Research Article

A Novel Method Defends against the Path-Based DoS for Wireless Sensor Network

Dong Chen, 1 Zhenjiang Zhang, 1 Fan-Hsun Tseng, 2 Han-Chieh Chao, 3,4 and Li-Der Chou 2

1 School of Electronic and Information Engineering, Key Laboratory of Communication and Information Systems, Beijing Municipal Commission of Education, Beijing Jiaotong University, Beijing 100044, China
2 Department of Computer Science and Information Engineering, National Central University, Taoyuan 32001, Taiwan
3 Department of Computer Science and Information Engineering, National Ilan University, I-Lan 26047, Taiwan
4 Department of Electrical Engineering, National Dong Hwa University, Hualien 97401, Taiwan

Correspondence should be addressed to Zhenjiang Zhang; zhjzhang1@bjtu.edu.cn

Received 31 March 2014; Accepted 23 June 2014; Published 8 July 2014

Academic Editor: Jianwei Niu

Copyright © 2014 Dong Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

WSNs are significantly different from the traditional network architecture due to its wireless communication, energy limitation, and computation constraint and environment of the application. Because of these differences, security becomes a critical issue. The path-based denial of service (PDoS) attacks harm the network maintenance and cause serious damage in the resource constrained WSNs. In a PDoS attack, an adversary can overwhelm sensor node and cluster head node to flood packets along the routing path so that intermediate node must keep active mode and exhaust the energy. In this paper, we creatively propose a novel method, which is operated at the base station to detect the malicious behavior. The proposed method is combined with triple exponential smoothing and Markov chain, so that it makes the detection results more accurate. Meanwhile, we first use the concept of black hole to defend the PDoS attack in WSNs. Simulation results are provided to evaluate the performance and illustrate the contribution of this mechanism.

1. Introduction

Wireless sensor networks (WSNs) are generally covered by hundreds of sensor nodes with computation, sensing, and wireless communication modes. And the applications of the WSNs are usually environment monitoring, home-care surveillance, habitat monitoring, military surveillance, and so forth. The sensor nodes are not only low power electronic devices but also deployed in remote areas where power resources are limited. Besides, they are subject to open wireless communication. Since the resources of the sensor nodes are severely constrained and may be deployed in an unattended or even hostile environment, WSNs can be easily attacked by denial-of-service (DoS) attacks, which cause information loss along with large energy expenditure [1]. In DoS attack, an adversary may compromise a sensor node to access all data stored on the node and perform insider attacks [2].

Different types of DoS attacks in different layers have been discussed in [3], and some countermeasures to defend against them are proposed. But in the numerous DoS attack, there is a special form of attack called the path-based DoS (PDoS). The PDoS was first pointed out by Deng et al. [4] in 2005. They described that a PDoS attack begins with the sensor nodes and cluster heads (CHs), compromised of an adversary that floods numerous packets through multihop communication to base station or sink node along the established routing path. As a result, the intermediate nodes in the routing path have to keep active mode and forward the packets so that they cannot return to sleep mode normally. Generally speaking, the PDoS targets the intermediate nodes within the routing path to exhaust their energy. Figure 1 has shown how the PDoS launches the attack.

In this paper, we propose a novel method, which combines triple exponential smoothing and Markov chain for detecting the attack behavior. This method is completely different from other detecting algorithms. The proposed method is operated on the base station or sink node rather than in the intermediate nodes, because they have more power and energy. It brings great benefit in conserving
energy of the intermediate nodes. Meanwhile, inspired by the concept of black hole, we propose the one-hop black holes mechanism to defend the attack packets sent by the compromised CH. In our mechanism, we put the one-hop intermediate nodes away from the attack CH as the black holes, which attract the malicious packets and drop them. Moreover, the one-hop black hole nodes do not receive the normal data packets.

The rest of the paper is organized as follows. First, we discuss some previous schemes and indicate their problems in Section 2. Section 3 presents the adversary model and network model in the proposed framework. In Section 4, we show the details of our attack behavior detection algorithm. Section 5 illustrates how the mechanism of one-hop black holes defends the PDoS attack. The simulation results are shown in Section 6. Finally, we conclude the paper and give the future works.

2. Related Work

In order to defend against a PDoS attack, the intermediate nodes should be able to detect the malicious packets and then reject them. Deng et al. pointed out that two ways generally are adopted. One is to have the source node establish a separate shared key with other sensor nodes in the routing path. The other is rate control, which limits the number of packets an intermediate node can forward per second. But the highly restricted packet size and nodes at different locations need to forward different numbers of packets per second making these two ways hard to directly defend the PDoS attack. However, several schemes have been proposed to defend the PDoS attack, which are also based on these two ways.

Deng et al. [4] proposed a lightweight secure mechanism, which uses one-way hash chain to defend against PDoS attacks on intermediate nodes in a multihop end-to-end data path in WSNs. Perrig et al. [5] proposed a loosely time synchronous mechanism called the timed efficient stream loss-tolerant authentication (TESLA) broadcast authentication protocol, and it copes with the denial-of-service attacks. However, the time asynchronous problem causes the sensor node to be unverifiable whether the messages are valid or not before the trusted party releases the trapdoor key.

The en-route filtering schemes are widely proposed for intermediate nodes filtering the false data, which are generated by malicious aggregator nodes. Besides, they detect intruders engaged in what we have termed PDoS attacks. The basic idea is that the intermediate nodes share some keys with their member nodes in a node group or cluster. Member nodes generate MACs for reporting data by using the shared keys, and intermediate nodes verify the MACs before forwarding packets [6]. The bloom filter of the statistical en-route filtering (SEF) scheme was proposed by Ye et al. [7] and it is used to reduce the MACs size and ensure their security. Kraub et al. [8] proposed a secure ticket-based en-route filtering (STEF) scheme to protect the data-report. In the data-report, a certain commitment is added through this scheme and the commitment is created by the hash function such as SHA-256. Therefore, the data-report cannot be modified and forged by an attacker. Their proposed scheme defended against an adversary to inject false data into the sensor network.

Cheng et al. [9] proposed an efficient QoS-aware GOR (EQGOR) algorithm. To some extent, this algorithm can resist DoS attack and has a very low time complexity, which is specifically tailored for the resource limitation of sensor devices. But this mechanism is designed for the QoS provisioning in WSNs, and, in some respect, it does not meet the requirements of completely defending the DoS attack.

Li and Batten [10] proposed a solution that uses mobile agents to detect PDoS attacks easily. But this method is just suitable for the small scale WSNs. Ghosal et al. [11] proposed a dynamic TDMA based scheme, which can defend the PDoS attacks. However, it is not designed for the PDoS attack; the performance may be dissatisfactory.

Hence, most previous schemes need intermediate nodes to verify the truthfulness of each data that they received and decide to forward or drop. This wastes the energy consumption of the intermediate nodes. Moreover, the cluster
heads have to increase the bits in packet for verification, and this extra overhead also consumes the energy of intermediate nodes when the packets are forwarded. Compared with the previous papers, our mechanism is a novel solution to defend the PDoS and achieves the energy conservation for the intermediate nodes, and hence the network lifetime becomes longer.

3. Assumptions

3.1. Network Model. We focus on two-level distributed heterogeneous sensor network, in which the capacity of computation and energy of cluster head is higher than the sensor nodes. The CHs act as aggregator nodes and are compromised by the adversary. We call the nodes that just forward the packet as intermediate nodes or en-route nodes. Normally, the base station (BS) or base station has no limit on energy and the computation ability is much larger than other sensor nodes. Also, the BS or the sink knows the structure of nodes deployment; the base station knows all neighbor nodes of each other. But, it does not mean that the sink node has known the topology of the network.

3.2. Adversary Model. The adversary controls the compromised nodes and accesses all the secret data to perform insider attacks. The compromised CH floods numerous replayed and false data. Herein, we mainly consider a single point of attack which is able to damage the network for the CHs have more energy. If the adversary is mobile, the resilience scheme can defend the malicious attack.

4. Attack Behavior Detection Algorithm

Without loss of generality, the base station has better capability on energy and computation. Due to the reduced energy of the intermediate nodes, we adopt the base station to validate that the network has been attacked by PDoS or not.

But in this way there are two challenges that we have to overcome: (1) how to effectively and accurately judge that the network is attacked; (2) how to validate the PDoS attack as quickly as possible, so that the network can be resolved quickly and reduces the energy consumption. In this section, we adopt triple exponential smoothing of the time series forecasting and the Markov model based on the nodes energy to solve these problems [12, 13]. Two evaluation factors are considered, the number of the packets and the energy state of the node. Therefore, we can greatly improve the accuracy of the detection and prediction.

4.1. Prediction of the Packets Number with Triple Exponential Smoothing. Due to the located special environment and the characteristics of WSNs, the number of transmitted packets in the network fluctuates over time. For that reason, we choose triple exponential smoothing, which is more suitable for processing time sequence in quadratic curve shape, and forecasting and verifying the attacks. Packets number received by base station in each phase has been shown in Table 1.

| Phase (60 sec) | Node IP | Phase (60 sec) | Node IP |
|---------------|---------|---------------|---------|
| Phase 1       | IP1     | Phase 2       | IP2     |
| Phase 3       | IP3     | Phase 4       | IP4     |

Firstly, the base station will calculate the number of packets that is received from different node in each phase (60 sec) and then take the triple exponential smoothing method to forecast and verify.

Because the triple exponential smoothing values are the third time exponential smoothing based on the quadratic exponential smoothing values, so we need to calculate the first exponential smoothing value and then the secondary exponential smoothing values.

The formula of once and twice exponential smoothing are shown as follows:

\[ S^{(1)}_t = \alpha Y_t + (1-\alpha) S^{(1)}_{t-1}, \]
\[ S^{(2)}_t = \alpha S^{(1)}_t + (1-\alpha) S^{(2)}_{t-1}. \]

Then, according to the following, we continue to get the third exponential smoothing value:

\[ S^{(3)}_t = \alpha S^{(2)}_t + (1-\alpha) S^{(3)}_{t-1}. \]

The \( Y_t \) represents the actual value of the packet number. The \( S^{(1)}_{t-1} \) is the first smoothing value of phase \( t - 1 \) \((t > 0)\); the \( S^{(2)}_{t-1} \) and \( S^{(3)}_{t-1} \) are the twice and third smoothing values of phase \( t - 1 \). The \( S^{(1)}_t \) is the first smoothing value of phase \( t \), namely, the forecast value of the phase \( t + 1 \); the \( S^{(2)}_t \) and \( S^{(3)}_t \) are the twice and third smoothing values of phase \( t \). The \( \alpha \) and \( 1-\alpha \) are weighting factors.

In particular, because the attack happens at any time, we will increase the value of \( \alpha \) to improve the weight of recent data and relatively reduce the value of \( 1-\alpha \) to decrease the weights of the forward data.

The prediction of the packet numbers of any target phase is \( Y_{t+m} \); its mathematical model of triple exponential smoothing is

\[ Y_{t+m} = a_t + b_t m + c_t m^2. \]

The variable \( m \) is the forecast period; namely, the prediction of phase \( t + m \) is what you want. The coefficients \( a_t, b_t, c_t \),
and $c_i$ are all smoothing factors, and they are formulated as follows:

$$a_i = 3S_{t}^{(1)} - 3S_{t}^{(2)} + 3S_{t}^{(3)},$$

$$b_i = \frac{\alpha}{2(1-\alpha)^2} \left[ (6-5\alpha)S_{t}^{(1)} - 2(5-4\alpha)S_{t}^{(2)} + (4-3\alpha)S_{t}^{(3)} \right],$$

$$c_i = \frac{\alpha}{2(1-\alpha)^2} \left[ S_{t}^{(1)} - 2S_{t}^{(2)} + S_{t}^{(3)} \right].$$

Then, we can get the forecasting value of the phase $t + m$, by using the above formulas, which means the number of received packets from the same node in phase $t + m$ at base station.

The main characteristic of the PDoS attack is continuously sending large number of packets into the network, wasting the energy and power of immediate nodes. In a fixed time period, the number of attack packets is much greater than the normal packets. According to the experiment results and practical experience, we set an upper bound threshold $\theta$, which means that the number of packets sent by the same normal node cannot be larger than $\theta$. Therefore, the value of $\theta$ can be set freely according to the actual situation in the experiment environment.

Firstly, we acquire the forecasting values of phase $t + 1, t + 2, \ldots, t + m$. The value of $m$ can be set flexibly. Then, compare each forecasting value with the threshold $\theta$. If all of them are larger than $\theta$, it implies that the network has been attacked with the abnormal packets. However, this method cannot represent the attack launched by PDoS. Because there are many reasons causing the packet to attack. For example, the intermediate nodes repeatedly forward the same packet when the hardware failure or the ACK packets are not received.

In order to solve this problem and judge the PDoS attack accurately, we further monitor the residual energy of nodes which is based on the residual energy consumption value. The energy consumption of nodes is built by the Markov model; it further determines whether the network is attacked by PDoS.

4.2. Prediction Model of the Node Status Based on Markov Chain. By monitoring the nodes energy consumption in each phase, we mark the status of nodes in different time. Therefore, we can get the transfer probability of different status. Based on the transfer probability, we recall a Markov chain model to predict the node energy status in next phase.

First of all, we need to declare some basic conditions.

1. In each phase, the working time of each node is $T$, and in this paper $T = 60$ sec.

2. If the energy of node is consumed too much in the unit interval $\Delta T$ ($\Delta T = 1$ sec herein), the node state is regarded as abnormal at this moment and vice versa. If the data collection and forwarding is regular, the energy consumption in unit interval must be lower.

3. Without loss of generality, the energy consumption of each node is from high to low.

The energy of each node is divided into five levels, such as 100%, 75%, 50%, 25%, and 0%. Note that the percentage of energy is based on the residual energy of nodes. The monitor time is $\Delta T$; it means the node monitors the energy information every $\Delta T = 1$ sec. If the transfer hop of different energy status is larger than one, we regard this node as abnormal. For example, node A detects that the energy is 100% at $\Delta T_1$, and the energy is 50%, 25%, or 0 at $\Delta T_2$; we recognize node A as abnormal node.

In order to display the individual state of the Markov chain intuitively, we use characters “1,” “2,” “3,” “4,” and “5” to represent the 100%, 75%, 50%, 25%, and 0, respectively.

After that, we acquire the Markov state transition diagram as Figure 2.

Also, we derive the state-transition matrix from the transition diagram as follows:

$$\begin{pmatrix}
    p_{11} & p_{12} & p_{13} & p_{14} & p_{15} \\
    p_{21} & p_{22} & p_{23} & p_{24} & p_{25} \\
    p_{31} & p_{32} & p_{33} & p_{34} & p_{35} \\
    p_{41} & p_{42} & p_{43} & p_{44} & p_{45} \\
    p_{51} & p_{52} & p_{53} & p_{54} & p_{55}
\end{pmatrix}.$$  

In the following content, we use an example to elaborate and illustrate how to forecast the energy state of the node.

In the phase $i$, base station detects the energy information of each node per one second and records the state as normal or abnormal. Therefore, there are 60 states, which are 25 normal states and 35 abnormal states.

1. The number of state transitions from normal state to normal state is 11;
2. The number of state transitions from normal state to abnormal state is 15;
3. The number of state transitions from abnormal state to normal states is 12;
4. The number of state transitions from abnormal state to abnormal is 21.
Then, we make the “character 1” to present the normal state, and “character 2” presents the abnormal state. Hence, we can conclude the state as follows:

\[
p_{11} = \frac{11}{26}; \quad p_{12} = \frac{15}{26}; \quad p_{21} = \frac{12}{33}; \quad p_{22} = \frac{21}{33}.
\] (6)

The state transition matrix of the Markov chain is

\[
p = \begin{pmatrix}
p_{11} & p_{12} \\
p_{21} & p_{22}
\end{pmatrix} = \begin{pmatrix}0.423 & 0.577 \\0.364 & 0.636\end{pmatrix}.
\] (7)

From the matrix of \( p \), we find that \( p_{12} > p_{11} \), which means the energy state of the node is normal at phase \( i \). But the probability that the energy state is abnormal at phase \( i + 1 \) is larger than normal and \( p_{22} > p_{21} \) which means that the energy state of the node is abnormal at phase \( i \), but the probability that the energy state is also abnormal at phase \( i + 1 \) is larger than normal. Accordingly, we summarize that no matter what the energy state of the node is in the current phase, the probability of the energy state is abnormal and is larger than normal in the next phase. And we can judge that this node could be malicious.

Combining these two methods described above, we are able to judge exactly whether the network has been attacked by PDoS. Firstly, the base station adopts the method of triple exponential smoothing to forecast the number of the packets at phases \( i + 1, i + 2, \ldots, i + m \), which are sent by the same node and then compares these forecasted values with the threshold \( \theta \). If all values are larger than \( \theta \), we believe that the network has been attacked by abnormal packets, but maybe not the PDoS attack. Third, base station uses the method of prediction model about the node energy status based on Markov chain. If the energy state of the node in the next phase is abnormal, we may believe the node is malicious. At last, the judgment results are obtained. Only these two conditions are recognized as attacked by PDoS attack, the energy state of the node in next phase is abnormal, and the forecasting values of the packets which are larger than \( \theta \) are conformed at the same time.

The flow diagram of attack behavior detection algorithm is shown in Figure 3.

5. One-Hop Black Holes Mechanism

By using the attack behavior detection algorithm that has been described above in detail, it would be easy to detect whether the network has been attacked and locate where the adversary launched an attack accurately. However, just detecting attack behavior is not our ultimate goal because the network is still vulnerable to the PDoS attack. In addition, we are committed to propose an efficient mechanism, which is called one-hop black hole mechanism to defend the PDoS attack and make the attacked network return to normal. The details of this mechanism are described below.

Once the base station or base station detects that the network has been attacked, it also knows the IP address or other information that can uniquely identify the attack node (in this paper, CH is the attack node) through the proposed attack behavior detection algorithm. Then, it is easy to know the location of the adversary and the IP addresses that are one hop away from the adversary node for the base station knows the structure of the network in advance. With this information in hand, the base station will broadcast some specific packets that contain the corresponding IP addresses to the specific intermediate nodes. We call these special packets control packets. And these specific intermediate nodes are the nodes that are one hop away from the compromised CH. The purpose of the control packet is to turn the one-hop nodes around the compromised CH into the black holes. In other words, the control packets will transform these one-hop intermediate nodes into one-hop black holes. Using the only receiving/not forwarding character of black hole, the one-hop black holes will just receive the attacking packets sent by the compromised CH and then drop them without forwarding. At the same time, they will not receive the normal packets. Then, the attack packets cannot be flooded into the network, and the network successfully defends the PDoS attack. Figure 4 shows how the one-hop black holes defend the PDoS attack.

5.1. AODV Protocol. In order to verify and prove our scheme, we select the well-known AODV protocol as the routing protocol.

AODV is an on demand routing protocol and is capable of both unicast and multicast routing. It establishes routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the source nodes. Additionally, the AODV protocol forms tree structure which connects multicast group members. The trees are composed of the group members, and the nodes need to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and large scales of member nodes.

The routing table of AODV protocol is composed of the following fields:

1. destination IP address;
2. destination sequence number;
3. destination only flag;
4. next hop IP address;
5. hop count;
6. precursor list;
7. lifetime;
8. network layer interface;
9. other state and routing flags.

There are three main message types in the AODV protocol, which are route requests (RREQs), route replies (RREPs), and route errors (RERRs). Herein, we mainly introduced the RERR packets, because the following control packet is designed and modified by the RERR packets. The format of the RERR message is depicted in Table 2 and contains the following fields:

| Type | Description |
|------|-------------|
| 3    | N: no delete flag; set when a node has performed a local repair of a link, and upstream nodes should not delete the route; |
Reserved: set as 0; ignored on reception;
DestCount: the number of unreachable destinations included in the message and must be at least 1;
Unreachable destination IP address: the IP address of the destination became the unreachable address due to break link;

However, the AODV protocol is designed for applying in the ad hoc network; it is not completely suitable for the
Table 2: The format of RRER packets.

| 8 bits | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 bits | Type | N | Reserved | DestCount |
|--------|---|---|---|---|---|---|---|---|--------|------|---|-----------|-----------|
|        |   |   |   |   |   |   |   |   |        |      |  |           |           |
|        | Unreachable destination IP address (1) |               |               |           |       |
|        | Unreachable destination sequence number (1) |               |               |           |       |
|        | Additional unreachable destination IP addresses (if needed) |               |               |           |       |
|        | Additional unreachable destination sequence numbers (if needed) |               |               |           |       |

| 8 bits | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 bits | Type | N | Reserved | DestCount |
|--------|---|---|---|---|---|---|---|---|--------|------|---|-----------|-----------|
|        |   |   |   |   |   |   |   |   |        |      |  |           |           |
|        | Unreachable destination IP address (1) |               |               |           |       |
|        | Unreachable destination sequence number (1) |               |               |           |       |
|        | Additional unreachable destination IP addresses (if needed) |               |               |           |       |
|        | Additional unreachable destination sequence numbers (if needed) |               |               |           |       |

Sink node or base station

Figure 4: One-hop black holes mechanism.

path-based and hierarchical WSNs. For this reason, we modified the AODV protocol to make it applicable. According to the characters of the AODV, the control packet and the routing table are also revised and redesigned.

We design the control packet based on the RRER packet, and the format is shown in Table 3.

The meaning of each field is described as follows:

Type: 5;
A: acknowledgment required;
Reserved: set as 0;

V: void; it means the entry that unreachable IP address which is the destination IP address of the routing table belongs to void or invalid during the life time;
Life time: it means the length of invalid time; if the time goes out, the entry will return valid state from invalid;
Unreachable IP address: the address of base station or BS;
Black hole node IP address: the destination of the control packet;
Black hole node sequence number: the sequence number in the route table entry for the destination listed in the previous unreachable destination IP address field.

The base station will first broadcast the control packet. The nodes that received the control packet will verify the destination or not by themselves. The verification is checked through the black hole node IP address field of the control packet. If the IP address is not from black hole node, they will forward it again. When the one-hop nodes of the compromised CH receive the packet, they will send an acknowledgement message to the base station first. It is checked according to the field of A in control packet. Then, the routing table is updated. On the other hand, one-hop node/nodes of the compromised CH will locate the entry/entries that the unreachable IP address is set to the destination IP address of the routing table. After that, the other state and routing flags field of the entry/entries is/are set with V, to make the entry/entries void or invalid. This step ensures that the one-hop nodes of the compromised CH become the black holes. Then, the attack packets will be received and dropped by black hole nodes and cannot be flooded into the network.

Additionally, the time length that the entry is invalid can be set in the life time field based on the control packet. If time is out, the entry returns valid from the invalid state. This reflects the resilience of our scheme. When the attack has stopped or the compromised CH has exhausted the energy before the black holes, the black hole nodes can return to normal intermediate nodes and forward the normal packets with this scheme.

5.2. Modification of the SMAC Protocol. However, there is an important challenge that we should solve. If the network has been attacked in a period of time, which means the attacking
Table 3: The packet format of the designed control packet.

| 8 bits | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 7 bits |
|--------|---|---|---|---|---|---|---|---|---|-------|
| Type   | A | Reserved | V | Life time |
|        |    | Black hole node IP Address (1) |    |
|        |    | Black hole node IP Address (2) |    |
|        |    | . . . |    |
|        |    | Unreachable IP address |    |

For sync
For RTS
For CTS

Receiver
Listen period
Send data

FIGURE 5: The frame structure of the SMAC.

Sender

Timeout: $T$

Receive period
Sleep period

Receiver

FIGURE 6: The revised structure of the SMAC.

path has been established. The control packet cannot be received by the black hole nodes since they are busy with forwarding the attacking packet. In order to handle this problem, we make a little modification on the SMAC protocol. SMAC mechanism allows nodes to sleep periodically after a certain time of listening for reducing energy consumption.

Figure 5 describes the frame structure of the SMAC protocol. If the attacking path has been established, the SMAC needs to continue the receiving state and receives the attacking packets. Here, we add a timer in the SMAC, setting a threshold $T$ for receiving state. As illustrated in Figure 6, the receiving state will be forced into sleep state if timeout. The value of $T$ can be set initially and adjusted through the practical application. It would be specially mentioned that there is no a unique optimized value of $T$. According to the observation of our simulation, while the sending rate of the attack packet is different, the value of $T$ should be set different values to defend the attack with the shortest time. Then, the control packet may defeat the attacking packets when they compete with each other for the media at the new frame. Besides, the control packet can be successfully received by the one-hop nodes of the compromised. As the mentioned before, these nodes are able to become the black holes and defend the PDoS attack.

Table 4: Simulation parameters.

| Simulation parameter          | Value      |
|-------------------------------|------------|
| Node number                   | 50         |
| Base station number           | 1          |
| Compromised CH number         | 1          |
| Initial power                 | 20 (J)     |
| Packet size                   | 1000 (bit) |
| Normal packets average rate   | 0.1 (Mb/s) |
| Abnormal average packets rate | 0.5 (Mb/s) |
| Threshold $\theta$            | 15000 (packets) |
| $m$                           | 2          |

Figure 7: The remained energy with varying time.

6. Simulation

The simulation is conducted on NS2 simulator, and the used parameters are shown in Table 4.

We experiment a scenario to simulate the energy consumption of intermediate nodes. Figure 7 shows that the network was attacked at 4 minutes, and the base station detects that the number of packets was larger than 15000 in the next few minutes. Then, the control packet was sent to the one-hop nodes which are one hop away from the malicious nodes, and, after a short period of time, our scheme begin to defend the PDoS. Therefore, the energy conservation of the proposed scheme is higher than the result without scheme.
7. Conclusion and Future Work

In this paper, we propose a novel solution to defend the PDoS attack. We put forward an attack behavior detection algorithm using triple exponential smoothing and Markov chain. In particular, this algorithm is operated at the base station, which makes the minimum energy consumption of the intermediate nodes. Therefore, they do not need to detect every packet for verifying they are normal or abnormal. And two evaluation factors are considered, the number of the packets and the energy state of the node. These two factors are guaranteed to achieve the accuracy detection. Meanwhile, in order to completely defend the PDoS attack, we propose one-hop black holes mechanism, which makes the intermediate nodes that are one hop away around the malicious CH as the black holes. These nodes can just receive the attacked packets which are sent by malicious nodes and drop them. In addition, we design the recovery scheme for the one-hop black hole nodes to make the whole mechanism more flexible. In the future, we want to apply this mechanism to various and different network protocols and improve it for the better energy-efficient based on the existing basis.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research is supported by the National Natural Science Foundation under Grant no. 61371071, Beijing Natural Science Foundation under Grant no. 4132057, Beijing Science and Technology Program under Grant no. Z121100007612003, and Academic Discipline and Postgraduate Education Project of Beijing Municipal Commission of Education.

References

[1] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.
[2] C. Krauß, M. Schneider, and C. Eckert, "On handling insider attacks in wireless sensor networks," Information Security Technical Report, vol. 13, no. 3, pp. 165–172, 2008.
[3] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, 2002.
[4] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks," in Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 89–96, Alexandria, Va, USA, November 2005.
[5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: security protocols for sensor networks,” Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.
[6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in Proceedings of the IEEE Symposium on Security and Privacy, pp. 259–271, Berkeley, Calif, USA, May 2004.
[7] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839–850, 2005.

[8] C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, “STEF: a secure ticket-based en-route filtering scheme for wireless sensor networks,” in *Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES ’07)*, pp. 310–317, Vienna, Austria, April 2007.

[9] L. Cheng, J. Niu, J. Cao et al., “QoS aware geographic opportunistic routing in wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1864–1875, 2013.

[10] B. Li and L. Batten, “Using mobile agents to detect node compromise in path-based DoS attacks on wireless sensor networks,” in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM ’07)*, pp. 2507–2510, Shanghai, China, September 2007.

[11] A. Ghosal, S. Halder, and S. DasBit, “A dynamic TDMA based scheme for securing query processing in WSN,” *Wireless Networks*, vol. 18, no. 2, pp. 165–184, 2012.

[12] E. S. Gardner, “Exponential smoothing: the state of the art,” *Journal of Forecasting*, vol. 4, no. 1, pp. 1–28, 1985.

[13] R. A. Mini, B. Nath, and A. A. Loureiro, “A probabilistic approach to predict the energy consumption in wireless sensor networks,” in *4th Workshop de Comunicação sem Fio e Computação Móvel*, pp. 23–25, 2002.