An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Networks

Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang
Chaoyang University of Technology, Taichung, Taiwan, R.O.C.
{crching, s9733901, yfahuang}@cyut.edu.tw

***ABSTRACT*—A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor environmental conditions, such as battlefield data and personal health information, and some environment limited resources. To avoid malicious damage is important while information is transmitted in wireless network. Thus, Wireless Intrusion Detection Systems are crucial to safe operation in wireless sensor networks. Wireless networks are subject to very different types of attacks compare to wired networks. In this paper, we propose an isolation table to detect intrusion by hierarchical wireless sensor networks and to estimate the effect of intrusion detection. The primary experiment proves that isolation table intrusion detection can prevent attacks effectively.**

***Index Terms*—Wireless Sensor Networks, Intrusion Detection, Anomaly Detection, Attack Behaviors, Countermeasures**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) is a novel technology involving the deployment of hundreds of low-cost, micro-hardware, and resource-limited sensor nodes. It uses sensor nodes to sense important information. The applications of WSNs include military sensing, disaster response, health care, and intelligent house control [3]; can be configured to suit a wide variety of personal requirements. Once sensor nodes are deployed, they are self-organized and establish routes automatically. Information concerning surroundings is transmitted to a Base Station (BS). A WSN is typically deployed in an uncontrolled or unreachable environment. Each sensor node carries a limited, generally irreplaceable energy source. Therefore, energy conservation is the most important performance consideration for extending network lifetime.

As a result of reduced energy consumption, extended network coverage, and increased lifetime, Heinzelman et al. proposed a cluster-based, hierarchical WSN (CWSN) [9][16]. In a given period of time, CWSN will pick out a set of cluster heads (CHs). The CHs becomes the center of a cluster, while the other sensor nodes in this cluster are the member nodes. The member nodes (MNs) deliver sensed data to the BS through their cluster head. The data from member nodes is aggregated to high-level information by CHs for energy conservation. We use this architecture to construct an intrusion detection system.

WSN is usually deployed in security-sensitive environments, such as the battlefield. A CH is responsible for the aggregation of sensed data from its member nodes. The CH is the focal component of the intruder; hence it requires higher security in CWSN. The security requirements of CHs are different from those of MNs. Intruders use MNs to attack CHs. It is important to prevent malicious damage in WSNs. Research regarding intrusion detection systems (IDS) thus becomes one of the most important issues in WSNs. Most research regarding IDS concerns the accuracy of sensed data, malicious sensor nodes, authentication methods, etc. [6][8][12][18].

The IDS of wired networks use rules databases to detect anomalous information [11]. The IDS trains those attack data into rules databases. When an intruder attacks a host computer, the IDS compares the rules databases with the package of attack data and raises an alarm to the manager who decides whether the package is anomalous or not. This is a passive IDS. In a WSN, IDS is an important security tool against outsider attackers. It focuses on detection of misbehavior or malicious nodes and the application of countermeasures appropriately. When IDS detects WSNs misbehavior, it will isolate the malicious node from the WSNs. Thus, not only the detection of malicious nodes is important, but also the application of countermeasures is effectively.

The rule database of IDS in wired networks is bigger than WSNs rule databases. In wired networks, the database must store more than one thousand rules for comparison with error data. However the WSNs only store a few types of intruder misbehavior because of the limitation of memory storage. So the intrusion detection methods of wired networks cannot be used in WSNs [20].

A WSN has limited resources, communication and calculation consume energy. The network lifecycle becomes short, if the IDS processes a great quantity of data or transmits it frequently. Hence, it is useless to evaluate efficacy of IDS in wired networks. The present research arranges an evaluation method of efficacy in WSNs and wired networks.

In this paper, we discuss types of attacks on wireless sensor networks and how to prevent them. We also propose an isolation table to detect intrusions in wireless sensor networks. The method is divided into four stages: the definition of IDS, the CH monitors member nodes, the member nodes monitor CH, and the system backing up the isolation table. Intruders attack WSNs through MNs and use them to depose the CH and to alter routing

doi:10.4304/jnw.5.3.335-342

information. Thus we focus on preventing intruders from obtaining member nodes to attack WSNs.

A wired network estimates its performance by accuracy of delivery and recall rate. However, wireless sensor networks use limited resources to sense data; hence IDS energy consumption is an important consideration. The objectives of this paper are listed as follows.

1. Generate IDS isolated intruders in WSNs.
2. Reduce IDS energy consumption to extend WSNs lifecycle.
3. Determine the balance between energy consumption and WSNs security.

The remainders of the paper are organized as follows. Section II introduces the intrusion detection system and related technologies. In Section III, we specify the Isolation Table Intrusion Detection System (ITIDS). Section IV illustrates the experimental results and discussion. Finally, we make conclusions and discus future work in Section V.

II. The Intrusion Detection System of Wireless Sensor Networks

Wireless networks broadcast data that allowing intruders to intercept it and to analyze Access Point (AP) authentication. Once the intruder obtains associated keys, he can connect to the network and attack it freely. As wired and wireless networks contain differing attributes, attacks against them also differ. This section is focused on the study of related work regarding intrusion detection in wired and wireless networks.

A. Intrusion Detection Types

Sensor nodes and BS transmit data through wireless communication. Information communication consumes most energy in WSNs [13]. Sensor node communication consumes energy depending on the distance between source nodes and destination nodes. In addition, to reduce energy consumption, sensor nodes install a sleep device and set a sleep model. The sensor nodes switching from sleep to wake modes will consume much energy [19].

Recently, increasingly serious attacks have targeted WSN. The intruders combine different attack behaviors to achieve irregular attacks, making simple methods ineffective. We have used combination methods to detect the attacks and to defend against various types of attacks for better performance.

In next section, we will introduce two typical WSN IDS: Collaboration-based Intrusion Detection (CID) [22] and Routing Tables Intrusion Detection (RTID) [4]. CID is a continuous IDS that detects intrusion during the cluster duty-cycle. RTID is an event-driven IDS. While the attacks are occurring, the IDS will compare the attack data and raise alarms. Our system is a combination IDS. Managers can choose the detection model depending on the seriousness of the attack.

B. Collaboration-based Intrusion Detection (CID)

There are two roles in the cluster of WSNs: cluster head (CH) and member nodes (MNs) in the CID. The responsibilities of CH and MNs are different; so CID method uses several security levels to implement its system [22]. The CH must gather and integrate whole WSN data to control MNs and to communicate with BS. Therefore, it is important to reduce the energy consumption and defend against the intrusion of CH. To reduce energy consumption, MNs are divided into several Monitor Groups (MGs) to monitor CH. The architecture of CID is CH and the other nodes are MNs. An administrator sets N_m as the number of nodes in a cluster, and N_k as the number of nodes in MGs. N_g as the number of MG is calculated by N_m/N_k. The administrator sets a threshold $\gamma(1 \quad \gamma \quad N_k, N_k \in Z+)$; when the MNs raise alarms exceeding a threshold, they can depose the CH.

The MNs sense data and the CH monitors MNs through authentication methods. The CH detects anomalous MNs and isolates them. When the CH has been changed, the intruder can use an anomalous node to attack WSNs, the drawback of this method; the advantages of CID are: (1) using cluster method to monitor WSN can save energy effectively; (2) the administrator sets threshold for different levels of security. When the CH is changed, this method cannot continue monitoring MNs because the new CH does not obtain isolation information of previous CH. So the new CH must detect the malicious nodes again, thus consuming additional energy.

C. Routing Tables Intrusion Detection (RTID)

When sensor nodes are deployed, the WSN builds routing tables into transmission data. This method uses the routing table to detect anomalous behaviors. Assuming node A can receive data from node B, node C and node D shown in Figure 1 [4].

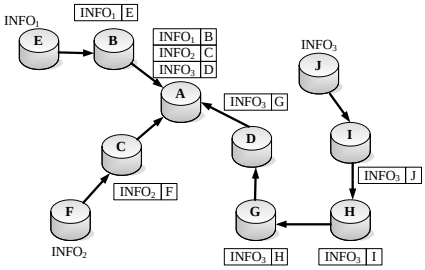

Figure 1. The anomaly detection table for IASN.

After deploying sensor nodes, each sensor node creates a routing table. This table contains the information of each node. When sensor node receives data, it authenticates data using the table Information Authentication for Sensor Networks (IASN). The authors combine Destination-Sequenced Distance-Vector Routing (DSDV) [14] and IASN to detect the anomalous behaviors.

The advantage of RTID is that an administrator can detect anomalies easily by comparing information with

DSDV and authenticating by IASN. The RTID can defend against outsider attackers. The drawback of this method is each node must store a DSDV table that will consume unnecessary energy and store duplicate information of the routing table. In the next section, we will describe the details of our proposed method.

III. The Isolation Table Intrusion Detection System (ITIDS)

The features of wireless sensor networks are limited resources and low computation. Thus an intruder will exhaust all WSNs energy to cause disconnection. The energy consumption of IDS is an important issue for system design. The WSNs consumes energy through sensing, transmitting, and computing data. Hence, intrusion detection must avoid consuming dispensable energy to detect malicious nodes. To continually isolate malicious nodes, we propose a method using isolation tables to avoid IDS consuming unnecessary energy.

There are four characteristics of ITIDS: one BS, one Primary Cluster Head (PCH), several Secondary Cluster Heads (SCHs), and the remaining sensor nodes are MNs. The definitions are shown as follows:

BS: The administrator uses BS to control whole WSN. The BS receives sensing data and isolation tables.

PCH: The duty of PCH is to gather sensing data and isolation tables from SCHs to BS. The PCH also divides its duty-cycle to SCHs of MGs to monitor it.

SCHs: SCHs calculate trust values to find malicious MNs. SCHs monitor PCH with MNs in MGs.

MNs: The MNs sense data to SCH. The MNs are divided into several MGs to monitor PCH in rotation.

The proposed method is divided into four stages: First, the system predefines IDS; next, the SCH monitors MNs; and then the SCHs and MNs monitor PCH; finally, the IDS backups the isolation table in BS. The related parameters of ITIDS are shown in Table 1.

TABLE 1.
RELATED PARAMETERS OF ITIDS

Parameter	Definition
N_k	The number of member nodes in monitor group
N_{INFO}	The data type of a transmission node
N_{id}	The member node identify
MG_{id}	The monitor group identity
E_n	The remained energy of member node(μJ)
γ	The threshold of member nodes raise alarm
A_n	The anomaly behavior record

A. Predefinition

Before the sensor nodes are deployed, the administrator can select a PCH and set the sensing type of each sensor node, the number of MG. After the sensor nodes are deployed, the MNs are divided into many MGs, depending on the setting number. The PCH selects a sensor node from each MG randomly as a SCH, and splits its duty-cycle into the SCHs duty-cycles equally. The transmission cost of WSNs is higher than the calculation cost. To save energy consumption the MN transmission hop is one hop to an SCH. After the predefinition processes, the IDS can start to detect malicious nodes and to monitor each node. Four functional characteristics of ITIDS that process their jobs are shown as follows:

BS: (1) the administrator sets sense data types in the routing table; (2) the administrator sets the default value of alarm threshold (γ) as 2/3 N_k; (3) the administrator selects a sensor node to be PCH; (4) the administrator sets the number of MG.

PCH: (1) select a sensor node from each MG to be SCH; (2) divide its duty-cycle to SCHs duty-cycle equally; (3) integrate sensing data and isolation table from SCHs to BS.

SCHs: (1) receive N_{id}, MG_{id}, N_{INFO} and remaining energy from each MN of MGs; (2) authenticate the original set of MNs information; (3) isolate and record malicious nodes in its isolation table; (4) integrate sensing data and its isolation table to PCH periodically.

MNs: (1) report MNs information to SCH; (2) transmit sensing data to SCH.

B. SCH Monitors MNs

In this stage, MNs are monitored by SCH. As SCH has higher authority, SCH can determine if MNs are anomalous. The SCH authenticates the report information of the MNs. If the MN information is erroneous, the SCH isolates it from WSN. The SCH records anomalous information in an isolation table. The isolation table of SCH records malicious MNs in its MG. The PCH integrates isolation tables of each SCH and transmits sensing data to BS periodically. If the data of MN is correct, the SCH aggregates these data and sends PCH information to BS.

The erroneous information of MN can be divided into different anomalous information, which can be determined as follows.

(1) Routing information has been changed; the intruder uses erroneous routing information to drop messages that consume energy. Attack behaviors such as spoofing, alteration, and replayed routing information or selective forwarding are stored in the isolation table.

(2) The remaining energy of MN exceeds the last recorded energy of MN. This is a sinkhole attack that uses the best energy and shortest path to encourage PCH choose it to transmit information. The malicious node drops the information. We record this kind of attack behavior as a sinkhole attack in the isolation table.

The four characteristics of ITIDS process their jobs as follows.

BS: receive sense data from PCH.

PCH: integrate isolation table and sensing data from each SCH.

SCHs: (1) receive sensing data and reporting information of MNs from its MG. (2) authenticate if the information is correct; (3) check if sensing information is different from original setting; (4) calculate the remaining energy and compare with last recorded energy to detect anomalies; (5)

calculate the trust value of each MN to find anomalies; (6) record anomalous information from its MG in isolation table; (7) integrate sensing data of each MN of its MG; (8) transmit information and its isolation table to PCH periodically.

MNs: (1) report MNs information to SCH; (2) transmit sensing data to SCH.

The SCH uses remaining energy and trust values to find malicious nodes. The formula parameters are listed in Table 2.

TABLE 2.
THE FORMULA PARAMETERS TABLE

Parameter	Definition
E_i	SCH calculates remained energy of N_i
E_{pi}	SCH records latest remained energy of N_i
E_{fi}	The response remained energy of N_i
Hop_i	The hop values of N_i transmit
H_e	Each hop consume energy
T_i	SCH calculates trust value of N_i
A_i	SCH compares N_i record data with transmission information accuracy
H_i	SCH compares N_i record data with transmission hop accuracy
T_a	Administrator set weight values of remained energy
T_b	Administrator set weight values of A_i
T_c	Administrator set weight values of H_i

SCH calculates the remaining energy as the latest recorded remaining energy minus energy consumption of the MNs response data. SCH compare values of calculation with the latest recorded remaining energy of MN. The range of E_{fi} is shown as (1).

$$E_i*0.9 \quad E_{fi} \quad E_i*1.1 \tag{1}$$

If SCH receive energy information outside a range of 110%-90%, SCH determines that MN is a malicious node. This method can avoid sinkholes, the most effective attack on BS. The SCH calculates the remaining energy (E_i) formula as (2).

$$E_i = E_{pi} - Hop_i*H_e \tag{2}$$

The SCH calculates the trust value by the remaining energy of N_i (E_{fi}). The SCH compares N_i with transmission information accuracy (A_i) and the SCH compares N_i with transmission hop accuracy (H_i). The manager sets different parameters against each security level. The combination of T is 100%. The administrator adjusts weight values among remaining energy, transmission information accuracy, and transmission hop accuracy. The SCH calculates trust value of each MN of MG. The formula is shown as (3) and (4).

$$T_a + T_b + T_c = 1 \tag{3}$$

$$T_i = E_{fi} * T_a + A_i * T_b + H_i * T_c \tag{4}$$

Weight values are adjusted to prevent WSN state. If the trust value of MN is anomalous, the SCH will isolate that MN and record anomalous information into its isolation table. When the SCH detects a malicious node, it transmits its isolation table to PCH immediately to back up that the PCH to avoid the isolation information error. This stage will continue until at the end of duty-cycle of PCH.

Similar intrusion methods are used in each attack, so we can defend against attack behaviors in the same way. The intruders use serious attack methods to infiltrate WSNs, such as Hello Flooding [15], Denial of Service (DoS) [7][23], Denial of Sleep (DoS) [5][17], Sinkhole, and Wormhole [2]. The intruders usually use simple methods to damage WSNs but they need more than one MN to attack WSNs. The attack behaviors in this stage use a stable model such as continuously broadcasting the same information or using the best performance to make neighbor nodes transmit information through it. We prevent doom attacks in two parts, as follows.

(1) Repeat Deliver: The intruders repeatedly transmit information to SCH to obstruct it. So we establish a time slot to prevent this attack. If the MN sends data frequently to SCH and the interval is less than the time slot, the SCH isolates it in the isolation table.

(2) The Efficacy: When the intruders want to obtain information from WSN, they improve their resource to allow sensor nodes to transmit information through it. PCH and SCH broadcast information to MNs and send data through malicious nodes to increase its efficacy. We use a routing table to record energy information. If MN energy is exceeds latest recorded remaining energy, the SCH isolates it in the isolation table.

C. MNs of MG Monitor PCH

The intruder attacks WSN by member nodes (MNs). So, the system focuses on detecting the attacks of MNs. Although MNs do not directly connect to PCH, PCH directly broadcasts information to each member node periodically. So, MN can determine whether the PCH is intruder or not. When a MN of the MG raises an alarm, it will wait for a timeframe. Suppose the remaining nodes have not raised alarm, the SCH determines the MN is a malicious node and records the error types in its isolation table. If the remaining nodes raise alarm and reach the threshold, the SCH will depose PCH. The PCH is replaced by the SCH of MG. The new PCH integrates the isolation table from each SCH of MG and sends BS the latest isolation table. The PCH chooses SCH from normal MNs of MG randomly. The PCH divides its duty-cycle into SCH duty-cycle equally. Four characteristics of ITIDS processing their jobs are shown as follows:

BS: (1) provide isolation table to new PCH; (2) receive information and isolation table from PCH.

PCH: (1) select new SCH from normal nodes of each MG randomly; (2) gather new isolation table to BS; (3) replace its duty-cycle to SCH duty-cycle equally.

SCHs: (1) monitor PCH with MNs; (2) If the raised alarms reach threshold, SCH deposes and isolates PCH; (3) replace PCH by the SCH of MG; (4) If the raised alarms do not reach threshold, it isolates MN.

MNs**:** (1) divide MNs into several MGs; (2) When the MG is in duty-cycle, MNs monitor PCH with SCH by rotation; (3) raise alarm when the PCH is anomalous.

D. An Example of ITIDS

In Figure 2, we give an example of ITIDS operations. Assume that there are 32 sensor nodes in a cluster and one BS, and the administrator divides them into five monitor groups. The administrator selects a sensor node to be the PCH and selects a SCH from each MG. The PCH divides its duty-cycle into the SCHs duty-cycle of MG equally. The alarm threshold is γ (two-thirds of nodes of the MG). When two-thirds nodes in the MG are raised alarms, the PCH will be deposed and isolated by SCH of MG. The SCH stores a routing table shown in Table 3.

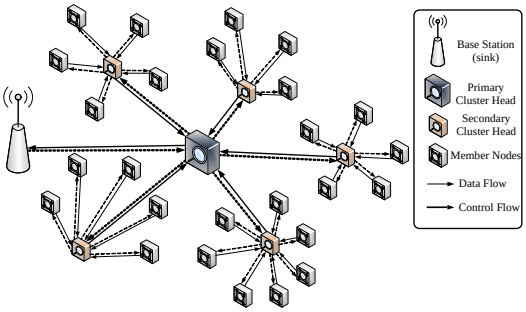

Figure 2. The architecture of ITIDS.

TABLE 3.
THE ROUTING TABLE OF SCH

N_{id}	G_{id}	N_{INFO}	E_{fi}(μJ)
N938_1	1	$INFO_2$	$7*10^6$
N123_2	2	$INFO_5$	$5*10^6$
N759_2	3	$INFO_1$	$2.3*10^6$
N267_1	5	$INFO_3$	$7.1*10^6$
N392_5	5	$INFO_3$	$6.8*10^6$

The routing table of SCH stores sensor node identification (N_{id}), MG identification (G_{id}), as shown in Table 3, the types of sensing information (N_{INFO}) and the remaining energy (E_n). The SCH compares the MN information with this table. If the information has errors, the SCH of MG isolates the MN. The SCH creates the isolation table shown in Table 4. This table contains sensor node identification (N_{id}), MG identification (G_{id}) and the cause of anomaly (A_n). There are four anomalous attack behaviors: (1) Faulty information: the delivered information is a fault type from the routing table. (2) Detection error: the MN raises a detection alarm but no attack occurs. (3) Redundancy: the same MN sends data to SCH redundantly. (4) Wrong source: the data source of transmission is wrong. This isolation table records the anomalous information. When PCH is changed, the BS will send this table to a new PCH to continue isolating malicious nodes.

TABLE 4.
ISOLATION TABLE

N_{id}	G_{id}	A_n
S564_9	3	Fault information
S392_5	5	Detection error
S516_3	3	Redundancy
S710_7	2	Wrong source

The intruder first captures a MN to attack WSN. Next, intruder attacks PCH to obtain all WSN information. The neighbor nodes of PCH are also an objective of the attack. Our research provides an effective method to detect intruders and to avoid PCH and SCHs infiltration. We compare the advantages of our method with CID and RTID, shown in Table 5.

TABLE 5.
THE COMPARE WITH IDS OF WSN

	CID	RTID	ITIDS
Hierarchical	V		V
DSDV		V	V
MG	V		V
Administrator	V		V
Authentication	V	V	V
Keep Isolation			V

Ⅳ. EXPERIMENTS AND DISCUSSIONS

We use Network Simulation 2 (ns-2) and C++ to evaluate ITIDS performance. The experimental hardware environment is AMD Athlon™ 64, 2.4 GHz CPU and 512 MB memory. We simulate the whole WSN in 10,000 square meters. The field is static and deploys 200 sensor nodes uniformly at most. Those sensor nodes broadcast radius are 50m. The PCH is in the central of WSN to collect information easily. This experiment will compare our method with CID and RTID based on the energy consumption, the transmission accuracy, and the performance. The experiments are based on authentication methods for SCH comparing MN information. The main detection types are doom stage attacks because intruders usually use them to destroy WSNs. These attack behaviors are most effective, reduplicating deliveries and transmitting data through incorrect paths. We do not discuss authentication attacks and encryption problems because we focus on IDS of WSN. Our implementation evaluation parameters are shown in Table 6.

TABLE 6.
THE IMPLEMENTATION ENVIRONMENT

Parameter	Values
Sensor Nodes	50, 100, 200
WSN Size	100 * 100 (m^2)
Location of PCH	(50,50)
Starting Energy	2J
Transmission Radius	50m
Transmission Consume	0.036w
Receive Consume	0.024w

A. The Estimation Method of Wired Networks IDS

In wired environments, the resources and the energy of a computer is infinite. The intruder intrudes the operation system by viruses or worms, such as Trojan horses. Hence, the IDS trains intruder behavior models using an artificial intelligence (AI) method. The system will be trained by old data for new attack behaviors. The primary estimating factors are precision and recall. The wired network IDS estimates parameters, as shown in Table 7.

TABLE 7.
THE WIRED NETWORK IDS ESTIMATION

Parameter	Definition
True Positive Rate (TP)	Attack occur and alarm raised
False Positive Rate (FP)	No attack but alarm raised
True Negative Rate (TN)	No attack and no alarm
False Negative Rate (FN)	Attack occur but no alarm

Helmer et al. show the precision formula in (5) [10]. Precision signifies that the attack has occurred and the IDS detects its correction. This formula consists of TP divided by TP plus FP to find precision rate.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{5}$$

Recall signifies that an attack has happened and IDS detects attacks from the attacks that have really happened. This formula consists of TP divided by TP plus FN to find the recall value shown in (6),

$$\text{Recall} = \frac{TP}{TP+FN} \tag{6}$$

Agarwal et al. observe that formula [1]. Once the attack has occurred, IDS detects it correctly. This formula uses TP plus TN divided by TP plus FP plus FN plus TN to estimate overall accuracy, as shown in (7),

$$\text{Overall} = \frac{TP+TN}{TP+FP+FN+TN} \tag{7}$$

A false alarm is defined as an intrusion occurring successfully or IDS being unable to detect it correctly. The formula uses FP plus FN to divide TP plus FP plus FN plus TN to calculate a false alarm rate, as shown in (8),

$$\text{False Alarm} = \frac{FP+FN}{TP+FP+FN+TN} \tag{8}$$

Those formulas mainly estimate the effects of wired network IDS.

B. The Estimation Method of IDS of WSNs

The sensor node is an energy-limited device. When the battery of a node is consumed, the node becomes unusable. Hence, effect estimation of WSNs is different from wired networks. If the IDS of WSN consume greater energy, the WSN will be disconnected. So we consider the consumed energy and remaining energy of the IDS. In this environment, we integrate estimating methods. The estimates parameters are shown in Table 8.

TABLE 8.
THE PARAMETERS OF WSNS IDS PERFORMANCE ANALYSIS

Parameter	Definition
Transmission Energy Consume (TC)	The consumption of transmission energy
Calculate Energy Consume (CC)	The consumption of calculation energy
Transmission Accuracy (TA)	Node Transmission Accuracy
Relay Accuracy (RA)	Node Relay Accuracy
Transmission Incorrectness (TI)	Node Transmission Incorrectness
Relay Incorrectness (RI)	Node Relay Incorrectness
Remained Energy of Node (RE)	Remained Energy of Node
Remained Nodes (RN)	Remained Nodes of WSN

Su et al. have proposed the energy consumption formula (9) [22]. They calculate the consumed energy of IDS on every node. The formula uses transmission energy and detection of energy consumption on whole sensor networks to estimate total energy consumption.

$$\text{Energy Consumption} = \sum_{i=1}^{n} TC_i + CC_i \tag{9}$$

Stresser et al. have defined the delivery accuracy formula [21]. When an attack occurred, the WSN maintains correct delivery. In (10), it uses sensor node transmission accuracy plus node relay accuracy to divide overall transmission to calculate delivery accuracy.

$$\text{Delivery Accuracy} = \frac{TA+RA}{TA+TI+RA+RI} \tag{10}$$

When an attack occurs, the WSN delivers incorrectly. The formula uses node transmission incorrectness plus incorrect node relay divided overall transmission to estimate delivery incorrectness, as shown as (11),

$$\text{Delivery Incorrectness} = \frac{TI+RI}{TA+TI+RA+RI} \tag{11}$$

They calculate the remaining resources in WSN to determine whether the energy is too low to affect the whole WSN, as shown in (12). The formula summarizes the remaining energy to divide the number of remaining nodes to estimate remaining resources.

$$\text{Remaining resources} = \frac{\sum_{i=1}^{RN} RE_i}{RN} \tag{12}$$

C. The Comparison Between CID, RTID and ITIDS

The CID method focuses on energy consumption and remaining resources that present in live nodes. The RTID method uses number of monitored nodes to calculate transmission accuracy. So, two types of experiments were conducted: compare number of live nodes with CID, and compare the transmission accuracy with RTID. We also analyze total energy consumption and average remaining resource for 50, 100, 200 sensor nodes, respectively.

a. Number of Alive Nodes

In the first simulation, the ITIDS shows the number of alive nodes to be 100, 200 sensor nodes, respectively, as shown in Figure 3. The number of live nodes means can be used to monitor our WSN. The overhead for PCH monitoring is high if the notion of collaborative monitoring is absent. An intruder can easily infiltrate our network because the usable monitor MNs decreases. The energy consumption of 200 nodes is faster than that of 100 nodes. The ITIDS causes MNs too die slowly because their hierarchical architecture. We simulate 100 sensor nodes in the ITIDS and CID. The results of the simulation show our WSN lifetime is better than CID.

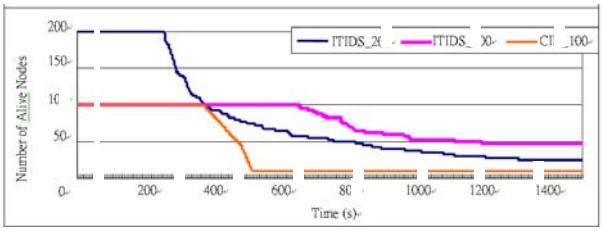

Figure 3. The comparison of the number of alive nodes between ITIDS and CID.

b. Transmission Accuracy

The simulation concerns the transmission accuracy in ITIDS and RTID by formula (10), as shown in Figure 4. First, the number of usable monitor nodes is less than 30 nodes. The intruder can use few nodes to depose PCH, so the accuracy of ITIDS is lower. When the number of monitor nodes is increased, the detection is easy; then the intruder must use more than two-thirds of sensor nodes to depose PCH. The accuracy is 95% when the number of monitor nodes is 100. The monitor energy is consumed slowly and monitors more effectively by rotation MG. The results of the second simulation show the transmission accuracy of ITIDS is better than RTID.

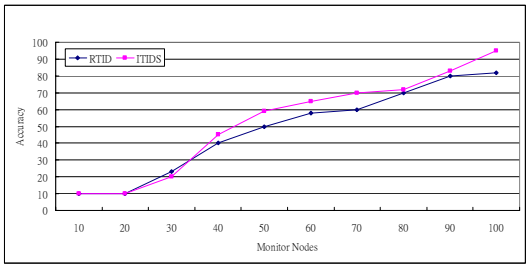

Figure 4. The comparison of the transmission accuracy between ITIDS and RTID.

c. Energy Consumption

In this simulation, we calculate the energy consumption of ITIDS by formula (9), as shown in Figure 5. Once the intruder attack is accrued in WSN, the energy consumption of ITIDS is faster than normal environment. The transmission flow is increasing while intruders are 200 nodes. The energy consumption showed whether the network was attacked or not. In Figure 5, the energy consumption is positive to the number of sensor nodes. So, the ITIDS use more sensor nodes, the energy of WSN consumes more quickly.

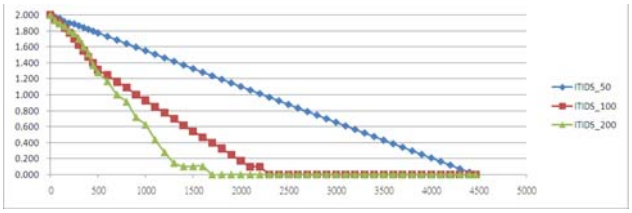

Figure 5. The total energy consumption in ITIDS.

d. Remaining resources

Figure 6 showed the average remaining resources of ITIDS by formula (12). In the case of 50 nodes, the message transmission of nodes is less than 100 nodes and 200 nodes. So, the average remaining resources go down smoothly. Once ITIDS uses more sensor nodes, the number of package transmissions grows quickly as the remaining resources decreasing fast. The result of the simulation shows ITIDS has more remaining resource in the case 50 sensor nodes than other two cases.

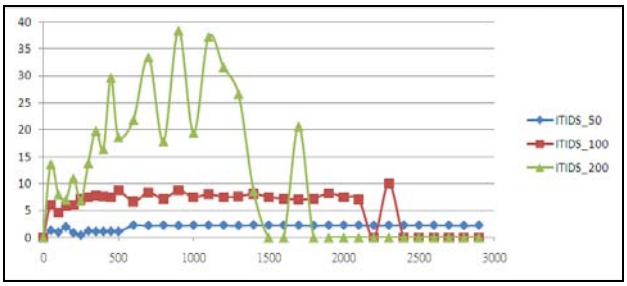

Figure 6. The average remaining resources of WSN in ITIDS.

V. CONCLUSIONS AND FUTURE WORKS

We have proposed a method to combine routing tables and isolation tables to detect anomalies. The IDS depends on attack behaviors to detect malicious nodes. When the WSN is intruded by malicious nodes, IDS detects a malicious node through its unusual behavior. The IDS compares sensor node behaviors with attack behaviors to determine anomalous information. If the node is anomalous, it will be isolated and recorded in the isolation table. The SCHs send an isolation table to PCH for integration. If there is no anomaly, the SCHs periodically send information to avoid nodes being infiltrated. Finally PCH updates the isolation table to BS periodically. When the PCH is changed, the new PCH can receive the isolation table from BS to continuously isolate anomalous nodes. The IDS must consider that WSNs has limited resources; thus, the estimation method is different between WSNs and wired networks. We have listed estimation IDS performance methods that were used in our performance evaluation. The CID method focuses on energy consumption and remaining resources to determine live nodes. The RTID method uses the number of monitored nodes to calculate transmission accuracy. Our primary experiment compares live nodes with CID, and compares transmission accuracy with RTID. The primary experiment proves our ITIDS can prevent attacks effectively.

When the remaining nodes decrease, the intruders can infiltrate WSN more easily. In this case, the intruders capture a few MNs that can depose our PCH because the alarm threshold decreases. A further study will be done on different detection methods to improve IDS using a few nodes to detect anomaly. In addition, we will find the balance between performance consumption and information security.

REFERENCES

[1] R. Agarwal and M. V. Joshi, “PNrule: a new framework for learning classifier models in data mining (a case-study in network intrusion detection),” *Proceedings of First SIAM Conference on Data Mining*, 2001.

[2] N. Ahmed, S. S. Kanhere, and S. Jha, "The Holes Problem in Wireless Sensor Networks: A Survey," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, pp. 4-18, April 2005.

[3] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, pp. 393-422, 2002.

[4] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks*, vol. 15, pp. 33-51, 2006.

[5] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Information Assurance Workshop, 2005. IAW '05.*, pp. 356-364, 2005.

[6] A. Chadha, Y. Liu, and S. K. Das, "Group key distribution via local collaboration in wireless sensor networks," in *Sensor and Ad Hoc Communications and Networks*, pp. 46-54, 2005.

[7] J. Deng, R. Han, and S. Mishra, "Defending against Path-based DoS Attacks in Wireless Sensor Networks," in *the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 89-96, 2005.

[8] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security (TISSEC)* vol. 8, pp. 228-258, 2005.

[9] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *Wireless Communications*, vol. 1, pp. 660- 670, 2002.

[10] G. Helmer, J. S. K. Wong, V. Honavar, and L. Miller, “Automated discovery of concise predictive rules for intrusion detection”, *Journal of Systems and Software*, Vol. 60, Issue 3, pp. 165–175, 2002.

[11] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*: John Wiley and Sons, 2005.

[12] Y. W. Law, J. Doumen, and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, pp. 65-93, 2006.

[13] R. Min and A. Chandrakasan, "A framework for energy-scalable communication in high-density wireless networks," in *the 2002 international symposium on Low power electronics and design*, pp. 36-41, 2002.

[14] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," *ACM SIGCOMM Computer Communication Review*, vol. 24, pp. 234-244, 1994.

[15] W. R. Pires, Jr., T. H. de Paula Figueiredo, H. C. Wong, and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks," in *Parallel and Distributed Processing Symposium*, pp. 24-30, 2004.

[16] L. Qing, Q. X. Zhu, and M. W. Wang, "Design of a Distributed Energy-efficient Clustering Algorithm for Heterogeneous Wireless Sensor Networks," *Computer communications*, vol. 29, pp. 2230-2237, 2006.

[17] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," *Vehicular Technology*, vol. 58, pp. 367-380, 2009.

[18] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed.: Wiley, 1995.

[19] E. Shih, et al, "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks," in *the 7th annual international conference on Mobile computing and networking*, pp. 272-287, 2001.

[20] T. S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," *Computer Standards & interfaces*, vol. 28, pp. 670-694, 2006.

[21] M. Strasser and H. Vogt, "Autonomous and distributed node recovery in wireless sensor networks," in *the fourth ACM workshop on Security of ad hoc and sensor networks*, pp. 113-122, 2006.

[22] W. T. Su, K. M. Chang, and Y. H. Kuo, "eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks," *Computer Networks*, vol. 51, pp. 1151-1168, 2006.

[23] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, pp. 54-62, 2002..

Rung-Ching Chen received the B.S. degree from department of electrical engineering in 1987, and the M. S. degree from the institute of computer engineering in 1990, both from National Taiwan University of Science and Technology, Taipei, Taiwan. In 1998, he received the Ph.D. degree from the department of applied mathematics in computer science sessions, National Chung Tsing University. He is Dean of College of Informatics in Chaoyang University of Technology and he is now a professor at the Department of Information Management in Chaoyang University of Technology, Taichung, Taiwan. His research interest includes web technology, pattern recognition, and applied soft computing and network security.

Chia-Fen Hsieh received the Master degree from department of Information Management at Chaoyang University of Technology in 2008. He is a candidate for doctor’s degree from graduate institute of informatics at Chaoyang University of Technology, Taichung, Taiwan. His research interest includes the security issue (intrusion detection in particular) of wireless sensor networks, ad hoc networks and wired networks.

Yung-Fa Huang received the Diplom-Eng. in electrical engineering from National Taipei University of Technology, Taipei, in 1982, M.Eng. degree in electrical engineering from National Tsing Hua University, Hsinchu, Taiwan, in 1987 and Ph.D. degree in electrical engineering from National Chung Cheng University, Chiayi, Taiwan, in 2002. He is the Department Head and associate professor of Information and Communication Engineerin, Chaoyang University of Technology. His current research interests include multiuser detection in OFDM-CDMA cellular mobile communication systems, communication signal processing, fuzzy systems and wireless sensor networks.