile ad-hoc networks[C]// International Conference on ICT in Business Industry and Government (ICTBIG), Indore, India, 2016: 1-5

[22] Yi P, Dai Z, Zhang S. Resisting flooding attack in ad hoc networks[C]// IEEE International Conference on Information Technology Coding and Computing (ITCC), Las Vegas, USA, 2005: 657-662

Zhao Min, born in 1995. She received her B. S. degree in communication engineering from Heilongjiang University in 2018. Currently, she studys at the Department of Communication Engineering of Heilongjiang University, Harbin, P. R. China. Her researches include indoor vision positioning and crowd source sensing.