Adaptively Supervised and Intrusion-Aware Data Aggregation for Wireless Sensor Clusters in Critical Infrastructures

Safa Otoum, *Student Member, IEEE,* Burak Kantarci, *Senior Member, IEEE,*
and Hussein Mouftah, *Life Fellow, IEEE*

***Abstract*—Wireless sensor networks have become integral components of the monitoring systems for critical infrastructures such as the power grid or residential microgrids. Therefore, implementation of robust Intrusion Detection Systems (IDS) at the sensory data aggregation stage has become of paramount importance. Key performance targets for IDS in these environments involve accuracy, precision, and the receiver operating characteristics which is a function of the sensitivity and the ratio of false alarms. Furthermore, the interplay between machine learning and networked systems has led to promising opportunities, particularly for the system level security of wireless sensor networks. Pursuant to these, in this paper, we propose Adaptively Supervised and Clustered Hybrid IDS (ASCH-IDS) for wirelessly connected sensor clusters that monitor critical infrastructures. The proposed ASCH-IDS mechanism is built on a hybrid IDS framework, and transforms the previous work by continuously monitoring the behavior of the receiver operating characteristics, and adaptively directing the incoming packets at a sensor cluster towards either misuse detection or anomaly detection module. We evaluate the proposed mechanism by introducing real attack data sets into simulations, and show that our proposal performs at 98.9% detection rate and approximately 99.80% overall accuracy to detect known and unknown malicious behavior in the sensor network.**

***Index Terms*—Anomaly detection, misuse detection, intrusion detection, machine learning, wireless sensor networks, clustering**

I. Introduction

With the wide usage and deployment of Wireless Sensor Networks (WSNs) and their integration with the Internet of Things concept, WSNs have been recognized as robust tools to meet the requirements for monitoring critical infrastructures such as smart grid, smart micro-grid, and/or production/manufacturing assets. WSNs employ various types of sensors, i.e., thermal and magnetic which help in monitoring the different aspect of systems such as pressure and temperature [1], [2]. In long term and continuous monitoring of these critical infrastructures, detection of malicious traffic activity (i.e. intrusion) has become of paramount importance.

Majority of the existing intrusion detection solutions rely on various data mining methods. These models have been verified to be very effective [3] [4] [5]. Although there has been remarkable progress in Intrusion Detection and Prevention research, sensor networks monitoring critical infrastructures are still vulnerable to unknown attacks.

In this paper, we aim to address detection of known and unknown intrusive behavior at the sensory data aggregation stage of WSN-based critical infrastructure monitoring systems. To this end, we propose an adaptive intrusion detection system (Adaptive-IDS), namely Adaptively Supervised and Clustered Hybrid Intrusion Detection System (ASCH-IDS) to classify the aggregated data. In ASCH-IDS, data gathered by sensors is directed into two machine learning-based subsystems namely misuse detection subsystem and anomaly detection subsystem. The former is effective in the detection of known attacks whereas the latter is effective in detecting unknown attacks. The Misuse Detection Subsystem (MDS) runs a random forest-based classifier to detect known attacks. The classifier basically compares the upcoming sensed traffic to attack patterns that are known from the training data to identify intrusive behavior. The Anomaly Detection Subsystem (ADS), on the other hand, employs an Enhanced-DBSCAN classifier to detect unknown attacks by comparing sensed data to normal patterns in training data-set. The key question here is the following: How to decide the destination subsystem for an aggregated data stream? Can a probabilistic routing scheme be used for forwarding the data to one of these subsystems for analysis. In our proposed solution (i.e., ASCH-IDS), we address these issues by adaptive supervision of our previously proposed Clustered Hierarchical Hybrid-Intrusion Detection System (CHH-IDS) [6]. The proposed scheme continuously keeps track of the Receiver Operating Characteristics (ROC) in each subsystem, and based on the improvement/degradation of the ROC behavior, it adaptively adjusts the proportion of aggregated data forwarded to one of the two subsystems. Our simulations on real attack data demonstrates up to 99% detection rate and up to 99.80% overall accuracy.

The rest of the paper is organized as follows: Section II provides a background and related work to motivate the proposed research. Section III presents the proposed ASCH-IDS methodology. Section IV presents the performance evaluation and relevant discussions on the proposal. Finally, the paper is concluded with future directions in Section V.

II. Related Work

As an example to WSN-based critical infrastructure monitoring scenario, effective IDS solutions against energy theft in

The authors are with the School of of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada.
E-mail: {sotou070, burak.kantarci, mouftah}@uottawa.ca

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

the power grid have been proposed by introducing WSN-based Advanced Metering Infrastructure (AMI) monitoring, and they have led to significant amount of dollar savings [7]. In a similar scenario, where an island of microgrid is monitored by a WSN, communication blackouts may occur among the sensors due to cyber attacks to the communication infrastructure [8]. Although there have been promising solutions against cyber attacks, it is worth noting that in critical infrastructures WSNs are deployed to monitor both cyber and physical infrastructures. For instance power sensors can be used to monitor and control a residential microgrid [9]. A grand challenge in such setting is the small size battery limitation of voltage sensors [10]. Although these challenges read sustainability issues, the integration of WSNs into a critical infrastructure such as a residential microgrid, introduces vulnerabilities for the cyber and physical infrastructures in the presence of malicious attacks. Therefore, while aggregating the data reported by a number of sensors, an effective IDS has to be implemented that can protect the aggregated data from both known and unknown attacks.

The primary goal of any IDS is to detect abnormal activity and raise an alarm in order to secure the network [11]. Computational intelligence, including machine learning, fuzzy logic and artificial neural networks, has been an effective tool for the recognition of abnormal activities in network traffic [12]–[14]. Basically, the objective of an IDS is to distinguish regular behavior from intrusive behavior via binary classification. Adaptive techniques for IDS have also been considered to improve classification accuracy. The authors in [15] presented a fully IDS validation process by using the adaptive and automated testing paradigm. As another example of an adaptive IDS, the study in [16] proposed the real time Adaptive Model Generation (AMG) architecture to implement data mining-based IDSs. In [17], the authors proposed a methodology of anomaly-based IDS which used the game theoretical approach. They designed a lightweight anomaly detection technique by achieving a trade-off between detection rate, energy consumption, and false positive rates [17].

To the best of our knowledge, an adaptive-IDS solution for WSN-based monitoring applications to deal with both known and unknown intruders remains an open issue. In our proposed scheme, ASCH-IDS, we present a dynamic adjustment methodology for the proportion of the sensed data directed to the anomaly and misuse subsystems.

III. Adaptively Supervised and Clustered Hybrid IDS (ASCH-IDS)

The proposed IDS framework for WSNs builds on our previous proposal, Clustered Hierarchical Hybrid-IDS (CHH-IDS) [6], which is illustrated in a minimalist way in Fig. 1. Table I presents the notation used in the description of the proposed framework, ASCH-IDS, as well as its predecessor, CHH-IDS.

A. The predecessor method: CHH-IDS

The predecessor, CHH-IDS operates on a clustered WSN that consists of N clusters each of which is made up of C sensor nodes. In each cluster, a Cluster Head (CH) is responsible for aggregating the data forwarded by the sensor nodes. Upon aggregation of the sensed data, the cluster head forwards the data to a central server where the IDS is actually deployed.

TABLE I
Notations used in ASCH-IDS system model

Notation	Description
N	Number of clusters
C	Number of sensor nodes in each cluster
S	Sensor Node
TP	True Positive
FP	False Positive
TN	True Negative
FN	False Negative
S_i	Index of a sensor node in a cluster, $i \in \{0, 1, , , c-1\}$
T_{agg}	Aggregator trust value
T^n_{agg}	Trust evaluation between the aggregator and node n
d_n	Degree of node n
Δn	Degree difference of node n
$SRSS_n$	Sum of received signal strength of node n
τ_n	Cumulative duration of node n being cluster head
T_n	Trust value for node n
M_n	Mobility factor of node n
W_n	Combined weight of node n
w_1	Weight factor for node n degree difference
w_2	Weight factor for $SRSS_n$
w_3	Weight factor for node mobility
w_4	Weight factor for node cumulative time
$M_1(t_i)$	True positive to False positive ratio at time t_i for ADSs
$M_2(t_i)$	True positive to False positive ratio at time t_i for MDSs
$M_1(\triangle t)$	True positive to False positive ratio with time difference $\triangle t$ for ADSs
$M_2(\triangle t)$	True Positive to False Positive ratio with time difference $\triangle t$ for MDSs
$\triangle t$	Time difference between $(t_{i+1} - t_i)$
$TP_1(t_i), TP_2(t_i)$	True Positive of ADSs and MDSs respectively at time t_1
$FP_1(t_i), FP_2(t_i)$	False Positive of ADSs and MDSs respectively at time t_1
α	Weight of the previous ROC characteristics in the evaluation of $M_1(t_i)$ and $M_2(t_i)$
$I(t_i)$	$M_1(t_i)/M_2(t_i)$
$\triangle R$	Adjustment (incremental/decremental) value for the proportion of sensed data forwarded to a subsystem
$R_a(t_i)$	Proportion of incoming data directed to ADSs at t_i
$R_m(t_i)$	Proportion of incoming data directed to MDSs at t_i

As its predecessor CHH-IDS, ASCH-IDS, as well, adopts the weighted cluster head selection algorithm [18], in which the cluster head is selected based on the comparison of each sensor weight with the other nodes inside its cluster. In the weighted cluster head selection procedure, each sensor is assigned a weight which is a function of its degree, Received Signal Strength (RSS), and mobility. The selection method goes through the following steps: i) Find the node degree d_n of each sensor, node degree refers to the number of neighboring sensors. ii) Calculate the degree of difference Δn, iii) Compute the sum of RSS for node n ($SRSS_n$), iv) Compute the mobility factor of each sensor node (M_n), v) Compute the cumulative time, τ_n which denotes the time passed since n has been appointed as a cluster head (cumulative time), and vi) Compute the combined sensor weight (W_n). The combined node weight equation is represented in (1) below

where w_1, w_2, w_3, w_4 are the weighing factors for the system parameters.

$$W_n = w_1 \Delta n + \frac{w_2}{|1/SRSS_n|} + w_3 M_n + w_4 \tau_n \quad (1)$$

In the equation, $\Delta n = |d_n - \delta|$, d_n is the degree of node n which refers to its neighbors, δ refers to the number of nodes that a cluster head can handle while Δn is the degree-difference of node n and $|1/SRSS_n|$ is the normalized RSS sum. Each sensor estimates its own weight, broadcasts it with its ID and compares it to neighbors' weight. The node with the minimum weight is chosen as the cluster head [18].

B. Data aggregation procedure

In CHH-IDS [6], each cluster head aggregates the sensory data from the other sensors in its corresponding cluster and sends the aggregated data to the centralized sink. The data aggregation method in [19] had been used in CHH-IDS. The data aggregation method measures the aggregator's trust score based on the trust score of each sensor along with the trust evaluation between the aggregator and the sensors [19]. We used the function in (2) [19] in CHH-IDS in order to calculate the trust score of CHs which are represented as the aggregators. In the equation, T_{agg} is trust value of the aggregator, T_n is the trust value of node n, and T^n_{agg} is the trust evaluation between the aggregator and node n.

$$T_{agg} = \frac{(\sum_{n=0}^{n-1}(T_n + 1) \cdot T^n_{agg})}{\sum_{n=0}^{n-1}(T_n + 1)} \quad (2)$$

In CHH-IDS, the aggregated traffic undergoes two parallel intrusion detection subsystems, namely the ADSs for the unknown attacks and the MDSs for the known ones, which refers to a hybrid system. ADSs of the CHH-IDS runs the Enhanced-Density Based Spatial Clustering of Applications with Noise (E-DBSCAN) algorithm. DBSCAN is a density clustering algorithm in which it studies clusters as dense areas of objects in the data space that are divided by areas of low density objects [20]. MDSs in CHH-IDS uses the Random Forest algorithm as a controlled classification method which works in two phases; the training and the classification phases [21]. It is basically a classification algorithm consists of tree-structured classifiers collection where each tree sends a unit vote for the most common class at each input [22].

C. Proposed Methodology

ASCH-IDS aims to keep track of the changes in the receiver operating characteristics of the misuse and anomaly detection subsystems, and adaptively adjusts the proportion of the sensed data forwarded to one of these two subsystems. The True Positive (TP) to False Positive (FP) ratios for ADSs and MDSs at time t_i are denoted by $M_1(t_i)$ and $M_2(t_i)$ as shown in Eqs. (3)-(4) below.

$$M_1(t_i) = \frac{TP_1(t_i)}{FP_1(t_i)} \quad (3)$$

$$M_2(t_i) = \frac{TP_2(t_i)}{FP_2(t_i)} \quad (4)$$

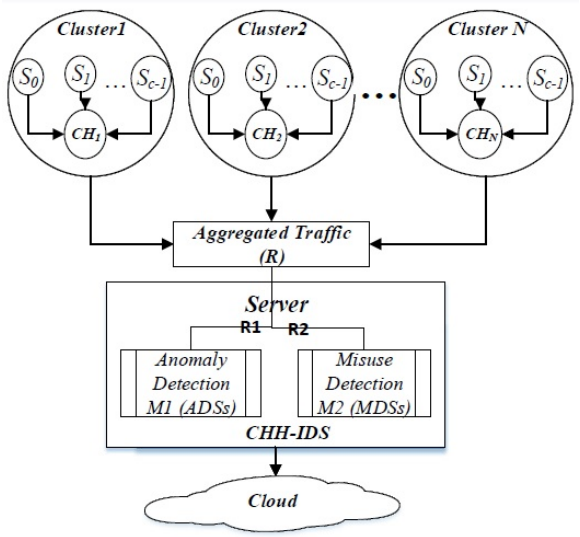

Fig. 1. A minimalist illustration of the system model. The cluster head aggregates sensed data from sensor cluster nodes. The aggregated data is distributed between the anomaly detection and misuse detection subsystems that.

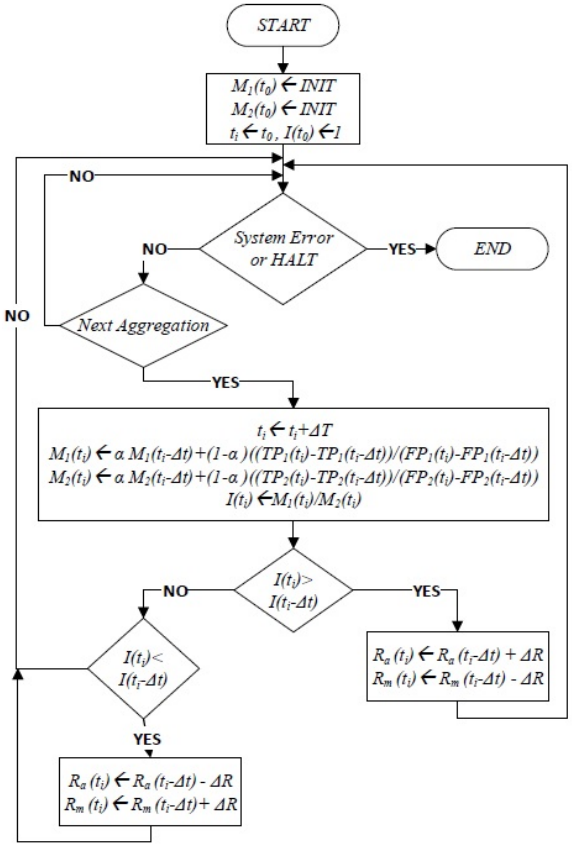

Fig. 2. ASCH-IDS Flowchart for a single decision making process.

As ASCH-IDs is proposed for real time operation, the TP/FP ratio is kept track as a running average value with time steps ($\triangle t$) as shown in Eqs. (5)-(6). It is worth noting that $\triangle t$=$t_{i+1} - t_i$.

$$M_1(\triangle t) = \frac{TP_1(\triangle t)}{FP_1(\triangle t)} \quad (5)$$

$$M_2(\triangle t) = \frac{TP_2(\triangle t)}{FP_2(\triangle t)} \quad (6)$$

When the ROC behavior of the two subsystems during the time step $\triangle t$ is obtained, the overall ROC behavior per subsystem can be calculated as a weighted sum of the current overall ROC behavior and the behavior during the time step as shown in Eqs. (7) and (8) shown below. In the equations, the α parameter denotes the weight of the overall TP/FP value that has been calculated so far and the TP/FP value during the time step $(\triangle t)$ where $t_{i+1} = t_i + \triangle t$ as described before.

$$M_1(t_{i+1}) = \alpha M_1(t_i) + (1-\alpha) M_1(\triangle t) \quad (7)$$

$$M_2(t_{i+1}) = \alpha M_2(t_i) + (1-\alpha) M_2(\triangle t) \quad (8)$$

Besides the ROC behavior in each subsystem, ASCH-IDS also keeps track of the relative running average ROC behavior of the two subsystems at any time t_i. To this end, an indicator $I(t_i)$ is introduced as shown in Eq.(9).

$$I(t_i) = \frac{M_1(t_i)}{M_2(t_i)} \quad (9)$$

The relative ROC behavior of the two subsystems is utilized in the decision of forwarding aggregated sensory data as follows: At time t_i, if $I(t_i) > I(t_{i-1})$, ASCH-IDS interprets this situation as better performing of the anomaly detection subsystem when compared to the performance of the misuse detection subsystem. Thus, increasing the sensed data proportion on the anomaly detection subsystem is expected to be beneficial for improving the overall performance. On the other hand, if $I(t_i) < I(t_{i-1})$, ASCH-IDS interprets the situation as better performing of the misuse detection subsystem when compared to the anomaly detection subsystem. In this case, the intuition is that increasing the data proportion on the misuse detection subsystem will help the IDS system improve the overall performance. For instance, if $I(t_{i+1}) > I(t_i)$, the ASCH-IDS is to increase the proportion of sensory data on M_1 and decrease on M_2 such as: $R_a(t_{i+1}) = R_a(t_i) + \triangle R$ and $R_m(t_{i+1}) = R_m(t_i) - \triangle R$ as formulated in Eqs. (10)-(11) where $\triangle R$ represents the proportional adjustment of sensor data for each subsystem. An overview of these steps is presented in detail in the flowchart in Fig. 2. It is worth noting that the flowchart presents the flow of a continuous decision procedure to adjust the sensory data proportion on each subsystem.

$$R_a(t_{i+1}) = R_a(t_i) \pm \triangle R \quad (10)$$

$$R_m(t_{i+1}) = R_m(t_i) \pm \triangle R \quad (11)$$

IV. Performance Evaluation

We evaluate the performance of ASCH-IDS to demonstrate the performance improvement of the adaptive IDS solution over its predecessor CHH-IDS in terms of accuracy and detection rates. To this end, we use the Network Simulator version 3 (NS-3) [23] with the simulation settings described in Section IV-A. In Section IV-B, we present performance results in terms of accuracy, detection rate, ROC, and precision-to-recall characteristics.

A. Simulation Settings

In the simulation environment, we simulate a WSN of 20 sensors that communicate via the Hierarchical-Dynamic Source Routing (H-DSR) protocol. The sensors are grouped in 4 clusters that spread out in a 100m x 100m area. We repeat each scenario 10 times, and in the figures, we present the average of ten runs with 95% confidence level. Table II lists a detailed presentation of the simulation settings.

TABLE II
Simulation settings

Simulation parameter	Value
Number of nodes	20
Routing protocol	H-DSR
Number of clusters	4
Simulation time	600s
Packet size	250 bytes
Trust range	[0,1]
Operational area	100m x 100m
Communication range	100m
Attack Types	DoS,Probe,U2R,R2L
$\triangle R$	0.03,0.05,0.1,0.15,0.20 and 0.25
α	0.7
$INIT$	0.5
DoS Attacks	Smurf, land, pod, Neptune, teardrop, back
Probe Attacks	Nmap, portsweep, satan, ipsweep
U2R Attacks	Perl, rootkit, buffer_overflow, load-module
R2L Attacks	Imap, guess_passwd, multihop, phf,ftp_write, spy, warezmaster, warezclient

The Knowledge Discovery in Data mining (KDD) CUP 1999 Data-set is used to validate the efficiency of the proposed ASCH-IDS system on the simulated WSN [24] [2]. The KDD CUP 1999 ID data-set helps in evaluating different IDSs methodologies. Attacks are considered under four categories as follows: Denial of Service (DoS), Probe, User to Root (U2R), and Remote to Local (R2L) attacks.

The KDD CUP 1999 ID data-set consists of three components, which are presented in detail in Table III. The 10% of KDD data-set is employed for the purpose of training, it covers 22 attack types and represent a sub-set version of the whole KDD data-set. On the other hand, the Corrected KDD data-set provides a data-set with different distributions other than the 10% KDD and whole KDD. The Corrected KDD dataset covers 14 additional attacks. The analysis of the ASCH-IDS is performed on the 10% KDD data-set since the 10% KDD works as a training set. To perform the experiments successfully, KDD CUP 1999 data-set containing connection records with variable distribution of attacks and normal classes are used in the proposed ASCH-IDS. In addition, the testing data-set proportion is different than the training data-set as well as the test data-set includes some types of attacks not in the training data-set.

B. Numerical Results

Accuracy (AR) refers to the ratio of the correctly classified occurrences, which are represented by True Positive (TP) and True Negative (TN) as shown in Eq. (12) where FN and FP are the False Negative and False Positive cases respectively.

TABLE III
KDD DATA SET DESCRIPTION [2]

KDD Data set	DoS	Probe	U2R	R2L
10% KDD	391458	4107	52	1126
Corrected KDD	229853	4166	70	16347
Whole KDD	3883370	41102	52	1126

$$AR = \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

AR has been traced for different scenarios in order to expect the system performance with different data rates as shown in Fig. 3. Fig. 3 illustrates the AR values for the anomaly detection subsystem, misuse detection subsystem, CHH-IDS and the ASCH-IDS. As seen in the figure, the proposed adaptive methodology results in the highest AR of 99.76%. The anomaly decision subsystem achieves better AR since the misuse detection subsystem achieves the least AR. The best AR was achieved by incrementing the data proportion on the anomaly detection subsystem as well as with decrementing the sensory data proportion on misuse detection subsystem with rate of $\triangle R = 0.25\%$.

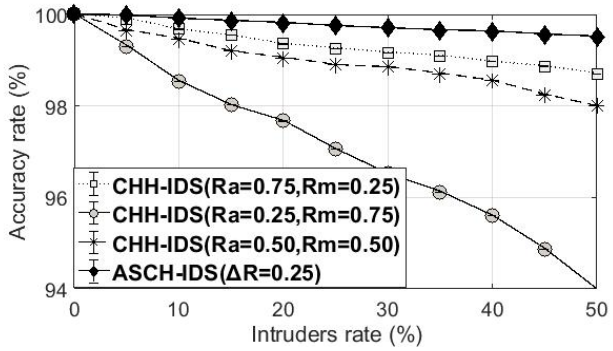

Fig. 3. Accuracy rates of CHH-IDS under fixed 0.75-0.25, 0.25-0.75 and 0.5-0.5 $R_a - R_m$ distribution for Anomaly and Misuse Detection Subsystems (ADS)(MDS), compared to ASCH-IDS with $\triangle R$ = 0.25. By keeping track of the ROC in the anomaly and misuse detection subsystems to adaptively adjust the proportion of sensory data, ASCH-IDS improves the accuracy significantly.

Detection Rate (DR) represents the ratio of sensor behavior that is truly recognized as intrusive. In other words, it represents the True Positive (TP) ratio as shown in Eq. (13) where FP refers to False Positive. DR for different data proportions scenarios has been traced in order to expect the system performance with them as shown in Fig.(4). Fig. 4 illustrates the DRs for the anomaly detection subsystem, misuse detection subsystem, CHH-IDS and the proposed Adaptive-CHH-IDS. The proposed ASCH-IDS – as a result of the adaptive decision making by tracking the ROC behavior in each subsystem – leads to the highest DR in detecting the intrusive behavior sensors when compared to each of the individual anomaly detection subsystem and misuse detection subsystem.

$$DR = \frac{TP}{TP + FP} \tag{13}$$

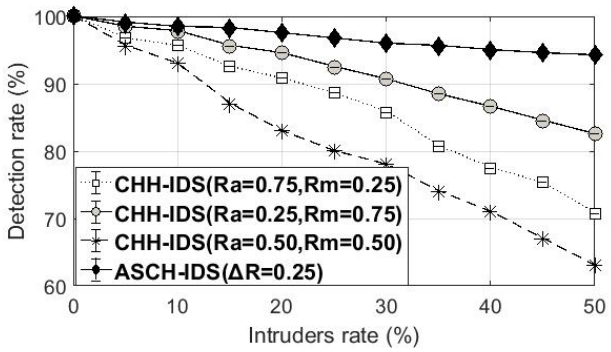

Fig. 4. Detection rates of CHH-IDS under fixed 0.75-0.25, 0.25-0.75 and 0.5-0.5 $R_a - R_m$ distribution for Anomaly and Misuse Detection Subsystems (ADS)(MDS), compared to ASCH-IDS with $\triangle R$ = 0.25. By keeping track of ROC in the anomaly and misuse detection subsystems to adaptively adjust the proportion of sensory data, ASCH-IDS improves the detection rate significantly.

Another conclusion that can be made from Fig. 4 is that the DR performance decreases by incrementing the data proportion on the anomaly detection subsystem as well as by decrementing the directed data proportion on misuse detection subsystem.

Receiver Operating Characteristic (ROC) curve characterizes the relationship between TP (Sensitivity) and FP (1-Specificity) for diverse cut-off points. Sensitivity versus specificity adjustment performance denoted by the area under the curve such that better performance is represented by larger area. ROC curves have been plotted for different scenarios in order to test the system performance with different proportional adjustment of sensor data as shown in Fig. 5. According to ROC curves, setting $\triangle R$ at 0.25, the overall performance can be improved effectively.

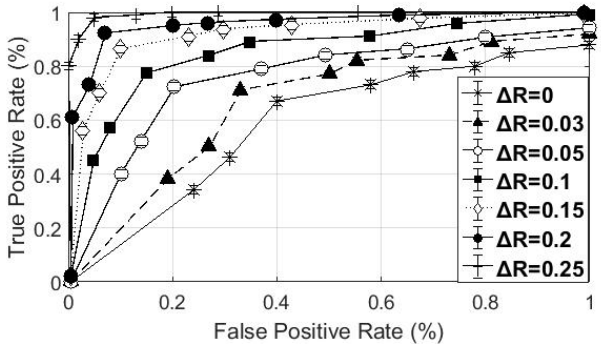

Fig. 5. ROC curve for different $\triangle R$. Area under the curve is the largest when $\triangle R$ is set to 0.25.

Precision-Recall rate curve is presented in Fig. 6 where recall and precision are formulated as $TP/(TP + FN)$ and $TP/(TP + FP)$, respectively. High recall and high precision are required to achieve high performance. Therefore the closer the precision-recall rate to one, the better the system performance [25]. Figure 6 shows that ASCH-IDS with $\triangle R = 0.25$ achieves a relatively high precision to recall ratio compared to other proportional adjustment of sensor data (i.e. other $\triangle R$ values). Therefore, setting $\triangle R$ at 0.25 achieves highly effective performance with a recall of 99.8%, and a precision of 90.1%.

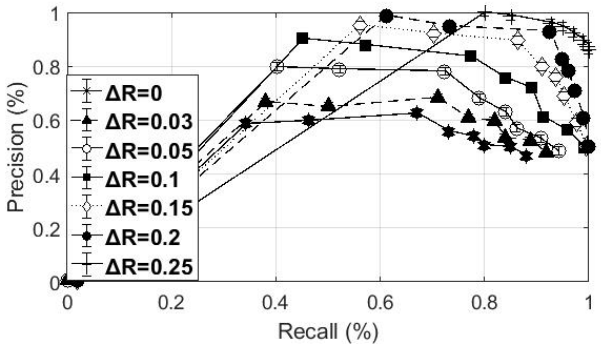

Fig. 6. Precision - Recall for different $\triangle R$

V. Conclusion

We have proposed Adaptively Supervised and Intrusion-Aware Data Aggregation for Wireless Sensor Clusters in Critical Infrastructures. The proposed scheme is called Adaptively Supervised Clustered and Hierarchical IDS (ASCH-IDS). ASCH-IDS adopts the previously proposed Clustered Hybrid and Hierarchical IDS (CHH-IDS) which consists of Misuse and Anomaly Detection subsystems. ASCH-IDS dynamically adjusts the proportions of sensory data directed to the ADS and MDS based on an indicator that keeps track of the receiver operating characteristic (ROC) behavior in each subsystem. The predecessor, CHH-IDS exhibits a detection rate and accuracy trade-off depending on the sensor data proportion forwarded to one of the two subsystems. The proposed ASCH-IDS undertook the intrusion problem by using adaptation strategy using different data proportions on ADS and MDS to detect dynamically known and unknown intrusions via unsupervised and supervised machine learning techniques, respectively. Thus, the adjustment on the data proportions lead to adapting the probability of calling supervised (or unsupervised) learning to detect intrusive behavior. We have evaluated the performance of ASCH-IDS through simulations and demonstrated that the proposed method performs with $\approx 99\%$ detection rate and $\approx 99.80\%$ accuracy in the presence of known and unknown malicious behavior in the WSN. Furthermore, we have pursued an empirical study on the ROC curve of the ASCH-IDS under various step values to increment/decrement the sensory data on a subsystem. We have shown that setting the incremental/decremental step value aggressively to 25% can ensure the best performance.

We are currently working on the implementation of fast optimization models to find the optimal sensory data distribution between the subsystems under varying conditions. Furthermore, we are investigating the impact of heterogeneous cluster sizes on the performance of our proposed solution.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation under Grant CNS-1647135 and in part by the Natural Sciences and Engineering Research Council of Canada Discovery under Grant 1056.

References

[1] S. Otoum, B. Kantarci, and H. T. Mouftah, "Hierarchical trust-based black-hole detection in wsn-based smart grid monitoring," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[2] S.Otoum, B. Kantarci, and H. T. Mouftah, "Mitigating false negative intruder decisions in wsn-based smart grid monitoring," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, June 2017, pp. 153–158.

[3] A. M. Chandrasekhar and K. Raghuveer, "Intrusion detection technique by using k-means, fuzzy neural network and svm classifiers," in *2013 International Conference on Computer Communication and Informatics*, Jan 2013, pp. 1–7.

[4] A. George, "Article: Anomaly detection based on machine learning: Dimensionality reduction using pca and classification using svm," *International Journal of Computer Applications*, vol. 47, no. 21, pp. 5–8, June 2012.

[5] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, 2nd ed. Springer-Verlag New York, 2009.

[6] S. Otoum, B. Kantarci, and H. T. Mouftah, "Detection of known and unknown intrusive sensor behavior in critical applications," *IEEE Sensors Letters*, vol. 1, no. 5, pp. 1–4, Oct 2017.

[7] V. Fanibhare, V. Dahake, and S. Duttagupta, "Energy theft detection using amids and cryptographic protection in smart grids," in *2016 International Conference on Internet of Things and Applications (IOTA)*, Jan 2016, pp. 131–136.

[8] S. Grimaldi, M. Gidlund, T. Lennvall, and F. Bara, "Detecting communication blackout in industrial wireless sensor networks," in *2016 IEEE World Conference on Factory Communication Systems (WFCS)*, May 2016, pp. 1–8.

[9] P. Diefenderfer, P. M. Jansson, and E. R. Prescott, "Application of power sensors in the control and monitoring of a residential microgrid," in *2015 IEEE Sensors Applications Symposium (SAS)*, April 2015, pp. 1–6.

[10] X. Wang and Q. Liang, "Efficient sensor selection schemes for wireless sensor networks in microgrid," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–9, 2017.

[11] K. Jayshree and R. S., "Intrusion detection using data mining approach," *International Journal of Science and Research (IJSR)*, vol. 3, no. 11, pp. 1142–1145, 2014.

[12] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," in *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, Sept 2017, pp. 000 277–000 282.

[13] N. Nokuthala Penelope Mkuzangwe and F. Nelwamondo, "A fuzzy logic based network intrusion detection system for predicting the tcp syn flooding attack," 01 2017, pp. 14–22.

[14] B. Subba, S. Biswas, and S. Karmakar, "A neural network based system for intrusion detection and attack classification," in *2016 Twenty Second National Conference on Communication (NCC)*, March 2016, pp. 1–6.

[15] J. Straub, "Testing automation for an intrusion detection system," in *2017 IEEE AUTOTESTCON*, Sept 2017, pp. 1–6.

[16] A. Honig, A. Howard, E. Eskin, and S. Stolfo, "Adaptive model generation: An architecture for deployment of data mining-based intrusion detection systems," in *IN*. Kluwer Academic Publishers, 2002, pp. 153–194.

[17] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An accurate security game for low-resource iot devices," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381–9393, Oct 2017.

[18] F. Belabed and R. Bouallegue, "An optimized weight-based clustering algorithm in wireless sensor networks," *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2016.

[19] W. Zhang, S. Das, and Y. Liu, "A trust based framework for secure data aggregation in wireless sensor networks," *IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, 2006.

[20] D. Ma and A. Zhang, "An adaptive density-based clustering algorithm for spatial database with noise," *IEEE Intl Conf on Data Mining (ICDM'04)*.

[21] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," *IEEE Trans. on Systems, Man, and Cybernetics, Part C*, vol. 38/5, p. 649659, 2008.

[22] "Random forests, leo breiman and adele cutler." [Online]. Available: http://www.stat.berkeley.edu/ breiman/RandomForests/

[23] "ns-3 tutorial." [Online]. Available: https://www.nsnam.org/docs/tutorial/html/

[24] "Kdd cup 1999 data." [Online]. Available: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[25] H. E. M. Elhamahmy and I. A. Saroit, "A new approach for evaluating intrusion detection system," in *Artificial Intelligent Systems and Machine Learning*, vol. 2, November 2010, pp. 290–298.