Sensor networks

Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications

Safa Otoum*, Burak Kantarci**, and Hussein T. Mouftah†

School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada
**Student Member, IEEE*
***Senior Member, IEEE*
†Life Fellow, IEEE

Manuscript received June 20, 2017; revised July 30, 2017; accepted September 8, 2017. Date of publication September 14, 2017; date of current version September 28, 2017.

Abstract—This article presents a hybrid architecture to identify intrusive behavior among networked sensors that monitor critical systems such as environment, medical, and smart grid. Monitoring through sensors is desired for critical applications such as epilepsy seizures, pollution, power quality assessment, and transformer monitoring. Wireless sensors are being widely used in critical applications due to their advantages including low-cost, flexibility, and communication efficiency. However, when sensors are networked to monitor a critical infrastructure such as the smart grid, they become the target of different types of attackers such as intruders via the communication medium. In order to maintain sensing in a secure manner, robust architectures are needed to identify intrusive behavior of sensors in a network. In this article, we present a hybrid architecture to detect intrusive behavior of sensors for both unknown and known intruders. The former requires anomaly detection, whereas the latter requires signature detection. The proposed architecture consists of two subsystems that co-operate to detect unknown and known attacks through duty-cycling of enhanced density-based spatial clustering of applications with noise and random forest methods. Through various tests on real intrusion data, we show that the proposed architecture has a strong potential to detect both known and unknown intrusive behavior of sensor nodes as the results show 99.73% detection rate with 98.95% overall accuracy.

Index Terms—Sensor networks, networked sensors, critical infrastructure sensing, security, intrusion detection, wireless sensors.

I. INTRODUCTION

Various types of sensors, such as magnetic, thermal, humidity, and pressure sensors, can be used in monitoring the healthiness of critical systems such as public safety, medical and smart grids [1], [2]. Lately, sensor networks have been used in smart grids as a critical infrastructure because of their flexibility, self-deployment features and low-cost [3]–[6]. Reliability and efficiency of the monitored critical infrastructures like smart power grid can be achieved by secure and reliable data aggregation and transmission of sensed data. Under such settings, sensors, as well as communication lines that interconnect sensors are vulnerable to various cyberattacks and particularly to intrusion that can interrupt the communication and manipulate the transmitted sensed data between the end points and distribution links. In addition to the protection techniques such as authentication and encryption on sensor data, intrusion detection is also essential for all-inclusive security of sensor networks to automatically detect different types of intrusions.

In this article, we propose a Hybrid-Intrusion Detection System (H-IDS) architecture that consists of two subsystems, namely the signature detection and anomaly detection subsystems. The former uses the supervised Random Forest (RF) algorithm [7] for known intrusive behavior whereas the latter uses E-DBSCAN to identify unknown intrusive behavior [8]. In order to avoid drawbacks and consolidate the advantages of these two methods, the Hybrid Intrusion Detection System (H-IDS) architecture enables both subsystems to duty cycle in order to identify an anomaly or possible misbehavior at any sensor in the networks. The proposed architecture implements a hierarchical trust-based aggregation of sensed data which undergoes one of the two subsystems. We evaluate the performance of the proposed method by using real intrusion data which prepared by ACM KDD'99 [9] on simulations. ACM KDD'99 presents a dataset that was generated from the Defense Advanced Research Projects Agency (DARPA) was prepared by ACM KDD'99 (special interest group on Knowledge Discovery and Data mining 1999 contest). Our results show that by letting anomaly detection and signature detection subsystems work in parallel, the detection rate can be enhanced up to 99.73%, while the accuracy reaches to 98.95%.

II. BACKGROUND AND MOTIVATION

Significant number of studies have adapted data mining techniques in their intrusion detection solutions for sensor networks [10], [11]. Some of these works addressed known attacks while the others addressed the unknown attacks. There are several challenges in both anomaly and signature detection, one of the challenges is the imbalance intrusion. Some intrusions such as Denial of Service (DoS) have more connections than other intrusion types such as the User to Root (U2R) intrusion [7]. Any data mining approach can potentially decrease the error rate regardless of intrusion types [7]. The authors in [12] used the specification-based intrusion detection technique for a secure medical sensing system where the patient's safety is

Corresponding author: Safa Otoum (e-mail: sotoum@uottawa.ca).
Associate Editor: R. Maeda.
Digital Object Identifier 10.1109/LSENS.2017.2752719

1949-307X © 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

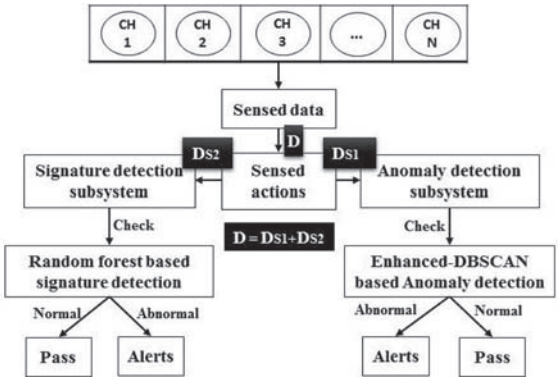

Fig. 1. Proposed hybrid-intrusion detection system (H-IDS) architecture.

Table 1. Notations Used in the System Model

Simulation parameter	Value
T_{agg}	Aggregator trust value
T_{agg}, n	Trust evaluation between node n and aggregator
T_n	Node n trust value
Var	Number of variables for each node
rec	Number of records for each variable
Tr	number of trees

the vital object. In [13], the authors proposed a hybrid intrusion detection framework based on random forest and k-means methods. The proposed system checks anomalies and analyzes signatures individually. In [14], the authors combined anomaly and misuse detection and proposed an integrated detection model in which they adopted Adaboost algorithm with hierarchical structures for anomaly detection of nodes. To the best of our knowledge, there is no definite detection method of intruders in sensor networks combining RF-based signature and E-DBSCAN-based anomaly detection.

III. PROPOSED SYSTEM MODEL

We consider a clustered sensor network that consists of a central server and N clusters each consisting of M sensors. In each cluster, the Cluster Head (CH) assumes the responsibility of data aggregation and transmitting the aggregated data to a central server. Each sensor node forwards its detected data to its CH. Our proposed framework consists of three modules: 1) CH selection module [15], 2) trust-based data aggregation module [16], and 3) detection of intrusive sensors via anomaly and signature detection subsystems, as illustrated in Fig. 1. As seen in the figure, the aggregated traffic passes through the intrusion detection module which consists of two subsystems that operate in duty-cycled fashion. Among these, anomaly detection subsystem aims to detect the unknown attacks on sensors whereas the signature detection subsystem aims to detect the known attacks. In Table 1, we present the notation that is used in the presentation of the system model, and the proposed scheme.

Once the sensed data is completely aggregated, it is distributed over the two detection subsystems following a time-slotted method such that the first X frames undergo anomaly detection, whereas the following Y frames undergo signature detection.

The signature detection subsystem in the proposal employs the random forest algorithm as a supervised classification method to detect known attacks on the sensors [17]. The random forest algorithm is a classification technique that consists of a collection of tree-organized classifiers, in which each tree casts a unit vote for the most popular class at each input [9].

On the other hand, the anomaly detection subsystem employs the Enhanced-DBSCAN (E-DBSCAN) algorithm as a clustering technique. DBSCAN is a density clustering algorithm that regards clusters as dense regions of objects in the data space which are separated by regions of low density objects [8]. DBSCAN is a clustering algorithm responsible for finding clusters starting from the nodes density distribution.

It is worth mentioning that CH selection in Fig. 1 is followed by trust-based data aggregation prior to distribution between the anomaly and signature detection subsystems. The trust-based aggregation method used in our tests is based on (1) where T_{agg} stands for aggregator trust value, T_n denotes node n trust value, in a cluster of k sensors. This method is based on the trust evaluation between each CH and its corresponding nodes inside each cluster. It starts with finding out the trust values of each node, each CH and the evaluation between both [16]

$$T_{agg} = \left(\sum_{n=1}^{k}(T_n + 1) * T_{agg}, n\right) / \left(\sum_{n=1}^{k}(T_n + 1)\right). \quad (1)$$

As the proposed system to detect intrusive sensor behavior consists of two subsystems, its runtime complexity is a function of the complexities of the other two algorithms. The time complexity of Random Forest can be extracted from decision tree complexity while random forest considered as a special model of decision trees. The complexity, C for building decision tree with r records and v variables is formulated in

$$\boldsymbol{C\ (Var,\ rec) = O(Var + rec\, log\, (v))}. \quad (2)$$

In building our random forest, the number of trees at the first step is Tr whereas the number of variables for each node is Var. $C1'$ is the complexity to build a single tree as defined in (3), shown below. By introducing multiple trees, the total complexity $C1$ translates into (4), shown below. When $O(\log(v))$ is assumed as the tree depth, the $C1$ can be formulated as in (5):

$$C1'\ (\text{single tree}) = O\,(\text{Var} * \text{rec}\log\,(\text{Var})) \quad (3)$$

$$C1'\ (\text{multitree}) = O\,(\text{Tr} * \text{Var} * \text{rec} * \log\,(\text{Var})) \quad (4)$$

$$C1'\ (\text{multitree}) = O\,(\text{Tr} * \text{Var} * \text{rec} * \text{depth})\,. \quad (5)$$

In the second subsystem where E-DBSCAN is run, the complexity -denoted by $C2$ is directed by the number of region query requests.

One query is performed for each point which gives a total runtime complexity of $O(n) < (n.\log(n))$ [18].

In our analysis and simulation of E-DBSCAN, we found the following executions steps: 1) The initialization step executed one time, 2) the comparison step takes place $(m + 1)$ times, and 3) the incremental step is executed (m) times. Thus, following [8] and [19], the $C2$ can be formulated as in

$$C2 = O\ (2 + (2m)) = O\,(m)\,. \quad (6)$$

The overall runtime complexity of the system to detect intrusive sensors can be calculated by $O((\text{Tr} * \text{Var} * \text{rec} * \text{depth}) + (2 + (2\ \text{m})))$. This leads to the complexity of $O(\text{Tr} * \text{Var} * \text{rec} * \text{depth})$ if $c.\,(\text{Tr} * \text{Var} * \text{rec} * \text{depth}) > (2 + 2\ \text{m})$ for constant c.

Table 2. Simulation Settings

Simulation parameter	Value
Number of nodes	20
Number of clusters	4
Routing protocol	H-DSR
Packet size	250 bytes
Communication range	100 m
Simulation time	300 s
Operational area	100 m × 100 m
Sensor types	Temperature sensors
Trust range	[0,1]
Attack Types	Defined in KDD CUP'99 Dataset

IV. PERFORMANCE EVALUATION

We evaluate the performance of the proposed system via simulations under ns-3. We have considered a network of 20 sensors that sense thermal data and adopt the Hierarchical-Dynamic Source Routing (H-DSR) protocol [19]. The sensors are spread out in a 100 m × 100 m area and make four clusters. We run each simulation scenario 10 times, and present the average of these runs with 95% confidence level. These can also be observed in Table 2.

A. Accuracy Rate (AR)

The accuracy rate is the first performance metric we have used to evaluate the proposed Hybrid Intrusion Detection System (H-IDS) on critical infrastructure sensors. Accuracy rate refers to the percentage of the correctly classified instances, which are also denoted by True Positives (TP) and True Negatives (TN) [20] as shown in (7). FN and FP are the False Negative and False Positive cases, respectively.

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}). \quad (7)$$

Fig. 2 illustrates the accuracy rates for the anomaly detection subsystem, signature detection subsystem, and the overall Hybrid Intrusion Detection System (H-IDS) on the sensors. As shown, the hybrid model achieves the highest accuracy rate of 98.95%. Anomaly detection achieves better overall accuracy rate since signature detection achieves less accuracy rates. On the other hand, signature detection subsystem helps in increasing the overall detection rate, as shown in the next subsection.

B. Detection Rate (DR)

The detection rate denotes the ratio of sensor behavior that is truly classified as intrusive. In other words, detection rate denotes the true positive ratio as formulated in (8), shown below, where FP and TP are the False Positive and True Positive cases, respectively.

$$\text{DR} = \text{TP} / (\text{TP} + \text{FP}). \quad (8)$$

Fig. 3 illustrates the detection rates for the anomaly detection subsystem, signature detection subsystem, and the overall Hybrid Intrusion Detection System (H-IDS) on the sensors. The proposed hybrid model leads to the highest detection rate in detecting the sensors that are in intrusive behavior when compared to each of the individual anomaly detection and signature detection subsystems. Since anomaly detection results lead to the lowest detection rate, incorporation of the signature detection subsystem via random forest helps in improving the detection rate.

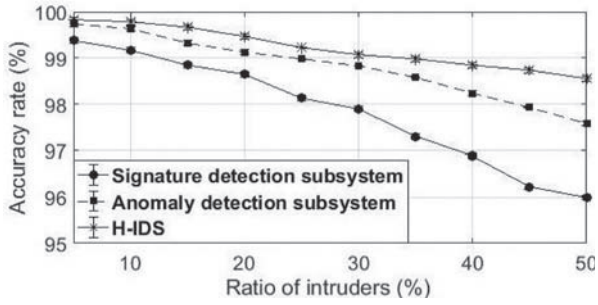

Fig. 2. Accuracy rate under the signature and anomaly detection subsystems, and H-IDS.

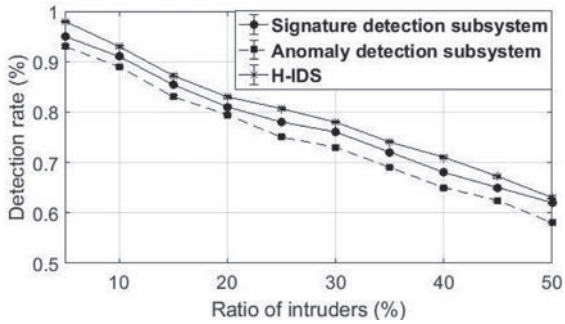

Fig. 3. Detection rate under the signature and anomaly detection subsystems and H-IDS.

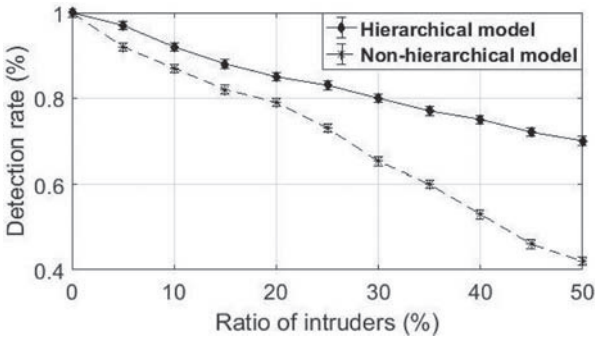

Fig. 4. Detection rate under hierarchical and non-hierarchical topologies.

C. Impact of Clustering Sensors

We also seek the benefit of using hierarchical network topology through clustering sensors. To implement a non-hierarchical topology, the system in Fig. 1 is slightly modified by appointing every sensor as the cluster head of a one-node cluster.

As seen in Fig. 4, by clustering in a hierarchical topology, the detection rate under a non-hierarchical solution can be reduced by 6% (under 5% intruder ratio) and by >45% (under 50% intruder ratio). The reason for this behavior is that the hierarchical topology enables trust evaluation for the cluster heads which results in trust score-based data aggregation. Thus, the sensed data that undergoes the H-IDS has already been fused with a certain trust score.

D. False Negative Rate (FNR)

False Negative (FN) refers to the percentage of intrusive sensor behavior, which has inaccurately been classified as non-intrusive, as formulated in (9), shown below, where FN, FP, TN, and TP are the

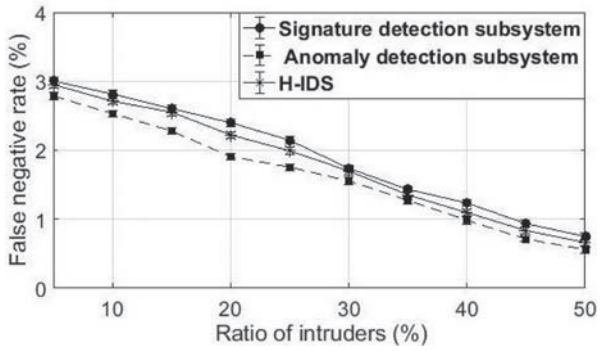

Fig. 5. False Negative rate under the signature and anomaly detection subsystems and H-IDS.

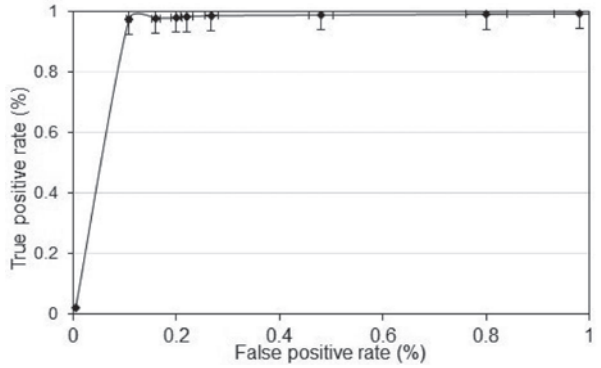

Fig. 6. Receiver operating characteristic (ROC) curve for H-IDS.

False Negative, False Positive, True Negative and True Positive cases respectively.

$$\mathrm{FNR} = \mathrm{FN}/\left(\mathrm{TP} + \mathrm{FN} + \mathrm{FP} + \mathrm{TN}\right). \tag{9}$$

FN is used to define a network's failure to detect intrusive sensor behavior under certain situations. In other words, malicious activity originated by the sensors are not detected or alarmed although and an alert should have been raised. In our tests, we set 0.5 of data to be directed to the anomaly detection subsystem while the other 0.5 is directed to the signature detection module. The FN based on this setting is shown in Fig. 5. By integrating anomaly detection with signature detection, the overall false negative rate has been reduced when compared to the case under the signature detection subsystem as anomaly detection via E-DBSCAN algorithm is capable of detecting unknown attacks which in turn can reduce FN intruder decisions on sensed data.

Fig. 6 presents the Receiver Operating Characteristic (ROC) curve which represents the relationship between the TP rate (Sensitivity) and the FP rate (1-Specificity) for different cut-off points. The larger the area under the curve, the better the sensitivity versus specificity trade-off performance is. Hence, it also confirms that the proposed H-IDS is capable of providing accurate detection.

V. CONCLUSION

In this article, we have proposed a new hybrid method to detect sensors that are in intrusive behavior while monitoring a critical infrastructure. The proposed methodology consolidates the advantages of anomaly-based and signature-based intrusion detection, and uses a trust-based hierarchical framework to aggregated sensor data. In the intrusion detection system, the anomaly detection subsystem employs a random forest model whereas the signature detection subsystem employs E-DBSCAN clustering. Through simulations, we have shown the effectiveness of the proposed approach by injecting real attack patterns into wirelessly networked sensors. The overall accuracy of our model can achieve a success ratio of 98.95% with up to 99.73% detection rate. False Negatives (FNs) may lead to severe consequences in such settings; however, our proposed solution can also reduce FNs that occur under the solely employed anomaly detection mechanism.

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, M. Ahmed, and H. T. Mouftah, "Sensor medium access control (SMAC)-based epilepsy patients monitoring system," in *Proc. 28th Canadian Conf. IEEE Electr. Comput. Eng.*, 2015, pp. 1109–1114.

[2] K. Lin, T. Xu, J. Song, Y. Qian, and Y. Sun, "Node scheduling for all-directional intrusion detection in SDR-Based 3D WSNs," *IEEE Sensors J.*, vol. 16, no. 20, pp. 7332–7341, Oct. 2016.

[3] E. Al-Shaer and M. A. Rahman, *Security and Resiliency Analytics for Smart Grids*. New York, NY, USA: Springer, 2016.

[4] T. Islam, S. C. Mukhopadhyay, and N. K. Suryadevara, "Smart sensors and internet of things: A postgraduate paper," *IEEE Sens. J.*, vol. 17, no. 3, pp. 577–584, Feb. 2017.

[5] G. C. Koutitas and L. Tassiulas, "Low cost disaggregation of smart meter sensor data," *IEEE Sens. J.*, vol. 16, no. 6, pp. 1665–1673, Mar. 2016.

[6] Y. Liu, C. Cheng, T. Gu, T. Jiang, and X. Li, "A lightweight authenticated communication scheme for smart grid," *IEEE Sens. J.*, vol. 16, no. 3, pp. 836–842, Feb. 2016.

[7] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," *IEEE Trans. Syst., Man, Cybern. Part C, Appl. Rev.*, vol. 38, no. 5, pp. 649–659, Sep. 2008.

[8] D. Ma and A. Zhang, "An adaptive density-based clustering algorithm for spatial database with noise," in *Proc. 4th Int. Conf. IEEE Data Mining*, 2004, pp. 467–470.

[9] Lincoln Laboraroty, "DARPA intrusion detection evaluation," Lincoln Lab., Mass. Inst. Technol., Lexington, MA, USA.

[10] T. Xinguang, D. Miyi, S. Chunlai, and L. Xin, "Detecting network intrusions by data mining and variable-length sequence pattern matching," *J. Syst. Eng. Electron.*, vol. 20, no. 2, pp. 405–411, Apr. 2009.

[11] B. Mirkin and R. Amorim, "Minkowski metric, feature weighting and anomalous cluster initializing in K-Means clustering," *Pattern Recognit.*, vol. 45, no. 3, pp. 1061–1075, 2012.

[12] R. Mitchell and I. R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan. 2015.

[13] R. M. Elbasiony, E. A. Sallam, T. E. Eltobely, and M. M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," *Ain Shams Eng. J.*, vol. 4, no. 4, pp. 753–762, 2013.

[14] X. Sun, B. Yan, X. Zhang, and C. Rong, "An integrated intrusion detection model of cluster-based wireless sensor network," *Plos One*, vol. 10, no. 10, Aug. 2015, Art. no. e0139513.

[15] S. Otoum, B. Kantraci, and H. T. Mouftah, "Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring," in *Proc. Int. Conf. IEEE Commun.*, 2017, pp. 1–6.

[16] J. Hur, Y. Lee, S. Hong, and H. Yoon, "Trust-based secure aggregation in wireless sensor networks," in *Proc. 3rd Int. Conf. Comput., Commun. Control Technol.*, 2005, vol. 3, pp. 60–69.

[17] L. Breiman and A. Cutler, "Random forests," [Online]. Available: http://stat-www.berkeley.edu/users/breiman/RandomForests/cc_home.htm, Univ. Calif., Berkeley, CA, USA.

[18] C. Kruskal, L. Rudolph, and M. Snir, "A complexity theory of efficient parallel algorithms," *Theor. Comput. Sci.*, vol. 71, no. 1, pp. 95–132, 1990.

[19] M. Tarique, K. E. Tepe, and M. Naserian, "Hierarchical dynamic source routing: Passive forwarding node selection for wireless ad hoc networks," in *Proc. Int. Conf. IEEE Wireless Mobile Comput., Netw. Commun.*, 2005, vol. 3, pp. 73–78.

[20] M. Abdulrazaq and A. Salih, "Combination of multi classification algorithms for intrusion detection system," *Int. J. Sci. Eng. Res.*, vol. 6, no. 1, pp. 1364–1371, 2015.