Volume: 10 Issue: 04 Pages: 3925-3937 (2019) ISSN: 0975-0290

Survey of Intrusion Detection Techniques and Architectures in Wireless Sensor Networks

Rakesh Sharma
Research scholar, Department of Computer Science &Engg., I. K. Gujral Punjab Technical University, Jalandhar, Punjab, India
Email: rakeshsharma3112@gmail.com
Vijay Anant Athavale
Professor, Department of Computer Science & Engg., Gulzar group of Institutes, Khanna, Punjab, India
Email: vijay.athavale@gmail.com

ABSTRACT

Advances in electronics and wireless communication technologies have enabled the development of large-scale wireless sensor networks (WSNs). However, WSNs practice from lots of constraints, with low computation capability, small memory, limited energy resources, vulnerability to physical capture, and the need of infrastructure, which enforce lonely security challenges mostly for the applications where confidentiality has key significance. There are diverse applications for wireless sensor networks, and security is very major issue for several of them. Before attackers can damage the WSN system (i.e., sensor nodes) and/or information destination (i.e., data sink or base station) in order to work WSNs in a secure way, any sort of intrusions should be detected.

Keywords - **Intrusion detection, IDS, security, wireless sensor network, WSN.**

Date of Submission: Sep 08, 2018 Date of Acceptance: Nov 29, 2018

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are useful to a variety of fields due to their simple and contemptible use features. To accumulate surrounding information regarding human behavior and activities, such as health care, military observation and exploration, highway traffic; to supervise physical and ecological phenomena, such as ocean and wildlife, earthquake, pollution, wild fire, water quality; to monitor industrial sites, such as building safety, manufacturing machinery performance, and so on [1]. Securing WSNs is critically important issue. Security attacks against WSNs are categorized into two major groups: Active and Passive. In passive attacks, attackers are typically secret (unseen) and moreover tap the message link to accumulate data; or tear down the performance elements of the network. Eavesdropping, node broken, node tampering/ destruction and traffic analysis types are passive attacks. An adversary essentially affects the operations in the attacked network in active attacks and this may be the reason of the attack and can be detected. For instance, the networking services may be corrupted or ended as a result of these attacks. Various types of active attacks are group into jamming, hole attacks (blackhole, wormhole, sinkhole, etc.), Denial-of-Service (DoS), flooding and Sybil types.

Intrusion is a legitimate activity in a network that is moreover achieved passively or actively. In a security system, if the initial systems of defense, “Intrusion Prevention,” do not avoid intrusions, after that the succeeding system of protection, “Intrusion Detection,” will act. It is the finding of some doubtful manner in a system performed by the network members so in any security issue, Intrusion Detection Systems (IDSs) present some or all of the following information to the other supportive systems: detection of the intruder, position of the intruder (e.g., solitary node or district), instance (e.g., date) of the intrusion, intrusion activity (e.g., active or passive), intrusion type (e.g., attacks such as worm hole, black hole, sink hole, selective forwarding, etc.), layer where the intrusion occurs (e.g., physical, data link, network). This information would be very helpful in mitigating and remedying the cause of attacks, as much defined information concerning the intruder is obtained. So, intrusion detection systems are essential for network security. WSNs have exclusive distinctiveness such as inadequate power supply, low transmission bandwidth, small memory size and data storage. WSNs have some general security goals such as confidentiality, integrity, data origin Authentication, Entity Authentication, Access control and availability. In addition, WSNs have precise security objects (1) Forward secrecy: preventing a node from decrypting any upcoming secret messages after it leaves the network. (2) Backward secrecy: preventing a joining node from decrypting any previously transmitted secret message. (3) Survivability: on condition that a certain level of service in the attendance of failures. (4) Freshness: ensuring that the data is new and no adversary can repeat old messages. (5) Scalability: sustaining a vast number of nodes. (6) Efficiency: storage, processing and communication boundaries on sensor nodes must be measured.

This paper is organized as follows: in section 2, intrusion detection systems are described. Section 3 presents various types of existing ids architectures for intrusion detection in WSN. In section 4, various challenges to ids deployment in WSN and section 5 conclude the paper.

II. INTRUSION DETECTION SYSTEMS (IDSS)

Any kinds of illegitimate or unapproved behavior in a network or a system will be considered as intrusions. An Intrusion Detection System (IDS) is a set of the tools, methods, and resources to facilitate distinguish, evaluate, and description intrusions. Intrusion detection is largely defense system that is installed in the region of a system or device and it is not an individual safety measure [2]. Intrusion is defined as: "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" and intrusion prevention techniques in [3], (such as encryption, authentication, access control, secure routing, etc.) are accessible as against intrusions. IDSs are forever measured as a subsequently wall of defense from the security point of analysis. As mentioned in [3], the likely prepared necessity of IDSs is given as: "low false positive rate, intended as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected". Intruders to a network can be classified into two types' external intruder and internal intruder. (1) External intruder: An outsider using diverse means of attacks to arrive at the network. (2) Internal intruder: A compromised node that used to be an associate of the network.IDS can detect both external and internal intruders, but internal intruders are harder to detect. This is due to that internal intruders have the necessary keying resources to counteract any protection taken by the authentication mechanisms. Intrusion can be of any type such as attempted break, Masquerade, Penetration, Leakage, DoS and Malicious use. IDSs may provide partial detection solution to those attacks. But of course, all system administrators would like to have perfect IDS that would able to detect all of the intrusions listed above [4], [5], [6]:

Based on deployment, the IDS can be categorized into three types: host-based intrusion detection system (HIDS), network-based intrusion detection system (NIDS) and Hybrid Intrusion detection System.

Host based Intrusion Detection System (HIDS): HIDS is disturbed among the measures on the host with the purpose of them are working and they are able of detecting the following intrusions: changes to important system files on the host, numerous breakdown access attempts to the host, abnormal method memory allocations, unusual CPU activity or I/O activity. By monitoring the real-time scheme usage of the host or by investigative log files on the host HIDS achieves this.

Network based Intrusion Detection System (NIDS): NIDS can examine a whole packet; payload inside the packet, IP addresses or ports either passively or actively by listens to the network transmissions.

Hybrid Intrusion Detection System: NIDS and HIDS system combine together form a Hybrid IDS and a well-organized way by the usage of the mobile agents. Mobile agents move to each host and perform system log file checks while a central agent checks the on the whole network traffic for the existence of anomalies.

Based on detection methodologies IDS can be classify as: anomaly based detection, misuse based detection, and specification based detection:

1) Misuse detection: In this case, the patterns have to be defined and given to the system and act or behavior of nodes is compared with well-known attack patterns. The disadvantages are that this method requests knowledge to build attack patterns and they are not able to sense novel attacks. Drawbacks of this approach is significantly reduce the efficiency in terms of system management, as the administrator of the network always has to offer IDS agents with an current database.

2) Anomaly detection: The approach prime describes the real features of a 'normal behavior', which are renowned by using automated training and this method does not search for exact attack patterns, but in its place it checks whether the behavior of the nodes can be measured as normal or anomalous. Then it flags any behavior that diverges from these behaviors as intrusions. The IDS would have high confidence to decide that the node is malicious if a sensor node does not act according to the distinct specification of a particular protocol; the wrong decisions made by IDS in terms of false positive and false negative alarms influence the accuracy of detection. The disadvantage of this method is that the system can illustrate valid but hidden behavior, which could show the way to a significant false alarm rate.

3) Specification-based detection: It is paying attention on discovering deviations from normal behaviors that are defined neither by machine learning techniques nor by training data as this method combines the aims of misuse and anomaly detection mechanisms. The specifications that describe what can be considered as normal behavior are defined manually and any action is monitored with respect to these specifications. The drawback of this approach is the manual development of all specifications, which is a time-consuming procedure for human beings and it cannot detect malicious behaviors which do not violate defined specifications of the IDS protocol. Sometimes misuse and anomaly-based detection techniques can be used that give birth to hybrid detection mechanisms.

III. WIRELESS SENSOR NETWORK INTRUSION DETECTION SYSTEMS

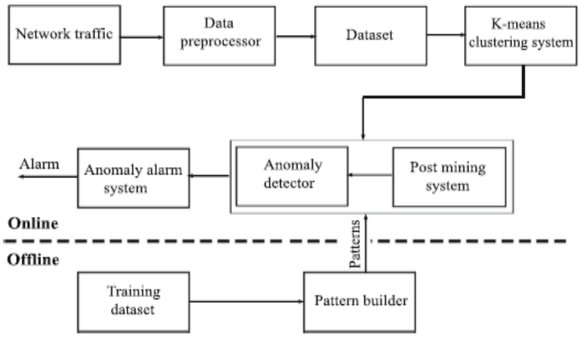
Noureddine Assad et al. (2015) propose a suitable probabilistic model which provides the coverage and connectivity in k-sensing detection of a wireless sensor network and also proved the capability of approach using a geometric analysis and a probabilistic model. The quality of deterministic deployment can be determined sufficiently by a rigorous analysis before the deployment and sensor deployment quality is a critical issue since it reflects the cost and detection capability of a wireless sensor network. However, when indiscriminate employment is required, determining the deployment quality becomes not easy. In the intrusion detection application, it is necessary to define more precise measures of sensing range, transmission range, and node density that impact overall system performance. They developed probabilistic models by deriving analytical expressions to differentiate the topological properties of network coverage/connectivity, designing and analyzing the intrusion detection probability and connectivity of network, with taking into report diverse parameters such as sensing range, transmission range, node density and node accessibility. The proposed model is investigated for intrusion detection in WSN to single-sensing/ multi-sensing detection and the connectivity in k-sensing detection of a WSN. The results enable the authors to design and analyze the homogeneous WSN, and help them to select the critical parameters of network in order to meet the WSN application requirements.

Michael Riecker et al. (2014) propose a lightweight, energy-efficient system, which makes use of mobile agents to detect intrusions based on the energy utilization of the sensor nodes as a metric. A linear regression model is applied to predict the energy consumption. They evaluate the proposed detection algorithm with regard to detection accuracy in a scenario with a flooding and a blackhole attack. They also study the influence of the history size and the walking strategies on the detection time. They neither require nodes to monitor their environment and collaborate with each other, nor do need to transfer audit data to a central point. Instead, use a mobile agent that collects energy readings and raises an alert if sudden changes occur. The feasibility of mobile agents used for intrusion detection in wireless sensor networks has been verified. The authors further showed that the energy consumption is a suitable metric to detect denial-of-service attacks. In simulations, they evaluated their proposed method for intrusion detection and were able to achieve high detection accuracy while maintaining a low false-positive rate.

Hussein Moosavi et al. (2014) suggest stochastic games with incomplete information in order to properly formulate and evaluate the intrusion detection difficulty in wireless sensor networks (WSNs). Security necessities of WSNs are taken into account to differentiate the game parameters and model the player objectives. To generalize the problem, the game data are assumed not to be fully known to the players, who take a robust optimization approach to address this data uncertainty and to assessing the validity and effectiveness of the framework, illustrative instances of the developed game model are generated. It is also shown; by numerical results that the robust approach in the presence of uncertainty reduces the sensitivity of the solution with respect to data perturbations, and thus improves design stability. Equilibrium analysis reveals how the inconsistent objectives of the intruder and intrusion detection system induce them to adopt different conservative instances toward data uncertainty. A nonzero-sum discounted robust stochastic game framework is developed to analyze the ID problem in WSNs. Equilibrium analysis of illustrative instances of the game demonstrates how the conflicting objectives of the players lead them to adopt different detection rates as per their conservative viewpoints on the uncertain game data. The numerical results also indicate that the robust stochastic game model, compared to its nominal counterpart, reduces the sensitivity of the solution to data perturbations and increases the design's stability. The uncertain parameters are assumed to be uniformly distributed, while real-world uncertainties may resemble a Gaussian distribution.

Mohammad Wazid et al. (2016) proposed a robust and efficient secure intrusion detection approach which uses the K-means clustering in order to extend the lifetime of a WSN. They propose a new intrusion detection technique for hybrid anomaly; K-means built patterns of attacks automatically over training data for the detection purpose. After that intrusions are detected by matching network activities against the detection patterns.

Figure 1 High-level description of hybrid anomaly detection scheme



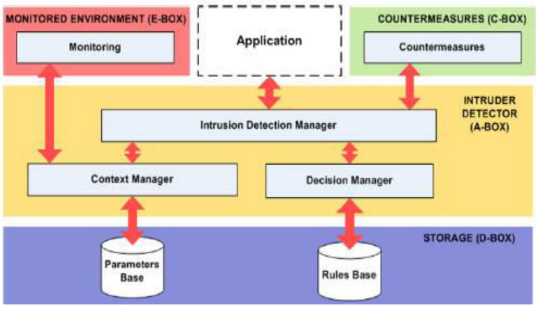
Source: Mohammad Wazid et al. (2016)

The authors assess the approach over a WSN dataset that is created using Opnet modeler, which contains a range of attributes, such as end- to- end delay, traffic sent and traffic received. The training dataset contains the normal values of the network parameters. The testing dataset is created in actual working mode consists of normal and abnormal values of the network parameters. Authors claim that proposed scheme achieves 98.6 % detection rate and 1.2 % false positive rate, which is better than the existing related schemes and the proposed technique has the ability to detect two types of malicious nodes: blackhole and misdirection nodes.

Helio Mendes Salmon et al. (2012) proposed the structure which is enlivened by Human Immune System (HIS) and the proposed system utilizes an enhanced decentralized and redid variant of the Dendritic Cell Algorithm (DCA). Which enables hubs to screen their neighborhood and team up for distinguish an intruder? Creators offered the design for a bland WSN IDS in light of the Danger Theory and the DCA, enlivened by the HIS was connected and altered for WSNs, where the sensors expected diverse parts from the highlights of HIS. Creators likewise listed different likenesses amongst HIS and WSN. The proposed IDS's activity stream is partitioned into four stages: (I)

Collection Phase; (ii) Analysis Phase; (iii) Decision Phase; and (iv) Reaction Phase. First and second stages are identified with DCA strategies, while the third stage is identified with lymph hub choice taking techniques. The fourth stage speaks to the versatile safe framework and its response against trespassers. Antigens and information signals are caught in the principal stage. In the second stage, input signs and antigens are examined to produce yield signals. These yield signals demonstrate DC development state. In the third stage, DCs exhibit and order the self and the non-self antigens, showing their level of variation from the norm. In the fourth and last stage, B and T cells start to deliver antibodies which will battle against a particular trespasser.

Figure 2 IDS Logical Architecture

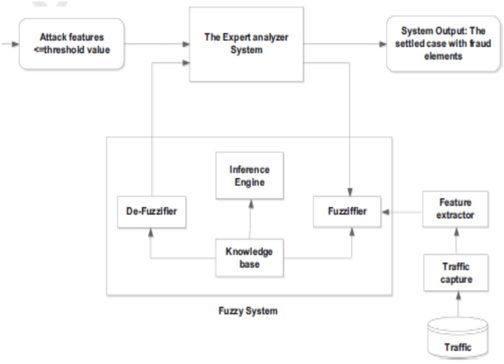


Source: Helio Mendes Salmon et al. (2012)

Authors do various trials to demonstrate the alignment of the proposed IDS and tried to meet the significance of the application running on the system, picking security to the detriment of sparing vitality or the other way around. Through these tests the IDS was turned out to be effective for WSNs. The memory assets outrageous by the distinctive parts played by the sensors were additionally examined. In the analyses, the proposed work with the previously mentioned strategies and other work, which utilized another hypothesis of HIS, called the Negative Selection Theory were looked at. This correlation demonstrated that, in spite of achieving lower estimations of rates of recognizable proof of the assault while it was happening (TP), the mistake rates created by the IDS amid an ordinary state of the framework were considerably littler (FP), demonstrating the effectiveness of the proposed altered calculation. The outcomes showed the effectiveness of the proposed IDS.

Shahaboddin Shamshirband et al. (2014) introduce the cooperative-based fuzzy artificial immune system (Co-FAIS). Co-FAIS are a modular-based defense strategy consequent from the danger theory of the human immune system. The agents synchronize and work with one another to calculate the irregularity of sensor behavior in terms of context antigen value (CAV) or attacker sand- up date the fuzzy activation threshold for security response.

Energy Figure 3 the architecture of the proposed Fuzzy Misuse Detector Module


Attack features <=threshold value
The Expert analyzer System
System Output: The settled case with fraud elements
Inference Engine
De-Fuzzifier
Fuzziffier
Feature extractor
Knowledge base
Traffic capture
Fuzzy System
Traffic

Source: Shahaboddin Shamshirband et al. (2014)

The sniffer module adapts to the sink node to audit data by analyzing the packet components and sending the log file to the next layer and the fuzzy misuse detector module (FMDM) integrates with a danger detector module to categorize the sources of danger signals. The infected sources are transmitted to the fuzzy Q-learning vaccination modules (FQVM) in order for particular, required action to enhance system abilities. The Cooperative Decision Making Modules (Co-DMM) incorporates danger detector module with the fuzzy Q-learning vaccination module to produce optimum defense strategies. To evaluate the performance of the proposed model, the Low Adaptive Clustering Hierarchy (LEACH) was simulated using a network simulator. The model was compared against other existing soft computing methods, such as fuzzy logic controller (FLC), artificial immune system (AIS), and fuzzy Q-learning (FQL), in terms of detection accuracy, counter-defense, network lifetime and energy consumption, to demonstrate its efficiency and viability. The proposed method improves detection accuracy and successful defense rate performance against attacks compared to conventional observed methods.

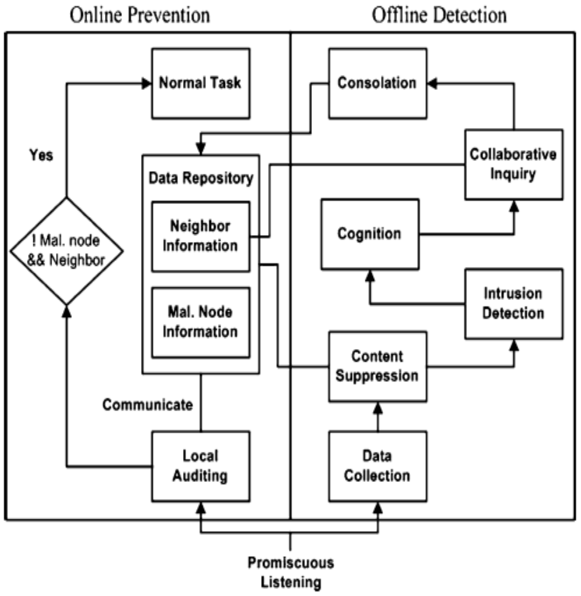
Sutharshan Rajasegarar et al. (2013) describes a distributed hyperspherical cluster based algorithm for identifying anomalies in measurements from a wireless sensor network, and an implementation on a real wireless sensor network test bed. The communication overhead incurred in the network is minimized by clustering sensor measurements and merging clusters before sending a compact description of the clusters to other nodes. An evaluation on several real and synthetic data sets demonstrates that the distributed hyperspherical cluster-based scheme achieves comparable detection accuracy with a significant reduction in communication overhead compared to a centralised scheme, where all the sensor node measurements are communicated to a central node for processing.

The effectiveness of the proposed approach is demonstrated using several real and synthetic data sets. Comparison to a centralised approach shows that this distributed approach can achieve significant reductions in communication overhead, while achieving comparable detection accuracy. Also, they provide a mechanism to select the parameter settings of the algorithm such that an appropriate trade-off between the detection accuracy and the communication overhead can be found. Authors claim proposed scheme is capable of identifying global anomalies at an individual node level. The evaluation on several real and synthetic data sets shows that the distributed approach achieves comparable detection performance to a centralised approach, while achieving a significant reduction in communication overhead.

Anil Kumar Sagar et al. (2015) analyzed the intruder detection probability with respect to network parameters such as sensing radius, node density. They also investigated the detection probability related to speed of intruder, availability of sensor nodes along with the time frame required to identify the intruder. In addition, they also discussed the k-detection probability to make the system more reliable. Furthermore, they developed the analytical framework for the expected hop count in multi-hop WSN. Simulations are performed using Matlab to investigate the intruder detection probability and hop count analysis for delivering the message to the destination. Proposed model can be used for analyzing the delay in message to reach the destination.

Ashfaq Hussain Farooqi et al. (2012) proposed, a novel intrusion detection framework securing WSNs from routing attacks. The proposed system works in a distributed environment to sense intrusions by collaborating with the neighboring nodes. It plant in two modes: online prevention allows protection from those abnormal nodes that are already stated as malicious while offline detection finds those nodes that are being compromised by an adversary throughout the next period of time.

Figure 4 Proposed intrusion detection frameworks



Source: Ashfaq Hussain Farooqi et al. (2012)

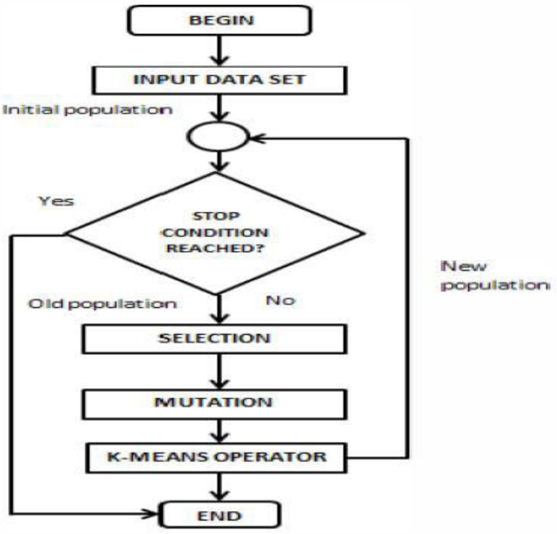
The foremost heart of the test is to provide an insight about centralized–distributed approaches (security systems in which monitor nodes analyze the network and communicate with the base station using any secure communication mechanism) and show that they do not figure out the actual condition of the network properly. The results show that if the node X sends the average value to the sink or base station to analyze the network whether it is in attack or not, it cannot figure out the actual scenario. But if the sensor node makes decision on its own and analyze the behavior of individual node, then it can detect the abnormal node efficiently. This shows that a centralized distributed approach cannot figure out the actual condition of the network properly. Therefore, a purely distributed security system is more appropriate for WNSs. The results show by authors shows that the specification-based detection scheme achieves higher detection rate and receives low false positive rate.

Ahmed Saeed et al. (2016) presented an intrusion detection mechanism by implementing an intelligent security architecture using Random Neural Networks (RNN). To validate the viability of the proposed security solution, it is implemented for an existing WSN system and its functionality is nearly verified by effectively detecting the occurrence of any apprehensive sensor node and irregular activity in the base station with high accuracy and minimal performance overhead. The effectiveness and overheads are evaluated by implementing the proposed IDM within the application running on the base station. The proposed IDM is mainly responsible to detect performance degradation attacks such as detection of unacceptable packets transmitted by a malicious sensor node with the endeavor to drain battery and unnecessary utilization of system resources (i.e base station transceiver). Any data corruption as the result of buffer overflow will also be detected by the proposed IDM as long as the application’s data memory is intact and program instructions are executing. As the sensor nodes are battery operated, the encryption maintain has been disabled to keep the power.

The efficiency of the proposed solution has been tested under unusual attack scenarios. To barely estimate these attack scenarios, placed a malicious sensor node in the range of base station. This malicious sensor node can transmit the packet containing more data as intended to receive or even transmitting packets containing invalid data. The length and format of data transmitted by valid sensor nodes is analyzed by placing another receiving node. Then the attacker sensor node starts transmitting its own packet leading to performance degradation and generating buffer overflow in the memory where the received data is being stored by the base station. In this way, the base station fails to execute the code in the correct manner. On the contrary, when the base station is protected with the proposed IDM, the security attacks are detected successfully and an alarm signal is generated for further action. The proposed IDM does not require dedicated hardware resources and presented negligible performance overhead with 10.45% increase in the power consumption and the feasibility of the proposed solution is verified for a WSN system, with the detection accuracy of 97.23%.

Sandhya G et al. (2014) present a conceptual framework for identifying attacks for intrusion detection by applying genetic K-means algorithm. The algorithm classifies instances to a pre-defined number of clusters. Intrusion detection systems include pattern analysis techniques to discover useful patterns of system features. These patterns illustrate user behavior. Anomalies are computed with the set of appropriate system features. The derived patterns comprise inputs of classification systems, which are based on statistical and machine learning pattern recognition techniques. Clustering methods are useful in detection of unknown attack patterns. Exclusion of unimportant features is critical for a simplified, faster and more accurate detection of attacks. Genetic algorithm based clustering offers identification of significant reduced input features and it is applied to differentiate normal and abnormal intrusion behavior and the rule base of intrusion detection is updated. Finally, a real-time intrusion detection rule base is set. Clustering helps in finding patterns in unlabeled data of many dimensions. The major advantage of clustering algorithm is the ability to learn from and detect intrusions in the audit data without explicit signatures. It can automatically detect groups of similar objects in data training. The Network Simulator ns-2.34 is used for implementing genetic k-means algorithm to detect intrusions in WSN using AODV protocol. The results show that high detection rate and low false positive rate are achieved, so makes the proposed methodology of detecting intrusions using genetic k-means algorithm more appropriate for dynamic environments.

Figure 5 Flowchart of implementing Genetic K-Means algorithm



Source: Sandhya G et al. (2014)

Shahaboddin Shamshirband et al. (2014) introduced a hybrid clustering method, namely a Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA). The Imperialist Competitive Algorithm (ICA) is adapted with a density-based algorithm and fuzzy logic for optimum clustering in WSNs. A density-based clustering algorithm helps to improve the imperialist competitive algorithm for the formation of arbitrary cluster shapes as well as handling noise. The fuzzy logic controller (FLC) assimilates to imperialistic competition by adjusting the fuzzy rules to evade possible errors of the worst imperialist action variety strategy. The proposed method aims to enhance the accuracy of malicious detection. D-FICCA is evaluated on a publicly available dataset consisting of real measurements collected from sensors deployed at the Intel Berkeley Research Lab and its performance is compared against existing empirical methods, such as K-MICA, K-mean, and DBSCAN. The results of the proposed framework demonstrated that it achieves higher detection accuracy 87% and clustering quality 0.99 compared to various existing approaches.

Guangjie Han et al. (2012) the authors propose a novel IDS based on energy prediction (IDSEP) in cluster-based WSNs. The key idea of IDSEP is to identify malicious nodes based on energy consumption of sensor nodes. Sensor nodes with abnormal energy consumption are identified as malicious ones. Moreover, IDSEP is designed to differentiate categories of ongoing DoS attacks based on energy consumption thresholds and compared with the existing IDSs, which primarily focus on monitoring behaviors of malicious nodes; IDSEP detects malicious nodes based on energy consumption. Additionally, IDSEP can distinguish categories of ongoing DoS attacks based on energy consumption rates of malicious nodes. They use Network Simulator-2 to evaluate performance of IDSEP. Simulation results show that the proposed IDSEP is more efficient than related work in detecting DoS attacks detects and recognizes malicious nodes effectively. The detection ratio of IDSEP is much higher than that of group-based intrusion detection.

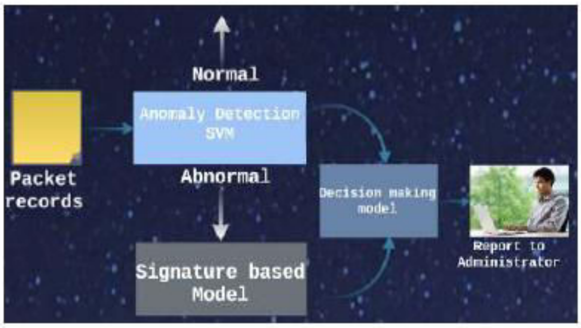
Maissa Elleuch et al. (2014) present an approach for the formal analysis of the detection performances of wireless sensor networks using the k-set randomized scheduling to preserve energy they formalized the notions of intrusion period, detection probability and delay using the measure theoretic formalization of probability theory in the HOL theorem prover. The obtained results are exhaustive and completely generic, i.e., valid for all parameter values; a result which cannot be attained in simulation or probabilistic model checking based approach. Furthermore, unlike most of the existing work that focuses on the validation of the functional aspects of WSN algorithms, the work is distinguishable by addressing the performance aspects. Finally, the proposed approach described by the authors can be generalized to tackle the formal analysis of the same randomized scheduling under other assumptions, or even other probabilistic problems in the WSN context. Indeed, the presented formalizations can be valuable for formally verify the same algorithm with, for example, a modified shape of the intrusion object. In addition, the higher-order-logic formalizations of some common random variables such as Bernoulli or Binomial can be very useful for the formal analysis of any probabilistic analysis problem.

Laura Gheorghe et al. (2013) propose a solution for protecting WSNs against internal attacks and faults by using a trust and reputation mechanism that relies on abnormal behavior detection. Trust mechanisms provide protection adjacent to broken down, malicious or uncooperative nodes. The computation of trust and reputation values takes into concern both historical values and the values determined in the current cycle. Trust is then computed from the historical trust and the recently computed reputation. The protocol includes three phases: the Learning phase, in which experience is computed based on these alerts received from TinyAFD, the Exchanging phase, in which experience relations are exchanged between neighbor nodes, and the Updating phase, in which trust and reputation are updated based on experience. ATMP has been implemented on top of TinyOS and has been tested using TOSSIM in several attack scenarios to evaluate the evolution of experience, trust and reputation. The protocol is adaptive because the trust and reputation values are modified in each cycle according to the alerts received from the TinyAFD and the protocol is collaborative because neighbor nodes exchange experience values in each cycle. Trust values can be used in routing protocols or aggregation mechanisms. Nodes with a low trust should be excluded from the network: their packets should not be routed and their sensor readings should not be aggregated. They performed a comparative evaluation of ATMP with other similar solutions and determined that their protocol covers a larger range of attacks, mostly because of the integration with a complex intrusion detection system. Evaluate the proposed solution and observe the evolution of experience, reputation and trust on the sensor nodes. Authors determined that reputation is decreased more slowly than understanding and more rapidly than trust. More importantly, the trust and reputation values disseminate more rapidly in the case in which malicious packets are not blocked by the detection framework. In comparison with other similar solutions, ATMP covers a larger range of attacks, because it uses the TinyAFD for anomalous behavior detection.

Masud Moshtaghi et al. (2014) propose a novel adaptive model for anomaly detection, as well as a robust method for modeling normal behavior. The evaluation results on both real-life and simulated data sets demonstrate the accuracy of approach compared to existing methods. Authors proposed an adaptive approach to create elliptical decision boundaries that adaptive model is used for anomaly detection in WSNs is proposed. They consider a data set collected within a given time window of samples in each sensor in a wireless sensor network. Initially, a small fraction of the above data is taken to model the initial data distribution at each sensor. They call this period the stabilization period that is compared with an earlier approach based on clustering ellipsoids, approach can achieve better results in non-homogeneous environments without adding extra load on the sensor nodes.

Yassine Maleh et al. (2015) propose a hybrid, lightweight intrusion detection system for sensor networks. The proposed Hybrid intrusion detection system (HIDS) takes advantage of cluster-based architecture to reduce energy consumption and this model uses anomaly detection based on support vector machine (SVM) algorithm and a set of signature rules to detect malicious behaviors and provide global lightweight IDS. The detection approach is integrated into a cluster-based topology to increase the network lifetime. This is achieved by designating one known node as a leader of the group (cluster-head) that forwards nodes packets (data aggregated) to the base station (BS) instead of sending their (nodes) collected data to a remote location (base station). Cluster head acts like a local base station sensor, and then clusters elect themselves to be a CH at any given time with a certain probability. They propose a cluster-based architecture that divides the array of sensors into a plurality of groups, each of which comprises a cluster-head (CH). In this architecture, every node belongs to only one of the clusters which are distributed geographically across the whole network.

Figure 6 IDS architecture



Source: Yassine Maleh et al. (2015)

Cluster head is used to reduce network energy consumption and to increase its lifetime. Simulation results show that the proposed model can detect abnormal events efficiently and has a high detection rate with lower false alarm. The combination of anomaly detection based on SVM and detection based on attack signatures allows the intrusion detection model to achieve a high rate of intrusion detection (almost 98%) with a number very reduces false alarms (near 2%). The performance of proposed intrusion detection model is evaluated using KDDcup'99 database.

Yun Wang et al. (2008) consider the issue of IDS according to two WSN models: homogeneous and heterogeneous WSN. Furthermore, they derive the detection probability by considering two sensing models: single-sensing detection and multiple-sensing detection and the network connectivity and broadcast reach-ability, which are necessary conditions to ensure the corresponding detection probability in a WSN. The simulation results validate the analytical values for both homogeneous and heterogeneous WSNs. The simulation is carried out for single-sensing and k-sensing detection models. The analytical and simulation results are compared by varying the sensing range, transmission range, node density, and node availability. In the simulation, sensors are deployed in accordance with a uniform distribution in a squared network domain. The simulation results verify the correctness of the proposed analytical model. This work provides insights in designing homogeneous and heterogeneous WSNs and helps in selecting critical network parameters so as to meet the application necessities.

Shahaboddin Shamshirband et al. (2013) suggest that Intrusion detection is best delivered by multi-agent system technologies and advanced computing techniques. The significance of the techniques and methodologies and their performance and limitations are additionally analyzed by the authors, and the limitations are addressed as challenges to obtain a set of requirements for IDPS in establishing a collaborative-based wireless IDPS (Co-WIDPS) architectural design. It amalgamates a fuzzy reinforcement learning knowledge management by creating a far superior technological platform that is far more accurate in detecting attacks. Due to the lack of a more detailed view of detection and prevention approaches using multi-agent system-based co-putational intelligence, authors presents a classification of three subclasses with an in-depth perspective on the characteristics: TAI-based, CI-based and MCIbased WIDPS. The performance of anomaly detection schemes for detecting attacks was measured by computing detection rates and false alarm rates for all the proposed methods and compares the detection rate and false alarm rate for the most popular detection methods(i.e.traditional artificial intelligence and computational intelligence),and the cooperative methods, such as the multi- agent based reinforcement learning(MCI).Superior performance of the RL approach comparing to neuro fuzzy and FCM and unsupervised SOM may be explained by the fact that the majority of computational intelligence methods with the help of multi-agent system shows the best performance by decreasing the complexity anomaly based detection rate. They conclude that the detection management techniques can be improved by minimizing the false alarm rates and increasing the detection rates in addition to decreasing energy consumption in WSNs.

Yun Wang et al. (2011) propose a novel k-Gaussian deployment strategy to leverage the advantages of both uniform and Gaussian random sensor deployment for efficient and effective intrusion detection. The key idea is to employ multiple deployment points in the area of interest and a subset of the total sensors are deployed around each deployment point following a Gaussian distribution and form a k-Gaussian distributed WSN. Authors also explore the intrusion detection problem in a k-Gaussian distributed WSN under the multi-level probabilistic sensing models theoretically and by simulations. The intrusion detection probability is formulated as a function of network parameters (i.e., number of sensors, sensing range, deployment points, distribution deviation, etc.), the intruder's behavior (i.e., the starting distance), and the application requirements such as Dmax. Theoretical derivations are validated by computer-based simulations and the theorems can be used to predict the performance of k-Gaussian distributed WSN. Authors show that the k-Gaussian distributed WSN statistically outperforms its counterpart uniform distributed WSN as well as Gaussian distributed WSNs under considered application scenarios.

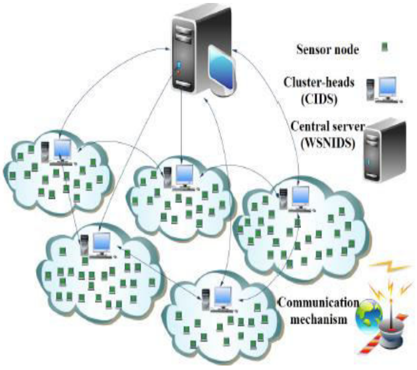
Shigen Shen et al. (2011) adopted the distributed-centralized network in which each sensor node has equipped an IDS agent, but only the IDS agent resided in the Cluster Head (CH) with sufficient energy will launch. Then, they apply the signaling game to construct an Intrusion Detection Game modeling the interactions between a malicious sensor node and a CH-IDS agent, and seek its equilibriums for the optimal detection strategy. They illustrate the stage Intrusion Detection Game at an individual time slot in aspects of its player's utilities, pure-strategy Bayesian–Nash equilibrium (BNE) and mixed-strategy BNE. Under these BNEs the CH-IDS agent is not always on the Defend strategy, as a result, the power of CH can be saved. As the game evolves, they develop the stage Intrusion Detection Game into a multi-stage dynamic. Intrusion Detection Game in which, based on Bayesian rules, the beliefs on the malicious sensor node can be updated. Upon the current belief and the Perfect Bayesian equilibrium (PBE), the best response strategy for the CH-IDS agent can be gained. Afterward, they propose an intrusion detection mechanism and corresponding algorithm. Simulation results have shown the effectiveness of the proposed game that can predict the type of member sensor nodes. Thus, the CH-IDS agent can choose its optimal strategy for defending the malicious sensor node's Attack actively.

Guorui Li et al. (2008) propose a distributed group-based intrusion detection scheme that meets all the requirements by partitioning the sensor networks into many groups in which the sensors in each group are physically close to each other and are equipped with the same sensing capability. The proposed intrusion detection algorithm takes simultaneously into consideration of multiple attributes of the sensor nodes to detect malicious attackers precisely. They show through experiments with real data that their algorithm can decrease the false alarm rate and increase the detection accuracy compared with existing intrusion detection schemes while lowering the computation and transmission power consumption compare the false alarm ratios and the detection accuracy ratios of the refined group-based intrusion detection scheme with alpha-quantile of the chi-squared distribution 0.99, 0.95 and 0.90, respectively. The false alarm ratio increases slightly with the decrease of the alpha-quantile. However, the change of the detection accuracy ratio is not obvious. At the same time, it can also reduce the monitoring power consumption with the requirement of grouping the sensor nodes in the network only once.

Hichem Sedjelmaci et al. (2011) propose a hybrid intrusion detection system for clustered WSN. Their intrusion framework uses a combination between the Anomaly Detection based on support vector machine (SVM) and the Misuse Detection. Anomaly detection uses a distributed learning algorithm for the training of a SVM to solve the two-class problem (distinguish between normal and anomalous activities). In addition, they use a hierarchical topology that divide the sensor network into clusters, each one having a cluster head (CH). The objective of this architecture is to save the energy that allows the network life time prolongation. In experiments, they used the KDDcup'99 dataset as the sample to verify the efficient of the distributed anomaly detection algorithm and valid it by compare with a centralized SVM-based classifier, which achieve a high level of accuracy detection. The proposed distributed learning algorithm for the training of SVM in WSN reaches high accuracy for detecting the normal and anomalous behavior (accuracy rate over 98%). Also a combination between the SVM classifier and Signature Based Detection achieve a high detection rate with low false positive rate and their approach reduces energy consumption.

Hossein Jadidoleslamy (2011) proposed a comprehensive model which has some main properties such as robustness, scalability, responsively, extensibility and incremental matching along with environment changes and its new conditions for Intrusion Detection Architecture (IDA). The main contribution of this architecture is its hierarchical structure; i.e., it is designed and applicable, in one or two levels, consistent to the application domain and its required security level. The focus is on the clustering WSNs, designing and deploying Cluster-based Intrusion Detection System (CIDS) on cluster-heads and Wireless Sensor Network wide level Intrusion Detection System (WSNIDS) on the central server. Suppositions of the WSN and Intrusion Detection Architecture (IDA) are: static and heterogeneous network, hierarchical and clustering structure, clusters' overlapping and using hierarchical routing protocol such as LEACH, but along with minor changes. The IDA is focused on integrating the accessible tools in security area of computer networks (like IDSs, logging, tracking and forensic analysis systems).

Figure 7 the proposed Intrusion Detection Architecture (IDA) for WSNs



Source: Hossein Jadidoleslamy (2011)

This model is a distributed model for intrusion detection on WSNs, which it is designed as even it can operates by only using minor and local accessible information in each cluster and cluster-head; i.e. it can uses from the local cluster-wide information to detects intrusions (it does not need to any another information: CIDS). Also, if necessary, sensor nodes, cluster-heads and WSNIDS cooperate to each others to take an appropriate decisions about if an attack occurred, or not; in other words, they share their information to each others, with collector and if necessary, with WSNIDS, to detect and make final decision on detected anomaly. The authors claim their research able them to improving the security level of WSNs.

K.Q. Yan et al. (2009) propose an Intrusion Detection System (IDS) created in Cluster-based Wireless Sensor Networks (CWSNs). According to the capability of Cluster Head (CH) is better than other Sensor Nodes (SNs) in CWSN. The proposed HIDS consists of an anomaly detection model and a misuse detection model. It filters a large number of packet records, using the anomaly detection model, and performs a second detection with the misuse detection model, when the packet is determined to intrusion. Therefore, it efficiently detects intrusion, and avoids the resource waste. Finally, it integrates the outputs of the anomaly detection and misuse detection models with a decision making model. This determines the presence of an intrusion, and classifies the type of attack. The output of the decision making model is then reported to an administrator for follow-up work. This method not only decreases the threat of attack in the system, but also helps the user handle and correct the system further with hybrid detection. To evaluate the performance of the misuse detection model, which is implemented by BPN though experiment. The simulation results present the performance of this method: the detection rate is 99.81%, the false positive rate is only 0.57% and its accuracy achieves 99.75%. The authors also find that the individual detection rate is very low when the training sample is not substantial. Therefore, the training samples must be a specific amount for the BPN to ensure the accuracy of classification.

Ioannis Krontiris et al. (2009) consider the problem of cooperative intrusion detection in wireless sensor networks where the nodes are equipped with local detector modules and have to identify the intruder in a distributed fashion. The detector modules issue suspicions about an intrusion in the sensor's neighborhood. They formally define the problem of intrusion detection and identify necessary and sufficient conditions for its solvability. Based on these conditions the authors develop a generic algorithm for intrusion detection and present simulations and experiments which show the effectiveness of proposed approach. They simulated a sensor network of 100 nodes placed uniformly at random in order to test proposed intrusion detection algorithm. The authors presented necessary and sufficient conditions for successfully exposing the attacker and a corresponding algorithm that is shown to work under a general threat model and investigation is performed in case of a single attacker (t = 1) gave very valuable insights into the solvability of cooperative intrusion detection.

Soumya Banerjee et al. Proposes a novel ant colony based intrusion detection mechanism which could also keep track of the intruder trials. The IDEAS system could work in union with the predictable machine learning based intrusion detection techniques to secure the sensor networks. The idea is to identify the affected path of intrusion in a sensor network by investigating the particular path or pheromone concentration. So behavior of the path of ant agents is being formulated through a knowledge base of rules, although the rules may also depict the possibilities of attack and proposed model of emotional ants presented the collaborative distributed intelligence as a distributed coordination problem in the face of uncertainty, incomplete information with soft time and resource constraints. Vital feature of the IDEAS framework is the ability to identify behavioral patterns, deliberate and act based on self organizational principle initiated with probability values.

Table 1.1 Summary of Wireless Sensor Network Intrusion Detection System

Authors	**Intrusion detection methods**	**Advantages**	**Disadvantages**
Noureddine Assad *et al.* [7]	Probabilistic model	The probability is increased while increasing the sensing range.	Affects the robustness of the connectivity due to small transmission range.
Michael Riecker *et al.* [8]	Energy-efficient system	Achieves low false positive rates.	Incurs unreliable and bursty links.
Hussein Moosavi et al. [9]	Game-theoretic framework	Improves the security and design stability.	Increase the number of compromised nodes.
Mohammad Wazid et al.[10]	K-means clustering	Avoids the detection mismatch.	Increases the incoming traffic in the WSN.
Helio Mendes Salmon *et al.* [11]	Artificial immune inspired system	Enhances the efficiency of the IDS system since it achieves low false positive.	Incurs larger delay in the intrusion detection system.
Shahaboddin Shamshirband *et al.* 12]	Fuzzy artificial immune system	Enhance the detection accuracy.	Fails due to high volumes of real time traffic.
Sutharshan Rajasegarar *et al.* [13]	Distributed anomaly detection	Improves robustness against the faulty or malicious node.	Due to large communication overhead, the performance gets degraded.
Anil Kumar Sagar et al. [14]	Probability based on network parameters	Significantly improves the detection probability.	Critical to detect the intruder when distance between nodes and intruder is greater than sensing range.
Ashfaq Hussain Farooqi et al.[15]	Stochastic games	The specification-based detection scheme achieves higher detection rate and Receives low false positive rate.	Complex to build, only for flat wireless sensor network.
Ahmed Saeed et al.[16]	Random Neural Networks (RNN)	The proposed solution is demonstrated for a wireless sensor nodes based system, with the detection accuracy of 97.23%.	Training is complex due to RNN's Vanishing Gradient or Exploding Gradient problems.
Sandhya G et al.[17]	K-means algorithm	High detection rate and low false positive rate are achieved	Suffers from disadvantages of k-means clustering such as degeneracy and cluster dependence.
Shahaboddin Shamshirband et al.[18]	Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA)	The proposed framework achieves higher detection accuracy 87% and clustering quality 0.99.	Complexity increased.
Guangjie Han et al.[19]	IDSEP	It is more efficient in detecting DoS attacks in WSN.	In the real WSN applications, there are many factors that will disturb the implementation of IDSEP, for example, propagation delay.
Maissa Elleuch et al.[20]	k-set randomized scheduling within the HOL theorem prover	The proposed approach generalized to tackle the formal analysis of the same randomized scheduling or other probabilistic problems.	Needs user intervention, proofs in HOL are interactive and require the intervention of User.
Laura Gheorghe et al.[21]	Adaptive Trust Management Protocol	Protocol covers a larger range of attacks, mostly because of the integration with a complex intrusion detection system.	Incurs huge communication overhead in exchanging experiences.
Masud Moshtaghi et al.[22]	Adaptive model	Adaptive model for anomaly detection, as well as a robust method for modeling normal behavior.	High computational overhead as decentralised approach is used.

Yassine Maleh et al.[23]	Hybrid intrusion detection system (HIDS)	High detection rate (almost 98%) and low false positive rate and low communication costs, which leads to improving the lifetime of the network.	Computational overhead, authors does not provide any attack scenario.
Yun Wang et al.[24]	Probability based on network parameters	Consider both homogeneous and heterogeneous WSNs by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range).	Computing a posterior may be extremely difficult.
Shahaboddin Shamshirband et al.[25]	Collaborative-based wireless IDPS (Co-WIDPS)	Minimizing the false alarm rates, increasing the detection rates and decreasing energy consumption.	Implementation not provided.
Yun Wang et al. [26]	k-Gaussian	The intrusion detection probability is formulated as a function of network parameters (i.e., number of sensors, sensing range, deployment points, distribution deviation, etc.), the intruder's behavior.	For computational reasons, it can fail to work if the dimensionality of the problem is too high (i.e. greater than 6 dimensions for instance).
Shigen Shen et al.[27]	Signaling game	The distributed-centralized Network model proposed has decreased the power consumption efficiently.	Complex to build in real applications.
Guorui Li et al.[28]	Distributed group-based	The proposed algorithm decreases the false alarm rate and increases the detection accuracy.	Behave well for large group size, for small group size power consumption is high.
Hichem Sedjelmaci et al.[29]	Hybrid intrusion detection system (HIDS)	In the proposed model most of routing attacks can be detected with low false alarm and reduces energy consumption	Depends upon features selected.
Hossein Jadidoleslamy et al. [30]	Hierarchical structure model	Based on agent and policy independent and autonomous agents, strong and comprehensive info-bases, dynamically reconfigurable, scalable, component-based and modular, high-flexibility and network-based architecture.	It is too rigid, or has too many levels; it can stifle initiative and make decision making a complex process.
K.Q. Yan et al.[31]	Hybrid intrusion detection system (HIDS)	In the proposed model the DR is 99.81%, the FP is merely 0.57%, and the accuracy is 99.75%	Depends upon feature selected for anomaly detection and if cluster head is compromised that may result in serious security breach.
Ioannis Krontiris et al.[32]	Generic algorithm	The proposed algorithm is lightweight to run on sensor nodes.	It cannot guarantee an optimal solution.
Soumya Banerjee et al.[33]	Ant colony based model	IDEAS technique could work in conjunction with the conventional machine learning based intrusion detection techniques to secure the sensor networks.	Probability distribution can change for each iteration.

IV. CHALLENGES IN DEPLOYING INTRUSION DETECTION SYSTEM IN WSN

Traditional Intrusion detection systems cannot appropriately detect suspicious activities in a WSN. For distributed nature of WSN infrastructure the ability of traditional intrusion detection system to handle and block large malicious attacks from offender may not be sufficient. Traditional schemes detect network intrusion by examining the all sensor node but some sensor node never launches them. This task is very tedious and time consuming. Much time and computing resources were wasted on normal analysis of data coming from a large group of sensor node in to detect well known attacks.

Either signature based (misuse based) or anomaly based (behaviour based) intrusion detection systems are not robust and efficient. Signature based intrusion detection system cannot detect unknown attacks while anomaly based intrusion detection has high false positive rate.

Intrusion detection systems that are deployed at individual node are vulnerable to node manipulation attack. Node can divert the any individual intrusion detect system or any detecting sensor deployed at any sensor node, which will make it difficult to detect network attack. The WSN architecture is highly dynamic, scalable and distributed in nature. The intrusion detection system to be successfully deployed in WSN, the intrusion detection systems have to cop up with the scalability of the wireless sensor network environment. The deployment strategy of intrusion detection system in is a big challenge in WSN environment.

So, the intrusion detection system for wireless sensor network should be light weight and no necessary information is passed between the client and server. The time taken by Intrusion detection system for detection and responding back to network intrusion in WSN is very high.

V. CONCLUSION

In this survey, various intrusions that can threat the confidentiality, integrity and availability of WSN services have been described. There are many solutions such as encryption, firewalls and others may not be sufficient, they can be act as first line of defence. This paper put stress on the use of intrusion detection system to secure WSN. A detailed design of intrusion detection system in WSN is presented. A comprehensive explanation of various intrusion architectures in WSN is also provided. The survey shows that so many different intrusion detection architectures already have been proposed which help in attack detection in WSN but they don't provide complete security solution. Each design lacks some features so we suggest that various detection mechanisms like signature based, anomaly based machine learning approaches and other soft computing should be incorporated to achieve the highest level security in WSN.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks”, *IEEE Commun. Mag.*, vol. 40, num. 8, pp. 102- 114, 2002.

[2] M. Ngadi, A.H. Abdullah, and S. Mandala, “A survey on MANET intrusion detection”, *International J.Computer Science and Security*, volume 2, number 1, pages 1-11, 2008.

[3] Y. Zhang, W. Lee, and Y.A. Huang, “Intrusion detection techniques for mobile wireless networks”, *J. Wireless Networks*, vol. 9, num. 5, pp.545-556, 2003.

[4] T.S. Sobh, “Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art”, *Elsevier J. Computer Standards and Interfaces*, volume 28, number 6, pages 670-694, 2006.

[5] T. Anantvalee and J. Wu, “A survey on intrusion detection in mobile ad hoc networks”, *Springer J. Wireless Network Security*, pages 159-180, 2007.

[6] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, “Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches,” *Proc. 1st International Workshop on Wireless Information Systems (WIS-2002)*, pp. 1-12, April 2002.

[7] Noureddine Assad, Brahim Elbhiri, Moulay Ahmed Faqihi, Mohamed Ouadou and Driss Aboutajdine, "Efficient deployment quality analysis for intrusion detection in wireless sensor networks", Wireless Networks, vol. 22, no. 3, pp. 991-1006, April 2016.

[8] Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani and Matthias Hollick, "Lightweight energy consumption-based intrusion detection system for wireless sensor networks", International Journal of Information Security, vol. 14, no. 2, pp. 155-167, 2015.

[9] Hussein Moosavi and Francis Minhthang Bui, "A Game-Theoretic Framework for Robust Optimal Intrusion Detection in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, vol. 9, no. 9, pp. 1367-1379, June 2014.

[10] Mohammad Wazid and Ashok Kumar Das, "An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks", Wireless Personal Communications, vol. 90, no. 4, pp. 1971-2000, October 2016.

[11] Helio Mendes Salmon, Claudio M. de Farias, Paula Loureiro, Luci Pirmez, "Intrusion Detection System for Wireless Sensor Networks Using Danger Theory Immune-Inspired Techniques", International Journal of Wireless Information Networks, vol. 20, no. 1, pp. 39-66, 2013.

[12] Shahaboddin Shamshirband, Nor Badrul Anuar and Miss Laiha Mat Kiah, "Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks", Journal of Network and Computer Applications, vol. 42, pp. 102-117, 2014.

[13] Sutharshan Rajasegarar, Christopher Leckie and Marimuthu Palaniswami, "Hyperspherical cluster based distributed anomaly detection in wireless sensor networks", Journal of Parallel and Distributed Computing, vol. 74, no. 1, pp. 1833-1847, 2014.

[14] Anil Kumar Sagar and D. K. Lobiyal, "Probabilistic Intrusion Detection in Randomly Deployed Wireless Sensor Networks", Wireless Personal Communications, vol. 84, no. 2, pp. 1017-1037, 2015.

[15] Ashfaq Hussain Farooqi, Farrukh Aslam Khan, Jin Wang and Sungyoung Lee, "A novel intrusion detection framework for wireless sensor networks", Personal and Ubiquitous Computing, vol. 17, no. 5, pp. 907-919, 2013.

[16] Ahmed Saeed, Ali Ahmadinia, Abbas Javed and Hadi Larijani, "Random Neural Network based Intelligent Intrusion Detection for Wireless Sensor Networks", In proceedings of International Conference on Computational Science, vol. 80, pp. 2372-2376, 2016.

[17] Sandhya G and Anitha Julian, "Intrusion Detection in Wireless Sensor Network Using Genetic K-Means Algorithm", In proceedings of IEEE International Conference on Advanced Communication Control and Computing Teclmologies, pp. 1-4, 2014.

[18] Shahaboddin Shamshirband, Amineh Amini, Nor Badrul Anuar, Miss Laiha Mat Kiah, Teh Ying Wah and

Steven Furnell, "D-FICCA: A Density-based Fuzzy Imperialist Competitive Clustering Algorithm for Intrusion Detection in Wireless Sensor Networks", Measurement, vol. 55, pp. 212-226, 2014.

[19] Guangjie Han, Jinfang Jiang, Wen Shen, Lei Shu and Joel Rodrigues, "IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks", IET Information Security, vol. 7, no. 2, pp. 97-105, 2013.

[20] Maissa Elleuch, Osman Hasan, Sofi`ene Tahar and Mohamed Abid, "Formal probabilistic analysis of detection properties in wireless sensor networks", Formal Aspects of Computing, vol. 27, no. 1, pp. 79-102, 2015.

[21] Laura Gheorghe, Razvan Rughinis and Razvan Tataroiu, "Adaptive Trust Management Protocol based on Intrusion Detection for Wireless Sensor Networks", In proceedings of IEEE International Conference on Networking in Education and Research, pp. 1-7, 2013.

[22] Masud Moshtaghi, Christopher Leckie, Shanika Karunaseker and Sutharshan Rajasegarar, "An adaptive elliptical anomaly detection model for wireless sensor networks", Computer Networks, vol. 64, pp. 195-207, 2014.

[23] Yassine Maleh, Abdellah Ezzati, Youssef Qasmaoui and Mohamed Mbida, "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks", The fiifth International Symposium on Frontiers in Ambient and Mobile Systems, vol. 52, pp. 1047-1052, 2015.

[24] Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang and Dharma P. Agrawal, "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks", IEEE Transactions on Mobile computing, vol. 7, no. 6, pp. 698-710, 2008.

[25] S. Shamshirband, N.B. Anuar, M.L.M. Kiah, A. Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique", Engineering Applications of Artificial Intelligence, vol. 26, no. 9, pp. 2105-2127, 2013.

[26] Yun Wang and Zhengdong Lun, "Intrusion detection in a K-Gaussian distributed wireless sensor network", Journal of Parallel and Distributed Computing", vol. 71, no. 12, pp. 1598-1607, 2011.

[27] Shigen Shen, Yuanjie Li, Hongyun Xu and Qiying Cao, "Signaling game based strategy of intrusion detection in wireless sensor networks”, Computers & Mathematics with Applications, vol. 62, no. 6, pp. 2404-2416, 2011.

[28] Guorui Li, Jingsha He and Yingfang Fu, "Group-based intrusion detection system in wireless sensor Networks”, Computer Communications, vol. 31. No.18, pp. 4324-4332, 2008.

[29] Hichem Sedjelmaci and Mohamed Feham, “ Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4 July 2011.

[30] Hossein Jadidoleslamy, “A hierarchical intrusion detection architecture for wireless sensor networks”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[31] K.Q. Yan, S.C. Wang, C.W. Liu, “A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks”, Proceedings of the International Multi Conference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 – 20, 2009.

[32] Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos,Felix C. Freiling, and Tassos Dimitriou, “Cooperative Intrusion Detection in Wireless Sensor Networks”, U. Roedig and C.J. Sreenan (Eds.): EWSN 2009, LNCS 5432, pp. 263–278, 2009. Springer-Verlag Berlin Heidelberg, 2009.

[33] Soumya Banerjee, Crina Grosan and Ajith Abraham, “IDEAS: Intrusion Detection based on Emotional Ants for Sensors”, 5th international conference on Intelligent systems design and application, pp. 344-349, Sep 2005.