Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks

Abror Abduvaliyev, Sungyoung Lee, Young-Koo Lee
Department of Computer Engineering,
Kyung Hee University,
Suwon, Korea.
{abror,sylee}@oslab.khu.ac.kr, yklee@khu.ac.kr

Abstract **- In this work, we propose the architecture of hybrid intrusion detection system (eHIDS) for wireless sensor networks. In order to get hybrid scheme, we use combined version of anomaly and misuse detection techniques. In addition, we use cluster-based wireless sensor networks to reduce communication and computation costs. We evaluate the performance of our scheme by simulating the network and comparing with other related schemes. The simulation results show that our scheme performs better than other schemes in terms of energy efficiency and high detection rate.**

Keywords – intrusion detection; wireless sensor networks; hybrid system

I. INTRODUCTION

In wireless sensor networks (WSNs), many researchers have so far focus on the individual aspects of security that are capable of providing protection against specific types of attacks. Recent years, many cryptographic-based security solutions have been proposed, but surprisingly less importance is given to intrusion detection issues of WSNs. The proposed cryptographic solutions alone cannot prevent all possible attacks. Thus, energy efficient and lightweight intrusion detection system is required to increase the level of reliability in a security solution for the applications of WSNs [1-3].

An intrusion detection system (IDS) is necessary to detect the attacks. An IDS is able to detect packets in the network and determine whether it is intrusion or not.

In this work, we propose energy efficient hybrid intrusion detection system for WSNs. We use both of anomaly and misuse detection. In order to get hybrid system, we use combined version of anomaly and misuse detection techniques. These techniques provide high detection rate and high accuracy of detection. In addition, we use cluster-based wireless sensor networks (CWSNs) to reduce communication costs and packet overheads. In this type of network, all sensor nodes are clustered, and a Cluster Head is selected to manage the operation of its own cluster and aggregate data from sensor nodes. CWSN helps to achieve the aims of less consumption of energy, an increase in the networks scale and a prolonged network lifetime. Many clustering protocols have been proposed, such as TEEN [13], APTEEN [13], and PEGASIS [13]. The example of the clustered WSNs can be seen in the Figure 1. Most of the time, the attackers consider the cluster head to be their first attack target because of its responsibility of data aggregation.

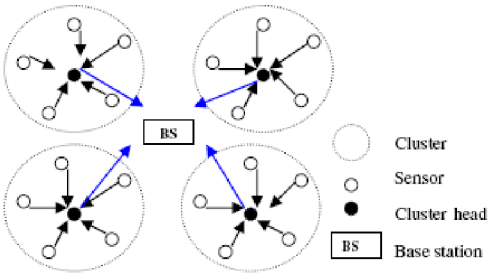

Figure 1. Simple scenario of clustered WSNs

The outline of this paper is organized as follows: In Section II, we give background information about IDS in WSNs and related works. In Section III, the proposed scheme and architecture of eHIDS are introduced. The simulation results and analysis of the proposed scheme are discussed in Section IV. We conclude our work with discussing further research directions in Section V.

II. BACKGROUND OF IDS IN WSNS AND RELATED WORKS

Sensor networks inherit all aspects of wireless networks, and they have their own distinct characteristics that make the design of a security model for WSNs apart from that of Ad hoc networks. R. Roman et al. [4] showed in his work that IDS proposed for ad hoc networks cannot be directly applied to WSNs. So, WSNs demand for a novel and lightweight design of IDS. There are three main techniques that IDS can use to classify the attacks [3, 6]:

Misuse detection: the action or behavior of nodes is compared with well-known attack patterns. In this case, attack patterns must be defined and given to the system. The disadvantages are that this technique needs the knowledge of to build attack patterns and they are not able to detect novel attacks, in addition, always someone has to update the attack signatures database.

Anomaly detection: this technique compares behavior of observed nodes with normal behaviors rather than attack patterns. This model first describes normal behaviors which are established by automated training and then flags as intrusions any activities varying from these behaviors. The disadvantages of this technique are that system can exhibit legitimate but unseen behavior which

leads to a substantial false alarm rate. Also, an intrusion that does not exhibit anomalous behavior may not be detected, resulting in false negatives.

Specification-based detection: this technique combines the aims of misuse and anomaly detection. This model is based on deviations from normal behaviors which are defined by neither machine learning techniques nor training data. The attack specifications are defined manually that describe what normal behavior is and monitor any action with respect to these specifications. The drawback of this model is manually development of attack specifications which is too time-consuming process for human beings.

As we consider proposing hybrid system, there are some proposed hybrid schemes such as HIDS [8] and eHIP [9].

In recent work [8], Yan et al. proposed hybrid approach for IDS. The algorithm contains of misuse detection model, anomaly detection model and decision making modules. The novelty of their method is the use of back propagation network (BPN) for anomaly detection module. First, the packet records are given to anomaly detection model to check for abnormal activities. If activity is determined as abnormal then it will be forwarded to both misuse detection model and decision making module. Then, the misuse detection model analysis received data with the help of BPN and sends them to the decision making module. Finally, the decision making module combines the outputs of both models to determine whether or not an output is an intrusion, and the category of attack. In case of intrusion, the module reports to the base station. The simulation results show that the scheme performs well for energy efficiency and computation cost of WSNs. The limitation is obtaining training data for determining the intrusion. Our work is motivated from this work and improves it in terms of completeness and reliability.

In [9], Su et al. proposed energy efficient hybrid intrusion prohibition system for CWSNs. They use both intrusion detection and intrusion prevention techniques in order to have hybrid security solution. Their system contains collaboration-based intrusion detection subsystem which uses cluster head monitoring and member node monitoring. In this scheme, member nodes monitor the cluster heads and the cluster heads monitor their own cluster members by using alarm table and HMAC. This scheme successfully detects the intruder in case of member nodes are monitors, but when cluster nodes are monitors, the scheme lacks the detection problem because of considering the only shared key between cluster head and member node. It is the fact that the shared key can be easily accessed by the attacker and used during the data transmission. In our scheme, cluster head has full capability of detecting the attacks by using hybrid IDS scheme. This approach has high accuracy and detection rate, also prolongs the network lifetime and scale of the network.

III. PROPOSED SCHEME

This section presents the detailed information about our proposed scheme.

As mentioned in Section I, we use the combined version of anomaly and misuse detection techniques. To the best our knowledge, anomaly detection alone performs a high detection rate and low accuracy while misuse detection has high accuracy and low detection rate. If we combine both techniques into one technique, then we will have hybrid technique which helps to achieve the goals of high accuracy and high detection rate.

Our proposed system consists of three models: anomaly detection, misuse detection and decision making model. Our approach mostly inherits the work in [8] with some improvements. First, the packets delivered to anomaly detection model are checked for abnormal activities. If model finds that intrusion is not occurred, the packets will be successfully forwarded to the BS. Otherwise, if anomaly detection model finds that intrusion is occurred, then the packets will be sent to misuse detection model and decision making model. The model compares received information with predefined patterns of normal attacks, then the model sends the results to decision making model. The information derived from both techniques is used as an input for decision making model. It integrates the outputs of anomaly and misuse detection models in order to decide whether intrusion is occurred or not. In case of presence of an intrusion, the model reports the results to the administrator of the network. Figure 1 shows a simple architecture of hybrid intrusion detection system for WSNs.

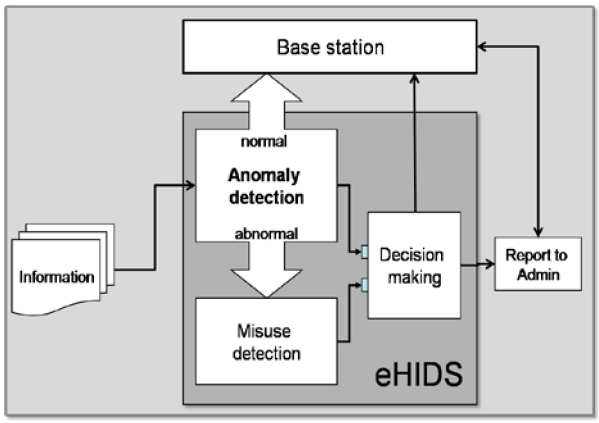

Figure 1. Architecture of eHIDS

In our proposed scheme, there are no local or global agents which are located in every sensor node. We have only IDS agent on CHs. This design helps us to achieve the aims of energy efficiency and low computational cost. According to assumptions, each sensor node is capable to have local and global agents as it was in previous works, but it burdens the entire network in terms of computation and negatively affects to the memory constraints of the sensor nodes. Thus, having IDS agent only on CHs significantly reduces computation costs.

A. Anomaly detection model

In anomaly detection phase, we use pre-defined rules to detect abnormal behaviors. Because the anomaly detection uses a defined model of normal behavior, a packet is determined to be abnormal by the system when the current behavior varies from the model of normal behavior. As a result, the anomaly detection usually determines the normal communication as abnormal communication, and creates the problem of erroneous classification. However, it seldom marks an abnormal communication as a normal communication. Therefore, the anomaly detection model is used to filter a large number of packet records first, and make further detection with the misuse detection model, when the amount of information decreases. Our anomaly detection model adopts a rule-based method, using the rule base to analyze the packets, and distinguish which packets are abnormal.

In our research, we use the rule-based method to construct the anomaly detection model [16]:

- Integrity rule: The packet payload must be the same along the path from source node to destination node.
- Delay rule: The delay of a packet from one node must be limited within a timeout
- Radio transmission range rule: All packets received by CH must be originated from one of its member nodes or previous hop through the detection of the average receive power.

B. Misuse detection model

In this phase, we use a machine learning algorithm called SLIPPER [12] to build the misuse detection model. The model will consist of multiple binary classifiers, which includes a set of rules. SLIPPER is a confidence-rated boosting algorithm, and each rule learned from its training dataset might not have very high prediction accuracy on new data. A rule R in binary classifier is forced to abstain on all data records not covered by R, and predicts with the same confidence C_R on every data record x covered by R. The confidence C_R was calculated when the rule was built in the training phase. A default rule which covers all data has negative confidence, while all other rules have positive confidence. The binary prediction engine is same as the final hypothesis in SLIPPER [28], which is:

$$H(x) = sign(\sum_{R_t:x\in R_t} C_{R_t}) \quad (1)$$

In other words, the final hypothesis sums up the confidence values of all rules that cover the data and the sign of the sum represents the predicted class label.

However, our binary prediction engines will output a signed sum of the confidence values of all rules that cover the data (not just the sign). We refer this signed sum to prediction confidence (PC). The magnitude of PC represents the confidence of the prediction. Since the detection model consists of multiple binary classifiers, a final arbiter is needed to pick one of the prediction results from those binary classifiers as its final prediction. The prediction confidence ratio (PCR) based arbitral strategy [29] could be used in the final arbiter in our intrusion detection system for wireless sensor network, because the computation required by this arbitral strategy is very light and meet the constrained computational power of sensor nodes. The PCR is defined by:

$$PCR = PC/MAX\{PC^1, PC^2, .., PC^m\} \quad (2)$$

Where PC stands for prediction confidence on a data record in test dataset while PC^i stands for the prediction confidence on the i^{th} data record in the training dataset with total m records. The prediction confidence ratio based final arbitral strategy can be expressed as follow:

$$i = \{j | PCR_j = MAX\{PCR_1, PCR_2, .., PCR_n\}\} \quad (3)$$

Where PCR_j is prediction confidence ratio and computed by Equation (2), and the i is the index of the binary classifier whose prediction result is selected to be the final prediction result.

C. Decision making model

The decision making model is used to combine the results of the anomaly and misuse detection models and determine whether an intrusion is occurred or not. It then reports the results to the administrator of network to help them handle the state of the system and make further countermeasures. In other words, the decision making model rises an alarm in case of if the output is counted as an intrusion.

This model also utilizes on rule based approach, using the rules to combine the outputs of two detection models, and its main advantages are that it is very simple and fast in terms of computation.

IV. PERFORMANCE EVALUATION

This section presents the performance of the proposed scheme.

A. Analytical analysis

In this part, we analyze and evaluate the proposed detection capability, to determine the performance of our scheme. The probability of detection an attack, P_D, depends on three factors: number of monitoring nodes in a cluster, probability of a missed detection of a monitor nods (i.e. cluster head), and our malicious counter threshold *X*. We defined K as the number of monitor nodes and P_C as the probability of a collision occurring in a transmission link:

$$P_D = \sum_{i=X}^{K} \binom{K}{X} (1 - P_C)^X P_C^{K-X} \quad (4)$$

We define P_F as the probability of a false positive for a legitimate node. The probability of false positive P_F is expressed by the following equation:

$$P_F = (1 - P_C)^2 P_C + {P_C}^2 (1 - P_C) \quad (5)$$

According to (5), we can easily derive the probability of false positive detection rate P_{FD} as follows:

$$P_{FD} = \sum_{i=X}^{K} \binom{K}{X} (1 - P_F)^X P_F^{K-X} \quad (6)$$

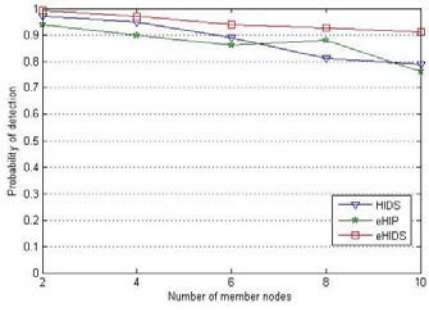

Figure 3. Probability of detection

As shown in Figure 3, the proposed scheme is effective when the number member nodes is increased. Also, the probability of a missed detection affects the efficiency of our scheme. However, eHIDS performs better detection results than other schemes, exceeding over 96%.

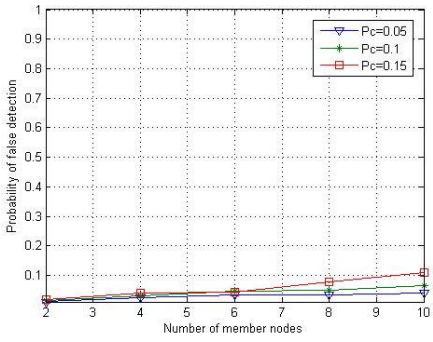

Figure 4. Probability of false detection

The probability of false positive detection is shown in Figure 4. It indicates that the increasing number of nodes results in an increase in the probability of a collision.

B. Simulation results

To evaluate the performance of our proposed hybrid detection scheme in realistic WSNs applications, we simulate the network with 100 sensor nodes, in a field of 100 meters x 100 meters, using Castalia, a WSNs simulator based on Omnet++ [11]. The sensor nodes are deployed in a randomized grid fashion. The TunableMAC which exposes many parameters to the user is used as the MAC protocol and Simple tree routing is used as a routing protocol. The detection algorithms in each cluster heads are implemented in the application layer of wireless sensor's stack. The rest of the specifications of a sensor node are defined in Table I.

TABLE I. SENSOR NODE'S SPECIFICATIONS

Initial battery of each sensor node	1×10^6J
Power consumption for transmission	1.6W
Power consumption for reception	1.2W
Power consumption in idle state	1.15W
Transmission power of the antenna	0.0280
Transmission and Reception gain	1.0
Carrier sense threshold	$3.652e^{10}$W
Receive power threshold	$1.559e^{11}$W

Figure 5 shows the performance of our scheme with malicious nodes in the network. Castalia simulator supports packet collision by setting the parameter *SN.WirelessChannel.CollisionModel*. We set the sensor nodes exhibiting malicious behavior by increasing their packet drop ratio, changing the fields of forwarded packets and sending false Hello packets with abnormal radio power. The results prove our scheme has a good packet delivery ratio.

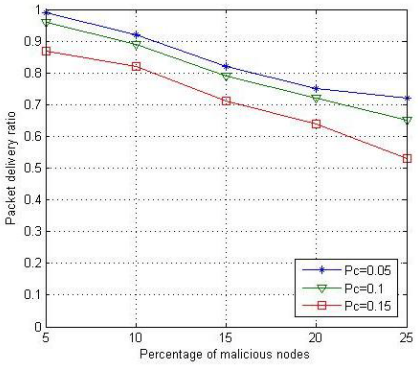

Figure 5. Packet delivery ratio

As the percentage of malicious nodes increases, revoking malicious nodes requires a particular period of time. So, the packet delivery ratio is quickly reduced, if malicious nodes increase.

Figure 6 illustrates the total amount of energy consumed by each node in the network. It can be clearly seen that eHIP is the most energy consuming scheme in this comparison. In this scheme, each node consumes on average 2,91J for the total packet transmission process, whereas eHIDS and HIDS consumes 1,93J and 2,58J respectively.

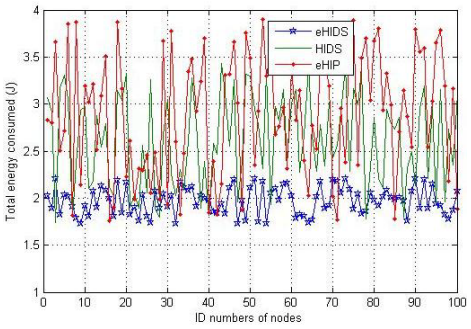

Figure 6. Energy consumption by each node

At first glance, it seems to be like the small amount of energy is consumed by each node, but if calculate the total amount of energy consumed in all nodes in the network; we can see the difference between schemes' performance. The total energy consumption of eHIDS is calculated as follows:

$$E_t = E_A + E_M \quad (7)$$

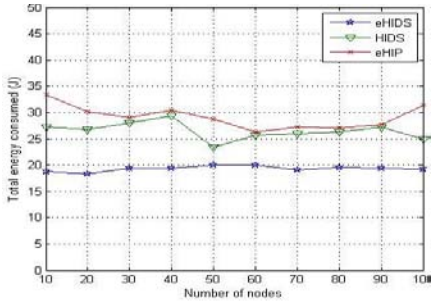

Figure 7. Total energy consumption

V. CONCLUSIONS AND FUTURE WORKS

We have proposed the hybrid intrusion detection system for WSNs. Our anomaly and misuse detection models help to achieve the aims of high accuracy and high detection rate. According to simulation results, our scheme performs well in terms of energy efficiency and computational costs. Also, the scheme has high detection rate and high accuracy of detection that does not contradict with our assumptions.

As the future research directions, we evaluate the scheme to detect various attacks and implement it in a real environment. Specially, evaluating it under radio jamming attack would be the most priority.

VI. ACKNOWLEDGEMENTS

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement)" (IITA-2009-(C1090-0902-0002)) and was supported by the IT R&D program of MKE/KEIT, [10032105, Development of Realistic Multiverse Game Engine Technology]. This work also was supported by the Brain Korea 21 projects and Korea Science & Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (No. 2008-1342). Prof. Sungyoung Lee is the corresponding author.

VII. REFERENCES

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", IEEE Comm. Magazine, Vol. 40, No. 8, pp. 102-114, Aug. 2002.
2. Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Communication Surveys, 2006; 8(2): 2–23.
3. Y. Zhang, P. Kitsos, "Security in RFID and Sensor Networks", Auerbach Publicatio, 2009.
4. R. Roman, Jianying Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks", Consumer Communications and Networking Conference, Vol. 1, pp. 640–644, 2006.
5. L. Guorui, H. Jingsha, and F. Yingfang, "Group-based intrusion detection system in wireless sensor networks", Computer Communications, Vol. 32, No. 18, pp. 4324-4332, 2008.
6. I. Krontiris, Z. Benenson, T. Giannetsos, F.C. Freiling, and T. Dimitriou, "Cooperative Intrusion Detection in Wireless Sensor Networks", EWSN 2009, LNCS, Vol. 5432, pp. 263-278, 2009.
7. R. Chen, Ch. Hsieh, and Y. Huang, "A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks", Proceedings of the ICUIMC-09, Suwon, Korea, pp. 238-245, January, 2009.
8. K. Q. Yan, S. C. Wang, and C. W. Liu, "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks", In Proc. of the IMECS 2009, Hong Kong, 2009, pp. 411-416.
9. 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, 2007.
10. S. Doumit and D. P. Agrawal, "Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor network", MILCOM 2003, pp. 609-614.
11. Castalia Simulator, http://castalia.npc.nicta.com.au
12. W. Cohen and Y. Singer, "A Simple, Fast, and Effective Rule Learner", Proc. of 6th national Conference on Artificial Intelligence and 11th Conference on Innovative Applications of Artificial Intelligence, Orlando, Florida, pp.335-342, July 1999.
13. A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Computer Communications, Vol. 30, No. 14, 2007.
14. T. H. Hai, F. khan, and E. –N. Huh, "Hybrid Intrusion Detection System for Wireless Sensor Networks", In Proc. of the ICCSA 2007, LNCS 4706, pp. 383-396, 2007.
15. T. H. Hai, E. -N. Huh, and Minho Jo, "A lightweight intrusion detection framework for wireless sensor networks", Wireless Commun. Mob. Computing, 2009.
16. R. da Silva et al, "Decentralized intrusion detection in wireless sensor networks", Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Montreal, Quebec, Canada, October, 2005.