© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Intrusion Detection in Wireless Sensor Networks

Deepak Singh Rajput, Nitesh Kumar Singh

Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

In recent years, the applications based on the Wireless Sensor Networks are growing very fast. The application areas include agriculture, healthcare, military, hospitality management, mobiles and many others. So these networks are very important for us and the security of the network from the various attacks is also a more important issue in WSN application now days. Stopping these attacks or enhancing the security of the WSN system various intrusion detection policies are developed till date to detect the node/s that is/are not working normally. Out of various detection techniques three major categories explored in this paper are Anomaly detection, Misuse detection and Specification- based detection. Here in this review paper various attacks on Wireless Sensor Networks and existing Intrusion detection techniques are discussed to detect the compromised node/s. The paper also provides a brief discussion about the characteristics of the Wireless Sensor Networks and the classification of attacks.

Keywords: Attacks, Intrusion detection, Intrusion detection techniques, Wireless sensor networks (WSN)

I. INTRODUCTION

The dashing progress in communication technologies proposes low-priced, low-power and multifunctional devices which leverages the idea of the sensors. The wireless sensor networks can be defined as a kind of networks that is formed by small sensors which are tightly deployed in an unattended environment. This network has no predefined infrastructure and can work in a structured or non-structured manner. According to [1], there are some features that

Make WSNs different from other Mobile Ad-hoc Networks (MANET). These differences include the following;

a) The number of nodes in WSN is greater compared to MANET
b) The great capacity of nodes in WSN compared to MANET
c) The high chance of sensor failures in WSN because of the deployment circumstances
d) The need for mobility causes the dynamic change of WSN topology
e) The high resource constraints of WSN in terms of power, storage, communication and processing capability

Yick et al. [2] categorized the WSN applications into two categories 1). Monitoring 2). Tracking. Each category is further categorized into many secondary categories. A large number of monitoring and tracking systems are already implemented and in the service to the public or the industry. However, describing such system is out of the scope of this survey.

To protect wireless sensor networks from the various weaknesses, preventive mechanisms like authentication and cryptography can be used to fend some type of attacks that are extruders. These type of methods or mechanisms define the primarily line of defense for the wireless sensor networks. However, some other type of attacks could not be prevented by these types of prevention mechanisms. Because these prevention mechanisms are used to detect only the outsider attacks not any insider attacks. So, for the insider attacks we need some other types of detection mechanisms, known as intrusion detection system [3].

II. METHODS AND MATERIAL

2. Characteristics of Wireless Sensor Networks

2.1 Self-Organization

Wireless sensor networks are formed by arranging great amount of sensor nodes in a domain. These Sensor networks protocols and algorithms have ability of self-organizing.

2.2 Multi hop Routing

Sensor nodes use multi-hop routing to promote their data to the upper nodes due to their short communication.

2.3 Resource Limitation

Wireless sensor nodes do not have a large battery life, larger transmission range and more computational power. They have limited memory. Although in the extent literature researches subjected to WSN are very generative, yet they still need to apply more efforts in the security of WSN. The arranging methods of WSN make them more defenseless to various attacks. WSN are used in applications where the sensors have physical interactions with the environment and are accessible by anyone makes them more vulnerable to security threats. The limitations [4] of WSN (in memory, energy and accessibility after deploying) make the use of existing security techniques infeasible. In this paper it is tried to mention the security threats and the intrusion detection mechanisms to protect from.

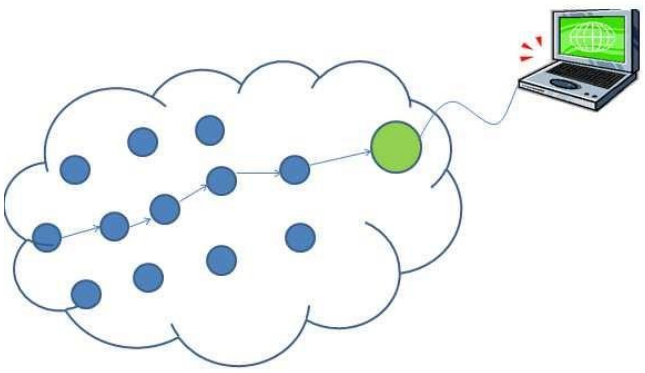

Figure 1 : Typical multi-hop Wireless Sensor Network Architecture

2.4 Challenges of Wireless sensor networks these communication limitations have been addressed by the start of multi-hop wireless networks, based on routing protocols from ad hoc networks. Akyildiz et al. [1] noted In contrast to other types of networks that this new creation of wireless sensor networks has several special requirements that raise novel technical challenges,

2.4.1 Varying network size

The number of sensor nodes can vary over time as nodes move or lose power.

2.4.2 Power constraints

In many situations the sensor nodes have a limited power supply, which makes communication much more expensive in comparison to local storage and computation.

2.4.3 Geographic or data-centric routing

Rather than relying on address-based routing, sensor nodes place greater importance on geographic routing or content based routing, where routing decisions can be made on the basis of the stuffs of the message, and whether there is span for local aggregation of measurements.

3. Security Threats

It defines the intrusion as any set of actions that are attempting to compromise the main components of the security system 1) The integrity, 2) Confidentiality or availability of a resource. In the same work, the intruder therefore was defined as an individual or group of individuals who take the action in the intrusion. The plainness of many routing protocols for wireless sensor networks makes them an easy target for the attacks. Wagner in [5] classifies the routing attacks into the following categories;

3.1 Spoofed, Altered, or Replayed Routing Information

While sending the data, the information in transition may be spoofed, altered, replayed, or destroyed. Due to the short range transmission of the sensor nodes, an

attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

3.2 Selective Forwarding

In this kind of attack a malicious node may decline to forward every message it gets, acting as black hole or it can forward some messages to the wrong receiver and simply drop others.

3.3 Sinkhole Attacks

In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the compromised node may listen to requests for routes, and then reply to the requesting node with messages containing a bogus route with the shortest path to the requested destination.

3.4 Sybil Attacks

In Sybil attack the malicious node presents itself as multiple nodes. The attack of this type tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attack can be performed against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection [11].

3.5 Wormholes

Wormhole attack [12] is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn't exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors. This attack would likely be used in combination with selective forwarding or eavesdropping.

3.6 HELLO Flood Attacks

This attack is based on the use by many protocols of broadcasting Hello messages to announce themselves in the network. So an attacker with higher range of transmission may send many Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion.

3.7 Acknowledgement

Some wireless sensor network routing algorithms require link layer acknowledgements. A compromised node may exploit this by spoofing these acknowledgements, thus convincing the sender that a weak link is strong or a dead sensor is alive.

3.8 Sleep deprivation attack

A particularly devastating attack is the sleep deprivation attack, where a malicious node forces legitimate nodes to waste their energy by resisting the sensor nodes from going into low power sleep mode. The goal of this attack is to maximize the power consumption of the target node, thereby decreasing its battery life. So, it is also known as battery exhaustion attack.

Table 1: Security attacks in WSN

Name of the attack	Characteristics
DoS attacks in different layers [17], [18], [19]	Flooding, jamming, misdirection
Sinkhole/Blackhole [20], [21]	Shortest path, drop the packets
Selective forwarding [22], [23]	Selectively drop the packets
The node replication [24], [25]	Add extra node to the network with the same cryptographic secrets
HELLO flood [26]	Flood with HELLO packets
Wormhole [27], [28]	Offer less number of hops and less delay which is fake
Sybil [29], [30]	A malicious node pretends to be more than one node
Sleep deprivation [31]	forces legitimate nodes to waste their energy

4. Intrusion Detection System

Intrusion detection system can provide protection from both inside and outside intruders. An intrusion detection system is necessary for the wireless sensor networks because simple security mechanisms such as cryptography cannot provide the better security. For example cryptographic mechanisms provide protection against some types of attacks from external nodes, but it will not protect against malicious inside nodes, which already have the required cryptographic keys. Therefore, intrusion detection mechanisms are necessary to detect these malicious nodes.

Two major approaches are used for the intrusion detection in wireless sensor networks 1) Signature based and 2) Anomaly based intrusion detection. In the signature based intrusion detection attack patterns or the behavior of the intruder is modeled (attack signature is modeled). In this the system will raise an alarm for an intrusion when the match is detected. However in the anomaly based intrusion detection the system will raise the alarm once the behavior of the network does not match with its normal behavior. Another intrusion detection approach is also present known as specification based intrusion detection. In this approach, the normal behavior (expected behavior) of the host is specified and consequently modeled.

4.1 Signature Based, Anomaly Based and Specification Based IDS

Signature based intrusion detection (also known as misuse detection) is one of the commonly used and up till now accurate methods of intrusion detection. Once a new attack is launched, the attack pattern is carefully studied and a signature is defined for it. The signature can be a name in characters within the body of the attack code, the targeted resources during the attack or the way these resources are targeted (attack pattern). This approach is very efficient for the known attacks and produces small number of FP alarms. However, as the main short coming of this approach, it is not capable of detecting novel attacks. Once the attack pattern is slightly altered, this approach will not detect the altered versions of the old attacks. Thus, this approach is only efficient in detecting previously known attacks. There is another approach for detecting the novel and unseen attacks that follows.

Another widely used ID method is the anomaly detection approach [6-9]. The basic idea behind this approach is to learn the usual behavioral pattern of the network. Consequently the attack is suspected once the network behaves out of its regular way or anomaly. However, networks' regular behavior is not similar for different networks. The network behavior is dependent on the date or the working conditions in the organization where the network is installed. The regular behavior model for the network can be variable. Considering these working conditions, the degree of freedom for the problem is large. One way to solve this problem is to make the IDS adaptable to the network environment where it is going to be installed. To do so, IDS will start to monitor and record the network behavior just after its deployment.

Assuming the recorded pattern as the regular pattern for the network, IDS will use it as the normal behavior of the network and will set a baseline. Once the network pattern deviates from this baseline pattern by more than a threshold value, it denotes an anomaly. As it was mentioned earlier, not every anomaly indicates an intrusion. This is especially true in this case, where the system is very dynamic. Thus, it is not clear if the detected anomaly should be assumed to be an intrusion or not. As a direct result of this uncertainty, anomaly based IDS will produce high FP alarms. As a remedy to this problem there should be a pruning system to detect FP alarms and cancel them. Keeping this shortcoming in mind this approach has a big benefit, that is, it is capable of detecting attacks or new releases of the old attacks.

A recently introduced approach is the specification based intrusion detection approach. Some reported works emphasize only on the signature based and anomaly based intrusion detection approaches [8, 10-12]. However, there are others who talk about all three of the approaches. The specification constraint in this approach is used for reducing the number of FP alarms [13, 14]. Specification based is not just applicable to the host systems but they can also be applied on the users as well. A genuine user is expected to behave in a certain way, or it can be specific that a user should beehave in this manner. This decision will improve the security but

with the expense of a less attractive user interface. Limiting the user actions and freedom may lead to making the application look less appealing to some users. It is expected to get better results by applying specification based ID methods on the system itself.

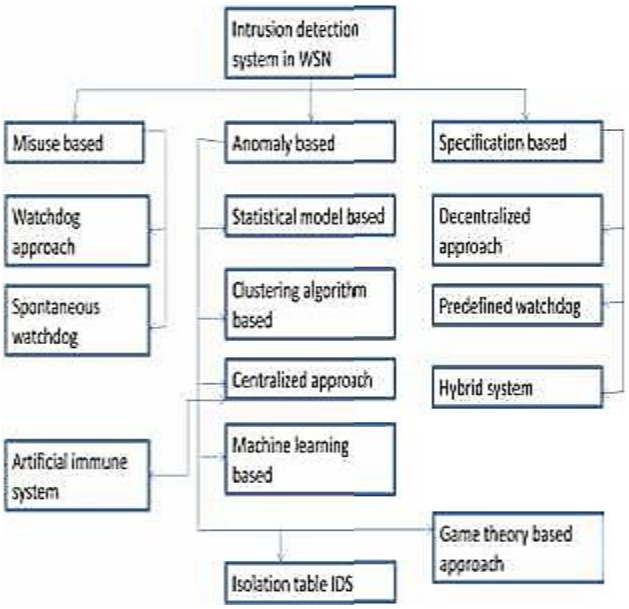

Figure 2 : Taxonomy of Intrusion Detection Systems in WSN

4.2 Network Based IDS and Host Based IDS Mukkamala et al. [15] consider that IDS has two categories 1) Host based IDS and 2) Network based IDS. They define these two types as follows: "A host based IDS monitors all the activities on a single information system host. It ensures none of the information system security policies are being violated. A monitors activities on a whole network IDS network and analyzes traffic for potential security breaches or violations."

The network based IDS are responsible to protect the entire environment of the network from the intrusion. This task asks for full knowledge of the system status and monitoring both the components of the network and the transactions between them. Agent technology plays a key role in this strategy. The host based IDS are only installed on a single host/terminal and are responsible for monitoring the status of that terminal/server only.

This type of IDS is responsible for the security of its host and will monitor the entire network activities in that host. One of the problems with the host based IDS are the high processing overhead that they impose on their host. These overheads will slow down the host and therefore it is not welcomed. This approach is quite popular among the researchers.

5. Various Types of Schemes Used to Build Intrusion Detection System

These schemes can be classified into three main basic categories (According to the prior knowledge available for attack detection) 1) Supervised learning based 2)Unsupervised learning based and 3) Semi-supervised learning based schemes .

5.1 Supervised Learning Based Schemes Supervised learning based schemes involve any kind of prior knowledge or training in order to build the normal profile during the training phase. In the testing phase, the new patterns will be compared with the build normal profile to detect any deviation. The rule-based intrusion detection schemes can be considered in this category since they are depending on a prior knowledge in the form of predefined rules.

5.2 Semi-Supervised Based Schemes

In this category, the training data has labeled instances of one class which is the normal class.

5.3 Unsupervised Based Schemes

In these types of schemes, methodologies do not require training data and instead of that some assumptions are considered that normal behavior is far different from the anomaly. Their problem, if this assumption is not always true, it will suffer from high false alarms.

III. RESULTS AND DISCUSSION

6. Related Work

The classification of the approaches is categorized in four main categories;

1. Rule based intrusion detection schemes
2. Data mining and computational intelligence based
3. Game theoretical based
4. Statistical based

6.1. Rule-Based Intrusion Detection Schemes in WSN
Rule based intrusion detection schemes are also known as specification based intrusion detection schemes. In these schemes, the detection rules are first designed by domain expert before the starting of the detection process. Many of these techniques follow three main phases 1) Data acquisition phase 2) Rule application phase and 3) Intrusion detection phase. In the following sub-sections, the key important schemes in this category are explored.

6.1.1 Decentralized IDS in WSN

The most cited rule-based intrusion detection scheme for WSN to detect many different kinds of attacks in different layers. In this scheme, there are three main phases involved 1) Data acquisition phase in which the monitor nodes are responsible of promiscuous listening of the messages and filtering the important information for the analysis.2) The rule application phase, in which the pre-defined rules are applied to the stored data from the previous phase, if the message analysis failed any of the rules test, a failure is raised and the counter increased by one. 3) The intrusion detection phase, a comparison is taken place between the number of raised failures produced from the rule application phase with a predefined number of occasional failures that may happen in the network. If the total number of the raised failures is higher, intrusion alarm is produced.

6.1.2 Malicious node detection in WSN

A solution to identify the possible malicious node based on the received signal strength measured in each node. They showed how to detect two kinds of attacks called HELLO flood attack and the wormhole attack in WSN by building a rule that compare the energy of the received signal and the energy of the same observed signal around the network. Although, this solution was one of the first solutions in the domain, it still restricted to those two types of attacks. In addition, sometimes there are other reasons rather than attacks that may cause a change in the signal strength which make this solution impractical.

6.1.3 An intrusion detection system for wireless sensor network A novel intrusion detection scheme that takes the benefits of neighboring node information to detect the node impersonation and resource depletion attacks. In this scheme each node can make a statistical profile of its neighbor's behavior based on two features which are the received power rate and the arrival packet rate. This scheme cannot to be generalized for a typical wireless sensor network application in which many types of attacks evolve continuously. In addition and similar to the scheme proposed , the building of the rules based on the received power rate is impractical since there are other factors that may affect this feature.

6.1.4 Towards intrusion detection in WSN introduce a lightweight scheme for detecting selective forwarding and black hole attacks in WSN. The key idea of their scheme is to make nodes monitor their neighbourhood and then communicate between each other to decide if there is an intrusion taken place. The scheme is further evaluated experimentally on a real WSN deployment.

6.1.5 Neighbour-based intrusion detection for WSN Intrusion detection architecture based on collaboration between neighbors. They evaluated their scheme for detecting three types of attacks: Hello flood, selective forwarding and jamming attacks. Their scheme was implemented for Collaboration Tree Protocol (CTP) on the TinyOS environment. Although, the collaboration among nodes makes this scheme strong, the communication overhead is a problem. In addition, the extracted features that are used to construct the rules like packet sending rate and packet dropping rate caused a high false alarm for detecting attacks. Another drawback of this study is that it did not consider the power consumption rate related to the performance which is a very critical issue in WSNs.

6.1.6 A new collaborative approach for IDS on WSN: to detect node repetition attacks. This scheme is based on determining some nodes to be monitored nodes for monitoring the behavior of other nodes in the network based on satisfying set of predefined rules suitable for a specific attack type. These monitor nodes are in turn monitored by special nodes called supervisor nodes which are responsible for correlating the evidences resulted by monitor nodes.

6.1.7 Intrusion Detection based on Traffic Analysis and Fuzzy Inference System in WSN: An intrusion detection scheme for WSN by utilizing two main traffic features: the packet reception rate and the packet inter-

arrival time in a time window and then apply the fuzzy inference to decide whether an attack has taken place or not. However, this scheme is based on fuzzy logic, so it needs the rules to be prepared prior the detection process. The dependence on the prior knowledge which is the rules makes such schemes impractical for a continuous streaming environment like WSN. In addition, the authors did not specify certain attacks to be detected by this scheme.

6.1.8 Advantages of Rule-based intrusion detection schemes for WSN:

a) Fast detection: because there is no training involved in these schemes. This feature fulfills the need for online detection when there is a continuous streaming of data in some WSN applications.
b) The computational complexity is not discussed here: since the schemes use only simple rules for detecting attacks.
c) Higher detection accuracy: since it depends on comparison with some predefined rules.

6.1.9 Shortcomings of Rule-based intrusion detection schemes for WSN

a) Detection generality: since these schemes depend on the rules prepared by experts for specific attack types, it cannot be generalized to detect other types of attacks because different attacks have different symptoms (features) that will derive different rules
b) Collaborative voting: most of the schemes based on collaboration between the neighbors that vote to decide about the occurrence of an attack. This voting mechanism may increase the communication overhead
c) Assumptions: most of the schemes put many assumptions prior to the building of their detection agent. These assumptions make their applicability difficult for different applications.

6.2 Clustering-Based Intrusion Detection for Routing Attacks in WSN data mining-based intrusion detection scheme for WSN. In this scheme, each node uses the fixed width clustering algorithm to build the normal profile from the node traffic behavior. This normal profile is used later to detect abnormal activities caused by attacks. The scheme is composed of three main stages: feature selection stage in which the most important features that characterize the network traffic have been selected; cluster formulation, by applying the Euclidean distance metric to measure the similarities between the data traffic points and then form the clusters; and the cluster labeling stage, in which the result clusters are labeled based on the assumption that the number of objects in the normal cluster is much more than that number in the anomalous one. This scheme has many advantages including, the ability of detecting unknown attacks since it is unsupervised. In addition, the number of features used to build the normal profile is suitable to make this scheme generic for detecting different types of attacks. Moreover, the fixed width clustering algorithm reduces the number of parameters required for clustering and requires only one pass through the traffic samples. However, this scheme has many drawbacks that make it unsuitable for the resource constrained WSN. The most important drawback is that, each node has to perform its own IDS independently, so this will consume the nodes' power quicker because of the clustering algorithm. Another drawback is that, the fixed distance threshold of the fixed width clustering algorithm makes this scheme inflexible.

6.2.1 Detecting selective forwarding attacks in WSNs using SVM A centralized IDS scheme to detect selective forwarding and blackhole attacks based on one class Support Vector Machines (SVM) and sliding windows. This scheme uses only 2D feature vector which are bandwidth and count hope for the classification. This scheme is totally centralized in such that feature selection, processing and decision making are all done by the base station. The authors argue that this scheme is energy efficient because it is entirely centralized and there is no involvement of the sensor nodes in the detection process. On the other hand, the small number of features makes this scheme very specific and cannot be generalized for different kinds of attacks. Although the use of Machine learning techniques provides the scheme with the generality by training the normal profile, this scheme only designed to detect two types of attacks. That means the choosing of the features is very important in making the scheme general to different types of attacks.

6.2.2 An Integrated Intrusion Detection System for Cluster-based WSNs

Integrated Intrusion Detection System (IIDS) scheme for cluster based WSN. This scheme is composed of three level IDS components called Misuse IDS deployed with the common sensor nodes, Hybrid Intrusion Detection System (HIDS) employed in the cluster heads and Intelligent Hybrid Intrusion Detection System (IHIDS) employed in the sink node. This composition of the IDS components is according to the different capabilities and probabilities that these entities may suffer from. The proposed IIDS consists of both misuse and anomaly detection modules to get the benefits of both approaches in increasing the detection accuracy and lowering the false alarms.

6.2.3 Advantages of DM/CI based IDS schemes in WSNs

a) Less communication overhead: since most of schemes are based on the hierarchical structure of the WSN, so there is less communication overhead.
b) Generality is guaranteed: since the normal profile is not based on specific traffic features
c) Scalability is also guaranteed: because the normal profile depends on the data and not on the architecture

6.2.3 Shortcomings of DM/CI based IDS schemes in WSNs

a) Slow detection: because the data mining techniques like clustering require learning the normal profile, they are slow and therefore are not satisfying the streaming feature of the WSN that requires a fast solution or real time solution
b) High computational complexity: because they involve the use of some complex machine learning algorithms or some difficult clustering approaches
c) High false alarms: because they build the normal profile for a data in a specific point of time and there is no quick update, the normal profile could be out of data.

6.3 Intrusion detection in sensor network: a non-cooperative game approach

In this framework, three different schemes have been applied to finding the most vulnerable node in WSN and protect it. The first scheme, an attack-defense problem is approached as two players, non-zero, non- cooperative game between the attacker and the sensor network. The second scheme uses the Markov Decision Process (MDP) to find the most vulnerable sensor node whereas the third scheme applies node's traffic as an intuitive metric to use it as an indicator for protecting the node. The evaluation of their schemes reveals its effectiveness of successful defense against attacks. This study needs an experimental investigation to prove the concepts of the three used schemes. Another limitation of this work is that, the strategy on when the MDP should be applied and when the theoretic game framework should be used to gain high success detection is not determined.

6.3.1 Game theory model for selective forward attacks in WSN

A framework using Zero-Sum game approach and selective node acknowledgements in the forward data path is proposed by Reddy and Srivathsan to detect selective forwarding attacks in WSN. The authors provide mathematical foundations for detecting malicious nodes using selected points in the forward data path. They proved that selective acknowledgements are very useful to detect the malicious nodes through simulations. However, like other game theoretical approaches, this framework need to be more investigated experimentally to prove its concept.

6.3.2 Advantages of game theory based IDS schemes in WSN

a) The game theoretical based IDS schemes do not need extra data to build the model and rather benefits from the routing information of the network.
b) The techniques used in these kinds of schemes are lightweight since no training is involved and are depending on some strategies

6.3.3 Shortcomings of game theory based IDS schemes in WS

a) It is obvious from the reviewed schemes that these schemes still concepts that need to be experimented extensively to prove their viability
b) The scope of the game theoretical based schemes is limited to some layers information like the routing and application layers information because it builds the strategies based on some information from the network layer and application layers.

6.4 An Anomaly Detection Algorithm for Detecting Attacks in Wireless Sensor Networks present a new scheme based on the Cumulative Sum algorithm (CuSum) for detecting different kinds of attacks in WSN. This algorithm is one of the change point detection algorithm used to detect the change of the mean value of random sequence. In this scheme, the CuSum algorithm is employed to detect the changes in the number of incoming and outgoing packets as well as the number of collisions. A set of monitoring nodes is selected so that each sensor node is monitored by at least one monitor node. This scheme's main drawback is that the monitor node can be a point of failure easily since it is a normal sensor node.

In addition, the implementation of such algorithm in a normal monitor node is power consuming.

6.4.1 Malicious node detection in WSN using an Auto regression technique

A strategy based on the past/present values generated by sensor nodes. In this study, the output of each sensor at each moment with its estimated value is computed to a predictor based on Auto Regression (AR) technique. If there is a big difference between the two values in any sensor then this sensor becomes suspicious and an action should be done to mitigate its effects. The authors presented a case study to prove the effectiveness of their concept with some assumptions that are set prior the design of the AR technique. These assumptions are common in other intrusion detection schemes for WSN but limit the applications of these schemes for different WSN applications.

6.4.2 Advantages of statistical based IDS schemes in WSN

The statistical based schemes are mathematically proven and can be used effectively only if the accurate probability distribution model for normal or abnormal traffic is obtained.

6.4.3 Shortcomings of statistical based IDS schemes in WSN

a) Usually the process of acquiring the correct probability distribution is not easy especially when no prior knowledge is available about sensor streaming data.
b) Many of statistical schemes do not fit well with the multivariate data.
c) The dynamic streaming of network data makes it difficult to keep the probability distribution model up to date.

7. Important Future Research Areas

In order to satisfy the requirements of an ideal intrusion detection scheme, some important research opportunities open for further research:

7.1 Detection Generality

To design intrusion detection schemes that can be used to detect different types of attacks.

7.2 Detection Speed

There is a need for a fast intrusion detection scheme that satisfy the dynamic and Continuous streaming of data in WSNs

7.3 Global Detection

In the cluster based intrusion detection systems, the clusters should co-operate with each other so that they can form a global intrusion detection system.

IV. CONCLUSION

As the WSN becomes necessary and used frequently for many applications, the need for securing them is also increasing due to the nature of their deployment and their resource restrictions. Cryptographic and authentication protocols have been proposed to protect these networks from outsider intrusions but fail to protect them from the insider ones. Many surveys have been published for anomaly detection but according to the best of our knowledge none of them tackle the problem of intrusion detection in specific. Instead, most of them focus on the anomaly detection in general assuming that the intrusion is kind of anomalies. In this article, we surveyed about the intrusion detection schemes in WSN. The classification includes four main categories: rule based, data mining and computational intelligence based, game theoretical based and statistical based. For each category, an analysis has been carried out for each scheme highlighting their advantages and drawbacks. Finally,

some important future research opportunities are pointed out for the future research.

V. REFERENCES

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, Wireless sensor networks: A survey, Computer Network. 38, 2002, 393-422.

[2] J. Yick, B. Mukherjee and D. Ghosal, Wireless sensor network survey. Computer. Network, 52, 2008, 2292- 2330

[3] A.P.R.D. Silva, M.H.T. Martins, B.P.S. Rocha, A.A.F. Loureiro and L.B. Ruiz et al., Decentralized intrusion detection in wireless sensor networks, Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, (QSSWMN; 25), 2005, 16-23.

[4] U. Bilstrup, K. S. Oberg, B. Svensson, and P.A. Wiberg, Capacity Limitations in Wireless Sensor Networks, Proceedings of ETFA2003, 9th IEEE International Conference on Emerging Technologies and Factory Automation, Lisbon, Portugal,2003, 16-19

[5] C. Karlof and D. Wagner, Secure Routing in Sensor Networks: Attacks and Countermeasures, In Proc. of First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[6] F. Neri, Comparing local search with respect to genetic evolution to detect intrusions in computer networks, Proceedings of the 2000 Congress on Evolutionary Computation, 1, 2000, 238–243.

[7] S. Mukkamala, G. Janoski, and A. Sung, Intrusion detection using neural networks and support vector machines, International Joint Conference on Neural Networks IJCNN02, 2, 2002, 1702–1707

[8] J. Guan, D. X. Liu, and B. G. Cui, An induction learning approach for building intrusion detection models using genetic algorithms, Proceedings of Fifth World Congress on Intelligent Control and Automation WCICA, 5, 2004, 4339–4342.

[9] C. Kruegel, T. Toth, and E. Kirda, Service specific anomaly detection for network intrusion detection, Proceedings of the 2002 ACM symposium on Applied computing, 2002, 201–208.

[10] J.E. Dickerson and J.A. Dickerson, Fuzzy network profiling for intrusion detection, Proceedings of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, 2000, 301–306.

[11] S.B. Cho, Incorporating soft computing techniques into a probabilistic intrusion detection system, IEEE transactions on systems, man, and cybernetics part c: applications and reviews, 32, 2002, 154–160.

[12] K. Yoshida, Entropy based intrusion detection, Proceedings of IEEE Pacific Rim Conference on Communications, Computers and signal Processing (PACRIM2003), 2, 2003, 840–843.

[13] T. Song, J. Alves-Foss, C. Ko, C. Zhang, and K. Levitt, Using acl2 to verify security properties of specification-based intrusion detection systems, Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003), 2003.

[14] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, Specification-based anomaly detection: a new approach for detecting network intrusions, 9th ACM conference on Computer and communication security, 2002, 265–274,

[15] S. Mukkamala, G. Janoski, and A. Sung, Intrusion detection using neural networks and support vector machines