Review on the development and future trend of the intrusion detection system (IDS)

Tingyang Sun
Jinan University, China
Jiahao Zhang
Jinan University, China
Yumeng Yang
Internet of Things Engineering， Computer Department Chongqing University, China

Abstract—**Invasion of attack technology and detection technology in a certain extent, is promote each other, in order to accurately and effectively detect known and unknown attacks, with superior algorithm in intrusion detection system and technology, mainly is the artificial intelligence technology, mobile agent technology, data fusion associated with information technology. The research is undertaken on the analysis of the existing technology, on the basis of review of research, the development trend of intrusion detection system (IDS development lay the foundation for subsequent theory. The author want to analysis technology including, but not limited to the following several aspects: (1) the information fusion technology. Fusion is the process of different sensors, low level of the relativity of warning according to certain algorithm into a higher level of warning information, which will help to solve the problem of false positives and omission. The fusion process is a huge, huge noise detection information detection and extraction of target process; (2) the evolution mechanism of the simulation. Through the analysis of existing bionic algorithm that is the immune algorithm, tabu search algorithm, artificial fish algorithm and its application in Intrusion Detection Systems; (3) the mobile agent technology. Detection method based on agent is very powerful, it allows the intrusion detection system based on agent to provide a combination of anomaly detection and misuse detection ability.**

Keywords: ***wireless sensor network, novel intrusion detection system with Huddling Engine & Synthetic resistant system (NIDSwHE&SRS), Artificial Immune System*.**

I. INTRODUCTION

Not at all like common systems, remote sensor systems not just expect to encourage the steady viability of self-arranging sensor hubs with low power, for example with expanded lifetimes, additionally have astute actuators. The actuators improve the agreeable exertion of sensor hubs to convey while transmitting information in regions including wellbeing, fighting and environment checking. For example, wellbeing observing models embrace remote sensors as unprecedented parts to constantly catch quantitative information from a colossal amount of wearable body device systems for more periods. An Amalgam Sensor Network design utilized sensors for the front line, which are talented in following attractive weapon signals produced by adversary powers. The latest production by exhibiting how strong fuzzy rationale is in occasion detection by checking smoke by means of temperature sensors connected all through the home-based situation; fire explosion may hence be distinguished, making the importance of device applications obvious. Current request outlines for remote sensors manage the cost of more noteworthy adaptability in building up correspondences and expansion system mechanization, however need in security and protection. The center shortcomings with these sensor hubs lie in the constrained asset gadgets, which are power and handling units. Consequently, weakness to different security dangers is strikingly high. In the meantime, a foe has aloof and dynamic capacities. It might ensnare sensor hubs through access to mystery data, for example, keys put away in the bargained hub notwithstanding the possibility to listen in and adjust, for example, replay, produce, alter and erase uncovered nodal conduct. In relieving security entanglements, conventional security strategies, for cases, firewall and cryptography are elective alternatives to anticipate outside interlopers. Fundamentally, they are illogical in totally turning away system assets from progressively modern inner assaults. An alternate safekeeping method fuses IDPS to distinguish and block interruption by pretenders [1]. Three detection techniques utilized are abuse, inconsistency, and the mixture model which is a mix of the initial two strategies. An abuse based system recognizes known examples by coordinating watched information utilizing straightforward standards.

Peculiarity based detection alludes to the finding of abnormal examples in estimation information that don't comply with the normal conduct [3]. As needs be [6], an inconsistency based arrangement deflects intrusion progressively systems by breaking down convention based assaults movement. The crossover detection approach supports the capacities of a present WIDPS by combining dual shrewd techniques for abuse and oddity. Scientist planned a cross breed Intrusion Detection Systems by fusing the bundle header inconsistency detection and system activity oddity detection systems, which are irregularity, based Intrusion Detection Systems with abuse based Intrusion Detection Systems Snort. The key idea driving the half and half detection is that abuse distinguishes known assaults while peculiarity finds obscure assaults. While conventional intrusion detection methodologies, for example, abuse, abnormality and half and half show generally sensible execution with respect to right uncovering of recognized assaults and untruthful alert rates, they neglect to identify obscure assaults. Hence, an oddity

detection methodology is considered as another option to recognize continually changing obscure assault conduct, yet it might likewise display great untruthful optimistic results contrasted and abuse detection, which is viewed as wasteful. Counterfeit consciousness (AI) systems assume a part in computerizing the interruption discovery procedure to decrease social intermediation. The identifying interference procedure in view of the customary computerized reasoning involves strategies, for example, fuzzy set and transformative figuring, which work as classifiers for peculiarity uncovering. In spite of the fact that these guidelines apply spread known examples, they can't adjust to the assaults' example changes. To ease the issue of assault changes, computational knowledge is viewed as a high-exactness detection technique to be utilized as a part of developing a smart detection show and to naturally recognize conflicting exercises. The outcome was more prominent security, yet the vitality productivity issues stayed to be tended to.

Hub based Intrusion Detection and Prevention Systems screens system movement, specifically arrange fragments or gadgets, after which it dissects system and convention behavior to distinguish suspicious exercises. Host Intrusion Detection and Prevention Systems watch all or bits of, the dynamic conduct and condition of a PC system. Not at all like Node Intrusion Detection and Prevention Systems which powerfully reviews system parcels, Host based Intrusion Detection and Prevention Systems identifies projects' entrance and assets. Host based IDPS offers the benefit of being anything but difficult to convey without influencing existing bases instead of Node based IDPS which distinguishes assaults at the vehicle convention layer through speedy reactions.

Inconsistency based intrusion detection systems have been extensively inquired about as cautious strategies to discourse the discovery of obscure assaults. Not at all like abuse based or mark based sorts of Intrusion Detection Systems, which exploit the foreordained mark of known assaults, inconsistency based Intrusion Detection Systems manages the recognition of novel sorts of assault that are obscure to the scheme. The procedures are finished through identifying variety in the schemes conduct from a formerly characterized ordinary system profile. Be that as it may, it is liable to false cautions as an aftereffect of the trouble in characterizing the ordinary state amid preparing. An expanding detection rate with less false cautions turned into an imperative test in the configuration of oddity based Intrusion Detection Systems. The counterfeit resistant system includes promising methods as naturally enlivened figuring that is connected to taking care of different issues in the data safety arena. The Artificial Immune System is motivated by the social resistant method, which can recognize inside cells and particles of the body from remote microorganisms, alleged self/non-self separately, secures the form against maladies. The human Insusceptible System, that is present in the human body is most part does this deprived of any earlier information of assaulting their construction. As self/non-self-separation is noteworthy property in Artificial Immune System, it is recommended that it is used in outlining productive oddity based Intrusion Detection Systems [2] and [4]. The Artificial Immune System recommends a multi-layered security structure for ensuring PC systems against assault, similar to HIS assurance against outside microorganisms in the human [5]. This assurance is refined completed Adaptive systems. Characteristic resistance is prompt; it is the principal line of safeguard for the human Insusceptible system and gives non-particular insurance. In this way, it has no earlier information of particular outcasts. The versatile invulnerable reaction, then again, is antigen-particular and is prepared utilizing a pre-characterized outline of particular assaults. Versatile safety likewise incorporates a reminiscence that makes reactions against a particular antigen more productive [7].

Like other peculiarity based detection methods, the Artificial Immune System additionally exploits observing varieties of the system's conduct as per a pre-characterized ordinary movement profile as a versatile resistant instrument. Consequently, the effectiveness of oddity detection in the Artificial Immune Systems is very subject to the information set. Generous exploration has been directed so far in the change and use of Artificial Immune System - based Intrusion Detection Systems, dominant part of which have used a pre-characterized along with disconnected information set as learning information for preparing the Intrusion Detection Systems. The proficiency will get diminished of the Intrusion Detection Systems by constraining its knowledgebase to that specific information set. In addition, it is to a great degree hard to make an information set of self-specimens with all varieties. Keeping in mind the end goal to adapt to this issue, in this original copy, the creator have proposed an inalienable resistant instrument by utilizing unconfirmed learning strategies are the principal streak of safeguard in Artificial Immune System based Intrusion Detection Systems.

The inborn insusceptible structure of the proposed engineering gives operational and dynamic order of the system streams to self as well as non-self. It is then utilized by the versatile invulnerable method to create assault particular finders. Machine learning (ML) strategies can be sorted out in light of the kind of information accessible amid preparing. Nearby are tri fundamental classes of ML: administered, semi-regulated and unconfirmed calculations. Managed ML calculations should prepared by the named information to recognize the ordinary and irregular conduct in system. Semi directed ML calculations can be prepared by assault allowed unlabeled information. The procurement marked information as of safekeeping specialists, or discovering assault free information groups for equally administered along with semi-regulated systems, is excessive. Late revisions demonstrated the possibility of unconfirmed learning methods in Intrusion Detection Systems in correlation with regulated learning based Intrusion Detection Systems [8].

Unsubstantiated ML systems plan the undetectable edifice of unlabeled information that has been set in short of any earlier learning. Grouping calculations put objects in view of their similitudes into a bunch or groups. Bunching calculations have been utilized for unsupervised Intrusion Detection Systems to characterize the conduct of the system [9]–[10].

II. RELATED WORK

The human safe system safeguards the human in contradiction of destructive and beforehand inconspicuous outside chambers utilizing lymphocyte cells. Cells that are outside are called antigens, for example, microorganisms and infections. The Synthetic resistant system (SRS) is intended for the computational method and roused by the human Insusceptible system. It is connected to taking care of different issues that were in arena of data security, IDS [11], [12]. Besides, it joins numerous qualities of the Human Insusceptible system that comprises of differences, mistake resilience, self-motivated learning, and amendment along with self-observing. Artificial Immune System has ability to separate amongst the identities that are the cells that are claimed by the method and non-identity that are the outside elements to the system as intrusions. In like manner, locators are conveyed in the system hubs to catch and bang any pernicious exercises. Human Insusceptible system utilizes a negative choice procedure to create full grown invulnerable system cells called Dcells.

Analyst proposed a negative choice calculation to use this procedure of the Human Insusceptible system aimed at a modern inconsistency detection procedure. The current procedure permits the detection of beforehand concealed destructive cells without any meaning of particular hurtful cells. The calculation incorporates three stages: characterizing self, creating locators and observing the event of inconsistencies. In the main stage, it builds up the typical conduct examples of an observed method to characterize 'identity'. It views the summarized ordinary examples as ‘identity’ examples. In the additional stage, it produces various youthful T-cells with random examples that are contrasted with every self-design characterized in the primary stage. In the event that any created design coordinates a self-example, the example neglects to wind up an indicator and is in this manner evacuated. Else, it turns into a full grown T-cell identifier and is used for checking consequent profiled examples of the observed system. Amid the next stage, if a T-cell indicator coordinates any recently profiled design, it is viewed as that that new inconsistency more likely than not happened in the observed system.

Scientist [13] set forward another connection amongst natural and processing sciences by proposing the manufactured immunology model. [14] Proposed the best thought in the usage of resistance in PC safety for self/non-self-segregation. So far various structures have been displayed in the use of the Artificial Immune System for Intrusion Detection Systems. Be that as it may, there are basically two principle ways to deal with applying Artificial Immune System. Unique methodology is traditional self along with non-self-segregation and additional is the use of a threat hypothesis as a additional aimed at the previous. A negative determination calculation is proposed to separate amongst self and non-self-substances. The calculation first makes an arrangement of finders randomly and then contrasts it and an arrangement of typical sets (self). On the off chance that any locators are coordinated with any self-element, the Hazard Model was proposed [15], [16]. As indicated by this theory the primary driver of an insusceptible reaction is that a microorganism damages system and in this manner it perilous to the system.

Specialist expressed that in Intrusion Detection Systems worldview the threat is detected and measured consequently after various intrusions in light of the harm created by the assault. Once a threat sign is recognized, it will be transmitted to the closest simulated immune response around the risk range [17].

In a multifaceted arrangement comprising of discovery, safeguard along with client sheets has been projected. A model was proposed in which the essential resistant reaction is advanced through hereditary calculation to an auxiliary safe reaction with improved identifiers that are journalist to memory cells (MC) in common safe systems. In the past research, the creator upgraded the current structure by suggesting a conveyed structure to lessen the preparing overheads and to build the proficiency of Intrusion Detection Systems [19]. Besides, the disseminated way of this model brought about a more noteworthy self-change highlight for this Intrusion Detection Systems. This work, in any case, uses disconnected learning information for preparing the Intrusion Detection Systems. Since the system conduct is altered in self-motivated design, another profile of typical and strange action should be prepared to the system progressively [18]. Keeping in mind the end goal to take care of this issue, in this original copy the creator have proposed an inalienable insusceptible instrument by usage of unsubstantiated learning.

Specialists have connected unsupervised machine learning calculations in Intrusion Detection Systems to conquer the issues of preparing and recognizing new assaults. Case in point, a viable continuous arrangement was proposed for Node Intrusion Detection Systems to identify known and obscure system assaults utilizing unsupervised neural systems. They connected a few neural systems to enhance the detection rate of intrusions [20] [21]. An unsupervised Node Intrusion Detection Systems was proposed, which utilizes distinctive bunching calculations to recognize assaults, for example, DOS/DDOS, Worm and Network checking. A tree-based subspace bunching method was displayed for unsupervised Node Intrusion Detection Systems in great information sets. It has been produced in the proposed method and broken down group solidness for every bunch by utilizing an outfit of

different group records. They have additionally presented a multi-target bunch marking strategy to name every steady group as ordinary or atypical.

III. Proposed Intrusion Detection System- novel intrusion detection system with Huddling Engine & Synthetic resistant system (NIDSwHE&SRS)

Figure 1 demonstrates projected novel interference discovery system that comprises of two primary motors which is known as the novel intrusion detection system with Huddling Engine and Synthetic resistant system (NIDSwHE&SRS). The Huddling Engine (HE) performs system activity bunching into the self as well as the non-self-groups through unsupervised learning methods. The Synthetic resistant system (SRS) motor comprises of operators that participate for intrusion detection. The expression "operator" initially originates since Synthetic Intellect and alludes to everything that can see in surroundings over sensors along with follow up on the atmosphere utilizing actuators. The term specialist alludes to programming operators in the current manuscript. Contrasted with the past work, in our past work the creator proposed a circulated model novel intrusion detection system with Huddling Engine and Synthetic resistant system (NIDSwHE&SRS) in which the creator tested expanded execution and productivity of these IDs as an aftereffect of a more prominent self-change rate contrast with a brought together structure. This is because of era of innovative reminiscence cells along with self-motivated organization and dissemination to all hosts, and along these lines an upgraded optional safe reaction. The Synthetic resistant system (SRS) motor prepares the essential identifiers created by the negative determination calculation in light of got data from the Huddling Engine. Also, it enhances the execution of essential finders as indicated by the intrusion report investigation as of all the hosts. In the design, the parcel preprocessing module is in charge of separating a few traits from the system movement to make system streams.

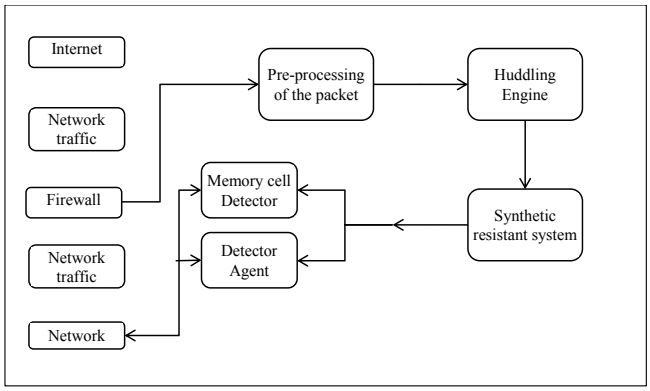

Figure 1. Proposed novel intrusion detection system with Huddling Engine & Synthetic resistant system (NIDSwHE&SRS) system architecture.

Synthetic resistant system (SRS) - based Intrusion Detection Systems: In the Artificial Immune System motor, the creator proposed three operators to utilize the versatile insusceptible reaction of the Synthetic resistant system (SRS) in Intrusion Detection Systems. Preparing specialist: first changes over the system stream data into the parallel string with an aggregate 100 piece extent as a stream contour. At that point, utilizing the negative determination calculation it creates and prepares the essential finders. The negative choice calculation first produces various random indicators and then prepares them with tests of marked streams from the bunch motor. In the event that each juvenile identifier coordinates every self-specimen of information set, another is created by disposing the earlier one. In the wake of checking every youthful indicator with every self-specimen, the rest of the locator sets experience the following stride of the negative determination calculation and get to be full grown finders. Each experienced locator will be crisscrossed with entire non-self-examples of marked streams.

Undesirable segment calculation utilizes the r-Contiguous coordinating piece part in order to form the coordinating amongst dual sequences. In the current strategy, two strings are coordinated in the event that they have at any rate r bordering indistinguishable bits. At last, the yield of the negative determination calculation is an arrangement of essential identifiers, which are chronicled and coordinated indicator set archive and it is then directed to contributor operator for dispersion to the nearby. The identifiers are comparable to essential safe reaction in the human insusceptible system.

Correspondent operator: appropriates indicators from the locator established to all hosts that are in system. Additionally, it has the duty to speak through all entity and bring into line them as indicated by alterations in identifier set. It additionally advances the stated stream as of the reminiscence cell locators and indicator operators to the analyser specialist.

Choice process is attempted on enacted finders to choose the locators with most elevated fondness for duplicating along with development of essential populace for hereditary calculation. The finders having a wellness esteem more prominent than or equivalent to cloning limit experience cloning. This procedure is rehashed and proceeded for a couple of eras until a locator with a wellness esteem higher than all victor identifiers is created. The advanced identifier from the hereditary calculation is dealt with as memory cell.

Host Adjacent Gauges: with a specific end goal to enhance the execution of Intrusion Detection Systems, identifiers are disseminated in all hosts in the system as opposed to an incorporated structure. Additionally, the novel intrusion detection system with Huddling Engine and Synthetic resistant system (NIDSwHE&SRS) appropriated

methodology is vigorous. Totally incoming and outbound system streams are tested utilizing the locators. In every host, the creator considers two identifiers as takes after. Finder operators: contain an arrangement of prepared indicators that can segregate amongst self along with the non-self-streams. The locators were non-particular and in charge of essential insusceptible reaction for peculiarities that happen interestingly. On the off chance that a stream matches a locator with a successful liking, that finder is viewed as an actuated identifier and the stream is suspected as an intrusion. In order to enhance precision of finding and lessen the false-positive blunders in Intrusion Detection Systems, the creator have characterized an intrusion edge.

MC indicators: made out of an arrangement of upgraded locators produced by the analyser specialist. As the optional reaction of the Synthetic resistant system (SRS), MCs need additional precise intrusion detection capacities. Subsequently, some stream that initiates whichever the indicators is dealt with as an intrusion.

Locator Life Cycle and Non-self-Updater: with a specific end goal to keep up the proficiency of identifiers, the creator proposes to characterize a lifespan to dispense with unused or frail indicators. Because of ML blunders, there is plausibility that a portion of the created locators have deficient detection capacity and continually incapacitated amid their lifetime. Such indicators have negative overheads to the system and lessen its execution. Thusly, keeping in mind the end goal to take care of this issue the creator characterizes a lifespan for all indicators, amid which the quantity of times the identifier is enacted is tallied.

IV. EXPERIMANTAL OUTCOMES

To assess the productivity of two prevalent grouping calculations, the creator used KDD-'99 information set. The quantity of tests of information set was 5000, which was adequate for playing out the assessment and correlation between thicknesses based grouping and K-implies. The parameter qualities were acquired in a progression of preparatory tests. The accomplished aftereffects of K-means and thickness based grouping calculations are acquired. the creator have measured parameters such as the FPR, TNR, Precision which evaluated by isolating the aggregate effectively grouped positives and negatives by the aggregate number of tests, Recall which assessed by partitioning the accurately identified oddities and the aggregate number of abnormalities, positive anticipated worth which assessed by separating the accurately ordered positives by the aggregate anticipated positive tally and at long last the score that is said to be the weighted normal of the exactness and review. In this test, because of capacity of thickness based bunching for finding self-assertively molded group, this calculation showed a superior rate of detection contrasted with K-mean. In our trial the greater part of the parameters for the system activity edge are gotten naturally and the creator just set as 10.

Figure 2 thinks about the self-change rate of Synthetic resistant system (SRS) based Intrusion Detection Systems in focal and disseminated modes. As indicated by this outline, the self-change rate in circulated mode is superior to anything unified mode and it compasses to its steady greatest sum after just 5 circles. This generally happens in the 20 rounds in incorporated mode.

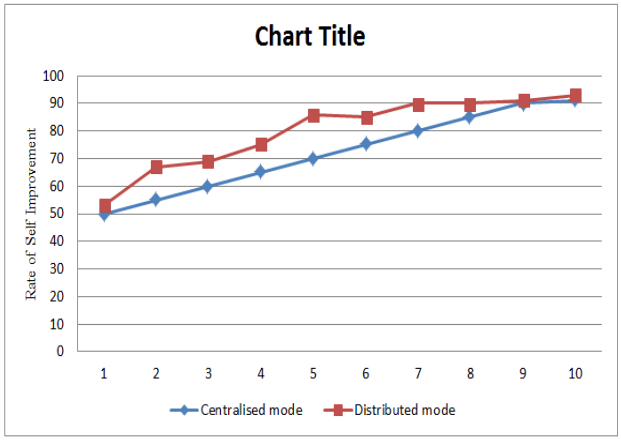

Figure 2. Comparison of rate of self-improvement in distributed and centralized mode.

V. CONCLUSION

In this manuscript, the creator displayed a novel engineering for an intrusion detection system in view of the Synthetic resistant system (SRS). The creator proposed novel intrusion detection system with Huddling Engine and Synthetic resistant system (NIDSwHE&SRS) characteristic invulnerability utilizing unsupervised machine learning strategies. As per our essential examinations the creator infers that among different strategies, thickness based grouping bunching is hearty and has the best potential for this reason. In this multi-layered structure, the Huddling Engine marks the system activity as self and non-self without past preparing or information about system stream profiles, along these lines going about as the principal line of guard in Synthetic resistant system (SRS)-based Intrusion Detection Systems and giving characteristic insusceptibility. The creator characterized a system estimation recipe as a dynamic edge to encourage the detection of anomalous system practices. The yield of bunching is utilized to encourage the preparation information for the versatile insusceptible system as online and ongoing preparing information. Essential identifiers in the wake of preparing are appropriated to has in the system and give essential safe reaction to our Intrusion Detection Systems. The creator exhibited the test aftereffects of proposed novel intrusion detection system with Huddling Engine and Synthetic resistant system (NIDSwHE&SRS) natural insusceptible instrument

utilizing our system estimation recipe. The creator additionally showed that the circulated structure for these Intrusion Detection Systems is more effective than the concentrated mode. Suspected intrusions reported from hosts are examined and an upgraded memory cell finder is produced through a hereditary calculation process. Memory cells are assault particular identifiers, which give an auxiliary insusceptible reaction. The creator characterized indicator life cycle to upgrade and dispense with feeble or wasteful locators to improve the execution of detection.

REFERENCES

[1] Anuar,N.B., Papadaki, M., Furnell, S., Clarke, N., 2012. Incident prioritisation using analytic hierarchy process (AHP): RiskIndex Model (RIM).SecurityComm. Networks,doi:10.1002/sec.673.

[2] Blasco, J.,Orfila, A., Ribagorda, A., 2010. Improving network intrusion detection by means of Domain-Aware genetic programming. In: International Conferenceon Availability,Reliability,andSecurity,pp.327–332.

[3] Curiac, D.-I., Volosencu, C., 2012. Ensemble based sensing anomaly detection in wireless sensor networks.Exp.Syst.Appl.39,9087–9096.

[4] Devarakonda,N.,Pamidi,S.,Kumari,V.V.,Govardhan,A.,2012.Integrated Bayes network and hidden Markov model for host based IDS. Int.J.Comput.Appl.41,45.

[5] Doelitzscher, F., Reich , C., Knahl , M., Passfall, A., Clarke, N., 2012. Anagent based business aware incident detection system for cloud environments. J.Cloud Comput. Adv.Syst.Appl.1,9.

[6] Dutkevych,T., Piskozub, A., Tymoshyk, N., 2007. Real-time intrusion prevention and anomaly analyze system for corporate networks. In: Fourth IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IEEE,pp.599–602.

[7] F. Hosseinpour, K. A. Bakar, A. H. Hardoroudi, and N. Kazazi, “Survey on Artificial Immune System As a Bio-inspired Technique for Anomaly Based Intrusion Detection Systems,” in Proceedings of the 2010 International Conference on Intelligent Networking and Collaborative Systems, 2010, pp. 323–324.

[8] Fisch, D., Jänicke, M., Kalkowski, E., Sick, B., 2012. Learning fromothers: exchange of classification rules in intelligent distributed systems. Artif. Intell,http://dx.doi. org/10.1016/j.artint.2012.04.002.

[9] Fragkiadakis,A.,Tragos,E.,Tryfonas,T.,Askoxylakis,I.,2012.Design and performance evaluation of alight weight wireless early warning intrusion detection prototype. J. Wireless Commun.Network2012,1–18.

[10] Hanson, M.A., Powell, H.C., Barth, A.T., Ringgenberg, K., Calhoun, B.H., Aylor, J.H., Lach, J., 2009. Body are a sensor networks: challenges and opportunities. Computer 42,58–65.

[11] Herrero, Á., Corchado, E., Pellicer, M.A., Abraham,A., 2009. MOVIH-IDS:a mobile visualization hybrid intrusion detection system. Neuro computing72, 2775–2784.

[12] Hosseinpour F., Meulenberg A., Ramadass S., Vahdani Amoli P., and Z. Moghaddasi, “Distributed Agent Based Model for Intrusion Detection System Based on Artificial Immune System,” Int. J. Digit. Content Technol. its Appl., vol. 7, pp. 206–214, 2013.

[13] Khan, S.A., Daachi, B., Djouani, K., 2012. Application of fuzzy inference systems to detection of faults in wireless sensor networks. Neurocomputing 94,111–120.

[14] Khanna,R.,Huaping,L.,Hsiao Hwa, C., 2009. Reduced Complexity Intrusion Detection in Sensor Networks Using Genetic Algorithm, International Conference onCommunications.IEEE,Dresden,pp.1–5.

[15] Kolias,C.,Kambourakis,G.,Maragoudakis,M.,2011.Swarmintelligenceini ntrusion detection: asurvey.Comput.Secur.30,625–642.

[16] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “An Effective Unsupervised Network Anomaly Detection Method,” in Proceedings of the International Conference on Advances in Computing, Communications and Informatics, 2012, pp. 533–539.

[17] P. Casas, J. Mazel, and P. Owezarski, “Unsupervised Network Intrusion Detection Systems: Detecting the Unknown Without Knowledge,” Comput. Commun., vol. 35, no. 7, pp. 772–783, Apr. 2012.

[18] S. and G. G. Feixian, “Research of Immunity-based Anomaly Intrusion Detection and Its Application for Security Evaluation of E-government Affair Systems.,” JDCTA Int. J. Digit. Content Technol. its Appl., vol. 6, no. 20, pp. 429 – 437, 2012.

[19] Wang H, Wang J. An Effective Image Representation Method Using Kernel Classification[C]// IEEE International Conference on Tools with Artificial Intelligence. IEEE, 2014:853-858.

[20] Wang J, Wang H, Zhou Y, et al. Multiple Kernel Multivariate Performance Learning Using Cutting Plane Algorithm[C]// IEEE International Conference on Systems, Man, and Cybernetics. IEEE, 2015.

[21] Bi C, Wang H, Bao R. SAR image change detection using regularized dictionary learning and fuzzy clustering[J]. 2014:327-330.