American Journal of Applied Sciences 9 (10): 1636-1652, 2012
ISSN 1546-9239

A Survey of Intrusion Detection Schemes in Wireless Sensor Networks

Murad A. Rassam, M.A. Maarof and Anazida Zainal
Department of Computer Systems and Communication
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia, 81310, Skudai, Malaysia

Abstract: Wireless Sensor Networks (WSNs) are currently used in many application areas including military applications, health related applications, control and tracking applications and environment and habitat monitoring applications. The harsh and unattended deployment of these networks along with their resource restrictions makes their security issue very important. Prevention-based security approaches like cryptography, authentication and key management have been used to protect WSNs from different kinds of attacks but these approaches are not enough to protect the network from insider attacks that may extract sensitive information even in the presence of the prevention-based solution. Detection-based approaches are then proposed to protect WSNs from insider attacks and act as a second line defense after the failure of the prevention-based approaches. Many intrusion detection schemes have been introduced for WSN in the literature. In this article, we present a survey of intrusion detection schemes in WSNs. First, we present the similar works and show their differences from this work. After that, we outline the fundamentals of intrusion detection in WSNs, describing the types of attacks and state the motivation for intrusion detection in WSNs. Then, we demonstrate the challenges of developing an ideal intrusion detection scheme for WSNs followed by the main requirements of a good candidate intrusion detection scheme. The state-of-the-art intrusion detection schemes are then presented based on the techniques used in each scheme and categorizing them into four main categories: rule-based, data mining and computational intelligence based, game theoretical based and statistical based. The analysis of each scheme in these categories is presented showing their advantages and drawbacks. By the end of each category, we state the general advantages and shortcomings of each category. The survey ends by recommending some important research opportunities in this field for future research.

Key words: Wireless Sensor Networks (WSNs), Mobile Ad-hoc Networks (MANET), Intrusion Detection Systems (IDS), Data Mining and Computational Intelligence (DM/CI)

INTRODUCTION

The fast advancement in communication technologies introduces cheap, low-power and multifunctional devices which leverage the idea of the sensor (Akyildiz *et al*., 2002). Wireless Sensor Networks (WSNs) can be defined as a kind of networks that is formed by (ten to thousands) of tiny sensors which are densely deployed in an unattended environment. This network has no predefined infrastructure and can work in a structured or non-structured manner. The resource-constrained feature plays the main rule in the ways that WSNs should work or deployed.

According to Akyildiz *et al*. (2002), there are some features that make WSNs different from other Mobile Ad-hoc NETworks (MANET). These differences include the following:

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

Corresponding Author: Murad A. Rassam, Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, 81310, Skudai, Malaysia Tel: +(60)173681303 Fax: +(607)5532210

Yick *et al*. (2008) categorized the WSN applications into two categories: monitoring and tracking. Each category is further categorized into many sub categories. A broad 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.

Based on the differences from other networks and because of the harsh environment in which they are deployed, WSN is very susceptible and vulnerable to many kinds of attacks either from inside or outside of the network. It is also clear that most of the security solution adopted for MANET cannot be directly used for WSNs for the same reasons (Akyildiz *et al*., 2002).

To protect WSNs against different kinds of vulnerabilities, preventive mechanisms like cryptography and authentication can be applied to prevent some types of attacks. This kind of preventive mechanisms formed the first defense line for WSNs. However, some attacks like wormholes, sinkhole, could not be detected using this kind of preventive mechanisms. In addition, these mechanisms are only effective to prevent from outside attacks and failed to guarantee the prevention of intruders from inside the network (Silva *et al*., 2005). Because of that, it is necessary to use some mechanisms of intrusion detection.

Intrusion Detection Systems (IDS) are considered to act as the second defense line against network attacks that preventive mechanisms fail to address (Silva *et al*., 2005). An Intrusion detection system is defined in (Debar *et al*., 1999) as “A system that dynamically monitors the events taking place on a system and decides whether these events are symptoms of an attack or constitute a legitimate use of the system”. However, there are many challenges posed against the application of the IDS for WSNs. These challenges are due to the lack of resources like, energy, processing and storage.

In general, IDS schemes are categorized into misuse IDS and anomaly IDS. The former matches the new observations with the signatures stored in the database of the IDS. The later detects the abnormal activities from the predefined normal profile in order to identify possible attacks. Furthermore, Anomaly IDS schemes can be classified into supervised based, semi supervised based and unsupervised based IDS. The supervised based intrusion detection schemes involve training the detection model which requires prior knowledge about what is normal behavior and what is anomaly. The semi-supervised intrusion detection schemes require the knowledge of one class either the normal or the anomaly to help build the model for detection. The unsupervised intrusion detection schemes do not require any prior knowledge to build the detection model and instead use some measurements to decide if the data instance is normal or anomalous.

Many techniques have been used to design intrusion detection schemes for WSN. Rule-based intrusion detection schemes can be considered as supervised anomaly intrusion detection schemes where a set of rules are defined before the detection process using assumptions, information, or experience known in advance. These schemes compare the attributes of network behavior to these predefined rules. If the attributes passed this comparison it is considered normal, else it is considered intrusions. Upon deciding of an intrusion, an alarm is raised to inform the system administrator to take an action.

Data Mining and Computational Intelligence (DM/CI) techniques are commonly used to build intrusion detection schemes in computer networks. However, the use of these techniques to build IDS schemes for WSN is either in its infancy stage or not fulfilling the special requirements of IDS in WSN.

Game theory concepts are also used to design some intrusion detection schemes in the literature. In these schemes, some game strategies have been used that simulate the intrusion detection process as a game between the attacker and the intrusion detection agent.

Statistical based intrusion detection schemes are common schemes used for general anomaly detection in WSN. However, some researchers used them for intrusion detection. These schemes are based on building of the probability distribution of the traffic data.

The contribution of this survey can be summarized in the following:

- Describes the fundamentals and challenges of intrusion detection in WSN
- Describes the requirements of intrusion detection in WSN
- Provides technique based taxonomy of the current intrusion detection schemes in WSN together with an evaluation of their satisfaction of the requirements
- Introduces some opportunities to be considered for the future research

Existing surveys: The first comprehensive and most cited survey in the field of WSN is introduced by Akyildiz *et al*. (2002). In this survey, the basic fundamentals of WSNs were explored including the potential uses of these networks as well as the review of factors that affect the design of the sensor networks and the communication architecture used by them. Other two surveys about the routing in WSN have been proposed (Al-Karaki and Kamal, 2004; Akkaya and Younis, 2005) however, they did not discuss the security issues.

Karlof and Wanger (2003) introduced an analysis of the security issues for routing in sensor networks. They described many kinds of attacks on sensor networks and suggest the suitable countermeasures that can help to mitigate them. Many surveys have been proposed for the security in WSN in general (Yun *et al*., 2008; Chen *et al*., 2009; Christin *et al*., 2010; Walters *et al*., 2007); however, all of them discussed only the prevention based schemes as well as the secure routing protocols. These solutions focused on protecting the network from the outsider attacks and ignore the insider intrusions and compromised nodes.

The first survey about the anomaly detection in WSN was introduced by Rajasegarar *et al*. (2008). In this survey, the authors introduced the state of the art techniques for anomaly detection in WSN and described their characteristics that differ from the anomaly detection techniques in traditional networks. Anomaly detection techniques in the mentioned survey have been classified into statistical techniques and non-parametric techniques. The rule-based schemes have been introduced as non-parametric schemes.

Outlier detection in wireless sensor networks survey introduced by Yang *et al*. (2010) is a very systematic and technical survey describes the outlier detection techniques used in WSN. It explores the challenges of designing effective outlier detection techniques as to motivate researchers to find solutions for such challenges. The most exciting contribution in this survey is the technique based taxonomy of outlier detection techniques based on three main criteria named the nature of sensed data, type of outlier and the degree of outlier. This classification is very useful for choosing the suitable technique based on the context of application and its criteria.

The most recent survey introduced by Xie *et al.* (2011) for anomaly detection techniques in WSN classified the detection techniques based on the architecture of WSN into flat based and hierarchical based techniques. Then, the anomaly detection methods were described for each structure. They concluded their survey by analyzing the performance of the reviewed techniques based on some performance metrics and show the possible research directions in future anomaly detection.

Although, the surveys (Rajasegarar *et al*., 2008; Yang *et al*., 2010; Xie *et al*., 2011) provide a systematic and comprehensive description of the anomaly detection techniques used in WSN, they only approach the problem of anomaly detection from the perspective of anomaly in general. Attacks or intrusions are considered to be a kind of anomalies because it affects the normal behavior of the system. The only survey that is available at the moment, according to the best of our knowledge in intrusion detection, is introduced by Farooqi and Khan (2009). However, this survey is not comprehensive and it does not show the weaknesses of the schemes as well as the directions for future research.

From this point, we start to make this survey as much as specialized and comprehensive on intrusion detection schemes for WSN. The main difference between this survey and the published surveys is that, the published surveys targeted the anomaly detection in general whereas this survey is very specific for the intrusion detection in WSN. The intrusion detection should be performed in real time but the anomaly detection could be performed after a predefined threshold of time.

Fundamentals of intrusion detection in WSN: We introduce the fundamentals of the intrusion detection in WSN, which includes the definition of the intrusion, types of intrusions/attacks in WSNs, the motivation and need for intrusion detection and the challenges of developing a good candidate intrusion detection scheme for WSN.

The definition of the Intrusion/Attack: Heady (1990) defines the intrusion as any set of actions that are attempting to compromise the main components of the security system: the integrity, 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. Zamboni (2001) adds the statement of success or failures of these actions so it also refers to the attacks against the computer system.

In the theme of wireless sensor network, the concept stills the same since the intrusion also target any of the components mentioned above. The nature of WSNs and its special characteristics like the harsh deployment, energy constraints and the media of communication makes them very susceptible to the intrusions more than other networks.

Types of attacks in WSN: Shi and Perrig (2006) categorized the attacks on sensor networks into three main categories:

Outsider versus insider attacks: based on the node that is launching the attack, if it belonging to the network so it is considered as insider attack, otherwise it is considered as outsider attack.

Passive versus active attacks: based on the impact that results from an attack. Passive attacks just monitor or eavesdrop on the data packets, whereas the active attacks do modify the data streams or reported false alarms to the base station.

Mote-class versus laptop-class attacks: based on the capability of the attacker in compromising the network. In mote-class attacks, a few nodes with a similar capability to the network nodes are used as attackers, whereas in laptop-class, an attacker uses powerful devices like laptops with higher transmission range, processing power and energy to compromise the network.

According to the security requirements needed for WSN, another classification of attacks is introduced in (Shi and Perrig, 2006) as the following:

- Attacks on secrecy and authentication: the standard protection against this category is by using the standard cryptographic techniques
- Attacks on network availability: usually referred as Denial of Service (DoS) attacks. This type could target any layer of the network
- Attacks against service integrity: known as stealthy attacks that can fool the network and make it accept false data streams by compromising a node and inject false data through it

Wang *et al*. (2006) used the classification work of (Shi and Perrig, 2006) and go further in classifying the DoS attacks that could target each layer of the WSN. A summary of the Wang *et al*. (2006) classification is in the following Table 1.

The motivation for Intrusion Detection in WSN: Generally, the deployment of WSN in an unattended environment and the use of wireless signals as the media for communication make it easy for eavesdroppers to get the signals. Moreover, the limitations in processing, storage and battery lifetime make the security issues of these networks difficult. Different types of attacks against WSN have been explored in the literature like, attacks on sensed data, selective forwarding attacks, sinkhole attacks, hello flood attack and many more (Karlof and Wagner, 2003).

Table 1: Taxonomy of attacks according to WSN layers (Al-Karaki and Kamal, 2004)

Physical layer attacks	Jamming attacks
	Tampering attacks
Data link layer attacks	Collision attacks
	Exhaustion attacks
	Unfairness attacks
Network layer attacks	Spoofed/alter routing information
	Selective forwarding
	Sinkhole attacks
	Sybil attacks
	Wormhole attacks
	Hello flood attacks
	Acknowledgment spoofing attacks
Transport layer attacks	Flooding attacks
	Desynchronization attacks

Furthermore, the fact that WSN is composed of numerous cheap and tiny devices and usually used in an open or harsh area, make them very vulnerable to different types of attacks (Rajasegarar *et al*., 2008; Wang *et al*., 2006). For example, the security of the WSN applied to the battlefield is very critical if the sensor nodes are invaded by the enemy.

All the proposed security solutions in the literature can be grouped into two main mechanisms: preventive-based and detection-based mechanisms. Preventive-based mechanisms, i.e., encryption and authentication, can be considered as the first level of defense against security breaches and can protect the network from outside known compromises. Some of these preventive based mechanisms even fail to prevent from some outsider attacks and cannot prevent from the insider attacks that is caused by some compromised nodes from the inside of the network itself (Silva *et al*., 2005). For those reasons, detection-based mechanisms are used after the preventive mechanisms fail to isolate the attacks and hence considered as the second level of defense. The detection based mechanisms help to protect the network from insider attacks as well as from the undetected outsider attacks.

The taxonomy framework of intrusion detection schemes used in WSN: The straightforward method to detect attacks in WSN is to build a profile of normal pattern behavior of the data and then use this profile to detect attacks. The new observed patterns whose characteristics are significantly different from the normal profile indicate a possible kind of attack. According to the prior knowledge available for attack detection, these schemes can be classified into three main basic categories: supervised learning based, unsupervised learning based and semi-supervised learning based schemes (Tan, 2007).

Supervised learning based schemes: involves training or any kind of prior knowledge 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. Their dependency on rules gives them an advantage over training based techniques; however, they have many drawbacks that will be discussed later in this review.

Semi-supervised based schemes: in this category, the training data has labeled instances of one class which is the normal class.

This feature gives them an advantage over supervised techniques and make them suitable for some kinds of applications that has an available one class data (Chandola *et al*., 2009). According to the best of our knowledge, we cannot find any scheme based on this category for intrusion detection in WSN and instead we found some schemes designed for general anomaly/outlier detection like the one-class SVM scheme used for anomaly detection (Rajasegarar *et al*., 2007; Zhang *et al*., 2009).

Unsupervised based schemes: in these schemes, techniques do not require training data and instead of that they make some assumptions 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. The measure used for calculating the deviation from normal behavior in these schemes like: distance measures are very computationally complex and hence not always suitable for the restricted resources WSN. Some clustering based and data mining approaches are proposed for the intrusion detection in WSN (Baig, 2011; Kaplantzis *et al*., 2007; Loo *et al*., 2006) and many more will be described later in this review.

The challenges of designing an IDS for WSN: There are many challenges that make the development of an ideal intrusion detection scheme for WSN non trivial. In the following, we state the main challenges that should be considered when designing ideal IDS for WSN.

Resource constraints: Usually, in classical networks, the IDSs are installed on powerful computers like mainframes on which they can operate efficiently. However, in WSN this is not possible because of the resource constrained sensors in terms of computation, memory and power consumption. Since WSN is composed of numerous number of tiny and cheap sensors and these sensors has very limited power, limited storage capacity, limited memory, limited power processing capability and limited signal bandwidth, it makes it very difficult to design an effective intrusion detection system.

Dynamic topology change: the continuous change in topology because of the movement of the sensor in some WSN applications makes it difficult for the IDS to cope with this dynamic change.

Continuous data streaming: huge amounts of data streaming results in the need for an online intrusion detection system to cater to this kind of data. In some applications, the online detection of intrusions is very critical and cannot be postponed.

Different types of routing protocols: different types of routing protocols are used to meet the requirements of different types of WSN applications. Therefore, the design of intrusion detection scheme for one kind of routing protocols could not be fit easily for other protocol and result in a very specific detection scheme.

Difficulty in building intelligent IDS models: because of the lack of the labeled dataset that contains both normal profiles and attacks, the use of artificial intelligence techniques that requires training is difficult if not impossible.

Lack of standards: According to the best of our knowledge, there is no intrusion detection model specific for WSN like other types of networks. The existence of such model will ease the process of standardization and make the evaluation of any proposed IDS scheme feasible compared to other schemes.

The requirements of intrusion detection in WSN: After clarifying the main challenges for designing any IDS for WSN, we are ready to set up the basic requirements that should be taken during the design of any scheme for intrusion detection in WSN. From the literature, we found that, some important requirements should be taken carefully during any design for a good IDS scheme as the following:

- Generality: since most of the proposed schemes are very specific, we need such general schemes that can detect as many attacks as possible
- Independent of prior knowledge: since the labeled data is not available and the collection of such data and classifying it into normal and attacks is non-trivial task
- Distribution: because the collection of the audit is distributive as well as the analysis together with the collaboration between the nodes, the implementation of the IDS agent should also be distributed to avoid the communication overhead caused by exchanging the information between the nodes
- Fast detection: to cope with the continuous streaming of data in some WSN applications
- High detection accuracy: this feature is a key characteristic of any IDS for any kind of networks

In addition, according to Krontiris (2008) the good IDS solution should fulfill some requirements that include the following:

- Localize auditing: since there is no centralized point for collecting audit data far from the base station in WSN, the proposed IDS should rely on the locality of collecting data in each sensor node.

The partially collection of data will introduce the challenge of increasing the false alarms

- Minimizing the use of the constrained resources: the scarcity of resources in these networks make it difficult to design a lightweight and at the same time efficient IDS. The limited power, memory, processing capability and limited bandwidth should be considered before developing the model
- Ensuring the availability of services and resources all the time: this means if some of the nodes are compromised this should not stop the function of the network. The network should still provide its services to the interested parties
- Fault tolerance even in the presence of the attack: the IDS should ensure the tolerability and recover from being attacked
- Ensuring the real time response for any kind of attacks: because there is a huge streaming of data over the time, a suitable real time solution is required
- Supporting scalability: because some of the nodes get damage and some others are needed to be added from time to time

Rule-based intrusion detection schemes in WSN: Also called specification based intrusion detection schemes. In these schemes, the detection rules are first designed by domain expert before the starting the detection process. Most of the techniques in these schemes follow three main phases: data acquisition phase, rule application phase and intrusion detection phase (Silva *et al*., 2005). In the following sub-sections, the key important schemes in this category are explored.

Decentralized IDS in WSN: Silva *et al.* (2005) propose the first and 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: data acquisition phase in which the monitor nodes are responsible of promiscuous listening of the messages and filtering the important information for the analysis; 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; 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.

According to Xie *et al*. (2011), this scheme brings a good framework to the class of rule-based intrusion detection. But, there is an important drawback of this scheme, which is the ambiguity in determining the number of monitoring nodes dedicated to the detection process, the way of choosing them and how to make sure that the way of selection will cover the entire network. In addition, this scheme is restricted to some types of attacks and the question which may rise up is what if new types of attacks emerge? All these drawbacks should be considered when designing any kind of intrusion detection scheme.

Malicious node detection in WSN: Pires *et al*. (2004) present 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.

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 has been proposed by Onat and Miri (2005). 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 in (Pires *et al*., 2004), the building of the rules based on the received power rate is impractical since there are other factors that may affect this feature.

Towards intrusion detection in WSN: Krontiris *et al.* (2007) introduce a lightweight scheme for detecting selective forwarding and blackhole attacks in WSN. The key idea of their scheme is to make nodes monitor their neighborhood 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.

This scheme benefits from the neighbors monitoring so that there is a kind of distribution that will minimize the computation load on a detection agent node. However, there will be an increase in the communication messages between nodes during the collaboration for voting that will increase the communication overhead and as a result will deplete the power of nodes quickly. It is clear that, this scheme lacks the generality that other schemes in the same category.

Intrusion detection scheme of sinkhole attack in WSN: More specific intrusion detection scheme to detect sinkhole attack was proposed by Krontiris *et al*. (2008). This scheme is composed of four modules: Local Packet Monitoring Module, Local Detection Engine Module, Cooperative Detection Engine and Local Response Model. The proposed scheme has been implemented in the TinyOS environment with MinRoute protocol. A suitable detection rules have been prepared to suite with the sinkhole attack.

Generally, this scheme satisfies the distribution feature of IDS which is highly required on a large scale and autonomous environment like WSN. The problem here still with the communication overhead between the nodes to exchange useful information that helps in detecting the attack.

Neighbor-based intrusion detection for WSN: Stetsko *et al*. (2010) present an 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.

A new collaborative approach for IDS on WSN: Recently, a collaborative IDS scheme has been proposed by Lemos *et al*. (2010) 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.

Although, this scheme seems robust in protecting the network by using two layers of protection, there are some drawbacks that limit the usefulness of this scheme. To begin with, the supervisor nodes could be sources of failure if they have been compromised. Another drawback is related to the generality which is a major problem for the most rule-based schemes for intrusion detection. Many assumptions have been made for designing this scheme which caused inflexibility of application.

Fuzzy logic intrusion detection scheme for directed diffusion based sensor networks: Chi and Cho (2006) propose an intrusion detection scheme based on fuzzy logic. Some features of the traffic were extracted to build the fuzzy rules which are: node energy level, message transmission rate, neighbor nodes list and error rate in the transmission. The scheme was constructed to prevent and detect from the denial of service (DoS) attack which always drains the resources of the system. The base station or some monitoring nodes will be responsible for collecting the information messages from the neighborhood and the detection value will be calculated by the fuzzy controller based on the four features mentioned above

It is not clear how to choose the monitor nodes and how many nodes will be enough to protect the network. In addition, the need for an expert or sufficient experience to prepare the rule causes unadaptability of the scheme to detect new emerging attacks. Another drawback is that the chosen monitor node can be a point of failure if it is being compromised itself.

Fuzzy logic intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks: Another fuzzy logic based intrusion detection approach has been proposed by Moon and Cho (2009) to detect sinkhole attacks in directed diffusion based sensor networks. Two features related to the directed diffusion protocols are used which are the reinforcement ratio and the radius. The reinforcement ratio is the proportion of the reinforcement messages transmitted in an area to the number of sensing events from the nodes. The radius is defined as the number of hop counts between any two nodes in the area. In the case of the sinkhole attack, there will be more reinforcement message traffic in area than the normal number and the number of hop count will be smaller. The fuzzy logic controller will use these two features as an input to generate its output which is the detection value. If the result detection value is greater than a predefined security threshold, the controller will raise an alarm that a sinkhole attack has taken place in the area. Prior to the calculation of the detection value, the fuzzy rules should be set by an expert according to the symptoms of the sinkhole attacks.

Using fuzzy logic gives the flexibility of detection sinkhole attacks since the input values are not always sharp values. However, the main problem of any fuzzy based scheme is the need for manual setting of rules.

Intrusion Detection based on Traffic Analysis and Fuzzy Inference System in WSN: Ponomarchuk and Seo (2010) introduced 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 applies 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.

Advantages of Rule-based intrusion detection schemes for WSN:

- 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
- The computational complexity is not discussed here: since the schemes use only simple rules for detecting attacks
- Higher detection accuracy: since it depends on comparison with some predefined rules,

Shortcomings of Rule-based intrusion detection schemes for WSN:

- 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
- 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
- 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
- The absence of standardized evaluation metrics: it is obvious that most of schemes use different metrics to evaluate the effectiveness of the scheme

In the following Table 2 we summarize the rule-based techniques analyzed above and show the attacks that are targeted and the performance evaluation metrics used to evaluate them.

From the above Table 2, we can see that most of schemes are targeted for detecting specific attacks. We can also see that different evaluation measures used by different schemes which imply the absence of the standards of evaluation metrics. Computational complexity is not important to be evaluated in these schemes because; these schemes are very simple and do not need high computational capabilities since they only compare with very simple predefined rules.

Data mining and computational intelligence based schemes: Data mining and Computational Intelligence (DM/CI) techniques have been used extensively in building intelligent intrusion detection schemes in computer networks because of their ability to detect unknown attacks that the traditional signature based schemes fail to detect. In WSN, the use of DM/CI techniques for building IDS schemes still in early stages because of the difficulty of employing such techniques on the limited resources. The following sub-sections survey the DM/CI based intrusion detection schemes used to detect attacks in WSN.

Clustering-based Intrusion detection for routing attacks in WSN: Loo *et al*. (2006) propose a 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.

The authors claimed that, 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.

Table 2: summary of Rule-based schemes

Techniques	Attacks	Performance evaluation metrics
Silva *et al*. (2005)	-Negligence -Exhaustion -Blackhole -Selective forwarding -Content alteration -DoS -Wormhole -Hello Flood -Jamming	-Detection Rate (DR) -False Positive (FP) rate
Pires *et al*. (2004)	-Hello Flood -Wormhole	-Malicious node detection percentage -Malicious message detection percentage
Onat and Miri (2005)	-Node impersonation (Sybil) -Power depletion (DoS)	-Probability of false alarms -probability of detection - Average detection time
Krontiris *et al*. (2007)	-Blackhole -Selective Forwarding	-False Negative (FN) rate -No. Of false alarms
Krontiris *et al*. (2008)	Sinkhole	-FN rate - Neighbors with successful detection
Stetsko *et al*. (2010)	-Selective Forwarding -Jamming -Hello Flood	-Relation between FP and FN with a certain value of detection threshold
Lemos *et al*. (2010)	-Node repetition	N/A
Chi and Cho (2006)	-DoS	-FP and FN rates -Energy and detection rate with time
Moon and Cho (2009)	-Sinkhole	FP and FN ratios
Ponomarchuk and Seo (2010)	N/A	-Average DR

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.

Detecting selective forwarding attacks in WSNs using SVM: Kaplantzis *et al*. (2007) propose 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.

Intrusion detection in wireless sensor networks based on multi- agent and refined clustering: A multi-agent intrusion detection scheme proposed by Huai-Bin *et al*. (2009) to detect attacks in WSN. In this scheme the mechanism of detection is different for various functions: cluster heads are responsible for monitoring all common member nodes in the cluster, while the common member nodes are responsible for monitoring the header of the cluster. Four types of agents are installed on each sensor node to cooperate in the detection. Each node will execute different operations of detection according to its role either cluster head or common node.

Two clustering algorithms are used in this scheme in two stages. The first stage, Self Organizing Map Neural Network (SOM) is adopted for roughly clustering. The result of applying this algorithm which is the number of clusters and the cluster centers is then supplied for the second stage. The second stage involves the K-Means clustering algorithms to refine the clusters generated in the first stage.

The monitoring of the cluster heads on the nodes and the monitoring of the nodes of cluster heads boost the security process. However, the communication overhead is increased by communication between the nodes and their cluster heads. Another important drawback, is the use of two clustering algorithms SOM and K-Means which cause a very high computational overhead and therefore consume the node‘s power in a short time.

Optimized intrusion detection using Genetic Algorithm (GA): Khanna *et al*. (2009) introduce a scheme to speed up the detection accuracy and reducing the false alarms by choosing the appropriate nodes that will host the detection agents. Genetic algorithm was used to evaluate sensor node attributes and check its ability to be the Local Monitoring Node (LMN) that works as a trusted agent for the base station and capable of securely monitoring its neighbors. Some node attributes are evaluated like packet statistics, utilization data, battery status and the quality of service. The node fitness is then measured based on these attributes and as a result the GA chooses the node that is suitable and satisfying all these requirements to be the LMN.

The authors argue that, this scheme is extremely appropriate to cooperate with any detection schemes for conserving resources usage and cannot be used alone for the detection. The main drawback of this scheme is the high computational complexity of using GA because of the convergence time needed when the scale of the WSN is growing up.

Ant-based intrusion detection schemes for wireless sensor networks: Muraleedharan and Osadciw (2009), Banerjee *et al*. (2005) and Juneja and Arora (2010), propose intrusion detection schemes inspired by the ant colony algorithm. The idea behind these schemes is the use of multiple ant agents in parallel search algorithm to deploy pheromone values on nodes. The attacks in the network are detected using these pheromone values. The nodes in these models initially determine some direct and indirect paths amongst their neighbors. When the ant detects any path, it communicates the characteristic of the path through pheromone balancing to the other ants. After that, if there is any imbalance in pheromone values, an alert is raised to inform the administrator about a possible attack.

The main advantage of such kinds of schemes is the self organizing principle that is based on the probabilistic behavior. But, there are some drawbacks for such schemes include the high communication overhead caused by the congestion and the high storage consuming. The source node sends ant packets to all nodes through all possible paths that make congestion which result in high power consumption. In addition, each node has to store a very large list of pheromone values which utilizes the limited memory of the sensors.

Design and implementation of EAR algorithms for detecting routing attacks in WSN: Juneja *et al*. (2010) present an intrusion detection scheme for routing attacks in WSN based on EAR algorithm. It is an extension to their ant based scheme proposed in (Juneja and Arora, 2010). This scheme is based on three factors which are the Energy, Age and Reliability of the ant. The ants are classified into two main types: forward ants and backward ants. The forward ants report the information of the nodes in the path from the source node to the destination node, whereas the backward ants make use of the collected information to update the routing tables of nodes on their path and analyze the collected information to detect attacks.

Every node in the network has a log table that contains the information about their remaining energy, age of ant, the ratio of sent and delivered packets. The job of backward ants is to test values related to the stored values of the node and compares them with a predefined threshold value to verify that the path is reliable. The authors claimed that, different types of attacks that could be identified using this scheme include sinkhole, black hole and jamming attacks. It is clear that the main drawback of this scheme is the high power consumption because of the ant‘s processing in two directions at every node in the network. This also causes a high communication overhead and congestion. The store of the three statistics energy, age and reliability is not reasonable when the number of sensors is very high and the number of ant used is also high.

Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks: Doumit and Agrawal (2003) introduce a Hidden-Markove Model (HMM) based intrusion detection scheme for detecting possible attacks in WSN. In this scheme, the normal behavior profile of the nodes is first stored in a knowledge base and then compared with any suspicious activities of the node to handle the inconsistencies. The scheme is based on the HMM principle that states that the probability of a node being in a certain state depends only on its previous state. Although this scheme offers the scalability of adding new nodes, it only tackles the problem from a single node ‘view rather than a network ‘view.

An Integrated Intrusion Detection System for Cluster-based WSNs: Wang *et al*. (2011) proposed an 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.

The proposed IHIDS contains an anomaly detection module, misuse detection module, learning module and decision making model. The anomaly detection module can filter a large number of traffic packets because the sink node has unlimited capabilities. The normal output traffic from the anomaly module is passed and the abnormal traffic forwarded to the misuse module in order to identify the type of the attacks. If the misuse module could not identify the type, it is then forwarded to the learning module to learn the new attack type. The decision making module decides the type of attack and reports to the administrator.

The HIDS part which is employed in the cluster heads is similar to the IHIDS except that this part does not contain the learning mechanisms due to the limited cluster head resources. Instead, it updates their misuse knowledge base directly from the learning module in IHIDS. Because the resource of the common sensor node is very limited, it only contains simple misuse detection that matches the packets with the attack model to decide about any occurrence of any attack and inform the administrator.

The advantage of this scheme is the suitable design of the detection modules based on the capabilities and the probabilities of getting compromised. However, there are many drawbacks related to the detail design of the scheme. The use of Back Propagation Neural network (BPN) in building the misuse detection module implies a high computational complexity to be used in common sensor nodes that have very limited resources. In addition, the use of KDD'99 dataset to evaluate the scheme is not common in evaluating the IDS schemes for WSNs because of the different packet format and special need of WSN.

After analyzing the selected schemes above, the advantages and shortcoming of such schemes are presented in the following sub-sections.

Advantages of DM/CI based IDS schemes in WSNs:

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

Shortcomings of DM/CI based IDS schemes in WSNs:

- 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
- High computational complexity: because they involve the use of some complex machine learning algorithms or some difficult clustering approaches
- 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

The following Table 3 summarizes the mentioned schemes and shows their shortcomings.

Game theory based intrusion detection schemes in WSN: The essence of the interaction between the intrusion detection agent and the attacker can be represented scientifically by a game between two players. In these games, different strategies can be used by the intrusion detection agent in order to defend against the different strategies that attackers always use. In the following, some game theoretical based intrusion detection schemes in WSN are presented.

Detecting network intrusions via sampling: a game theoretic approach: Murali and Lakshman (2003) introduced a game theoretic framework for effective detection of network intrusions by developing a network packet sampling strategy. In this framework, the intruder will choose the paths that minimize the chances of detection while packet sampling strategy is used to maximize the chances of detection by the network operator. The game theoretic problem is first formulated and then the sampling schemes are developed so that to be optimal with the game approaches without exceeding a given total sampling budget.

This framework is among the first attempts to tackle the problem of intrusion detection using the game theory. The idea behind choosing the paths either from the intruder or the network operator leads to the common routing issues specifically in the routing protocols that are based on the shortest path to determine its way to the base station. This advantage would make this framework suitable for detecting some kinds of attacks in the routing layer that are based on the routing path information. However, this framework still needs extensive simulation experiments to prove its viability and effectiveness to detect attacks.

Table 3: summary of DM/CI based intrusion detection schemes in WSN

Scheme	DM/CI technique used	Shortcomings
Loo *et al*. (2006)	Fixed width clustering	High computational complexity because of the use of IDS agents in each node
Kaplantzis *et al*. (2007)	Support Vector Machines (SVM)	Centralized solution cause high communication overhead
Huai-bin *et al*. (2009)	Clustering/ SOM +K-Means	Very high computational complexity
Khanna *et al*. (2009)	Genetic Algorithms (GA)	High computational complexity needed for convergence
Muraleedharan and Osadciw (2009)	Ant Colony	High communication overhead
Juneja *et al*. (2010)	Ant Colony	High computational complexity high communication overhead
Doumit and Agrawal (2003)	Hidden Markove Model (HMM)	Nodes' level processing rather than network view
Wang *et al*. (2011)	Back Propagation NN (BPNN) Adaptive Resonance Theory (ART)	High computational complexity of BPNN to be use in misuse detection in common sensors

Intrusion detection in sensor network: a non cooperative game approach: Agah *et al*. (2004) proposed a non-cooperative game framework for the defense of nodes in WSN. 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 authors claimed that 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.

Detection of denial-of-message attacks on sensor network broadcasts: A detection scheme of Denial of Message (DoM) attacks in WSN is introduced by McCune *et al*. (2005). This scheme is designed for the broadcasting protocols in which the messages are broadcasted to the nodes periodically. The scheme is based on the Secure Implicit Sampling (SIS) method that enables the broadcasting base station to detect the failure of nodes to receive its broadcast in a probabilistic manner. The idea behind the SIS is that it works by extracting the authenticated acknowledgments from an unpredictable and tunable subset of nodes per broadcast so that it will minimize the acknowledgment implosion on the base station. The game theoretic approach here is used to evaluate the SIS method in facing optimal attackers that try to maximize the number of nodes denying the broadcasting of network messages.

Although this scheme is opening the door for research in this important area and as shown in the study agrees well with the simulation scenarios, it has many limitations. The assumption that the nodes are always stable and immobile adds unrealistic constraints to the application of sensor networks for some critical environments. Another unrealistic assumption is that the node does not fail over time and this is not always true since there are many other reasons that may cause the failure of a node at any time.

An intrusion detection game with limited observations: Alpcan and Basar (2006) presented an intrusion detection game model based on the 2-player zero sum stochastic (Markov) approach. The model represents the interaction between two players which are the potential malicious attacker from one side and the IDS from the other. The observations of the sensors are captured and reported to the IDS as a finite state Markov chain. In this model, a numerical analyze has been used to study the optimal strategic solutions as well as the evolution of player‘s cost under the game parameters. The model also considers the case that the players optimize their strategies with the lack of information about the WSN characteristics by involving the Markov Decision Process (MDP) and Q-learning methods.

The main advantage of this model is the use of the dynamic learning methods with the lack of information. This feature enables the players to consider the future costs for optimizing their strategies by the continuous learning about the potential attacks. However this model needs to be evaluated by simulation experiments in order to validate the effectiveness of the Markov based IDS rather than the numerical analysis used in the evaluation.

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 (2009) 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.

Advantages of game theory based IDS schemes in WSN:

- 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
- The techniques used in these kinds of schemes are lightweight since no training is involved and are depending on some strategies

Shortcomings of game theory based IDS schemes in WS:

- It is obvious from the reviewed schemes that these schemes still concepts that need to be experimented extensively to prove their viability
- 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

Statistical based intrusion detection schemes in WSN: The use of statistical techniques is common for anomaly detection schemes designed for WSN. These schemes use the probability distribution of either the normal or abnormal data as an evidence of attack behavior. The probability distribution model is first built and then compared to any deviation of data traffic generated later by the network. The following sub-sections describe some key statistical based intrusion detection schemes used in WSN.

An anomaly detection algorithm for detecting attacks in wireless sensor networks: Phuong *et al*. (2006) 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.

Group-based intrusion detection system in wireless sensor network: Li *et al*. (2008) propose a scheme in which, the sensor network is partitioned into many groups using delta-grouping algorithm. In this algorithm, each group of sensors that are physically close to each other and has nearly the same sensing capabilities are grouped together. Some monitor nodes are chosen to monitor each group alternatively. After that a statistical distribution-based anomaly detection algorithm is used to detect the anomalies caused by attacks. According to the authors, this scheme takes into consideration multiple attributes of the sensor nodes in order to increase the accuracy of the detection.

The high computational complexity of the grouping algorithm and the statistical distribution algorithm is the main drawback since the common sensor node has limited resources. In addition, the monitoring node becomes a point of failure if compromised. However, this scheme has many advantages including the detection generality because of the use of several typical traffic features over the network.

Statistical wormhole detection in WSN: Buttyán *et al*. (2005) proposed two mechanisms which are the Neighbor Number Test (NNT) and the All Distances Test (ADT) for detecting wormhole attacks in WSN. In the first mechanism NNT, the increase of the number of neighbors of the sensor is used as an indicator that new links have been created by the wormhole attack. The second mechanism, ADT, the decrease of the lengths of the paths between the nodes is used as an indicator to the shortcut links created by the wormhole attacks. It is assumed that the sensor nodes send their neighbors information to the base station where the algorithm is applied on the reconstructed network graph by the received information.

Both mechanisms have been investigated by simulation and showed that they are effective in detecting wormhole attack with some limitations related to the radius of the area that is affected by the wormhole. The authors reported that high accuracy is achieved when the wormhole radius is comparable to the radius of the sensor radio range. However, these mechanisms only detect the presence of the wormhole attack but they do not provide any mean for localization of the affected area. Another drawback is related to the sending of neighbors’ information to the base stations by the sensor nodes and results in intensive communication overhead and consumes the power of the nodes on the way to the base station.

Malicious node detection in WSN using an Auto regression technique: A strategy based on the past/present values generated by sensor nodes is presented by Curiac *et al*. (2007). 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.

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.

Shortcomings of statistical based IDS schemes in WSN:

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

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

- Detection generality: to design intrusion detection schemes that can be used to detect different types of attacks
- Detection speed: there is a need for a fast intrusion detection scheme that satisfy the dynamic and continuous streaming of data in WSNs
- The use of the lightweight Artificial Intelligence techniques: since these techniques have been used successfully for intrusion detection in traditional networks, it is expected that the use of them here would enhance the anomaly intrusion detection accuracy and generality
- The use of optimization techniques: these techniques could cooperate together with other techniques for choosing the best strategies of detection and the placement of detection agents
- The integration between techniques from different categories: as proved their success in other domains, it would be interesting to try such integration. i.e., the rule-based and the DM/CI based schemes can be integrated together in such strategy of game theory to get the advantages of all of them
- Reducing the false alarm rates related to the DM/CI: since these schemes depend on the labelled data collected from the network, there is a high false alarm related to the application of them. It is interesting to look for solutions to mitigate this problem for the context of WSN
- Distribution of the intrusion detection: because there is no single point in WSN can be used to install the IDS agent and because the log data is collected in each sensor node, there is a need for a real distributed intrusion detection scheme that can also minimize the power consumption results from the communication overhead with the base station in case of centralized IDS installation
- Unsupervised anomaly intrusion detection: in fact, there is no labelled data set available for intrusion detection in WSN. In addition, the design of such data set is not easy and costly task. It would be interesting to focus on the techniques, especially artificial intelligence and data mining techniques that do not require prior knowledge

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. First, we state the fundamental issues of intrusion detection in WSN showing the types of attacks, the motivation and the need for the intrusion detection in WSN and the taxonomy of techniques used in the literature. After that, the challenges faced in developing an ideal intrusion detection scheme were explored followed by the requirements for a good candidate intrusion detection scheme. The classification of the-state-of-the-art intrusion detection schemes proposed for WSN is then presented based on the technique used by each scheme.

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.

ACKNOWLEDGMENT

This research was supported by the Reseach Management Center (RMC), Universiti Teknologi Malaysia, under the GUP project VOTE. NO (03J50).

REFERENCES

Agah, A., S.K. Das, K. Basu and M. Asadi, 2004. Intrusion detection in sensor networks: A non-cooperative game approach. Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications, 30 Aug.-1 Sept., IEEE Xolore Press, pp: 343-346. DOI: 10.1109/NCA.2004.1347798

Akkaya, K. and M. Younis, 2005. A survey on routing protocols for wireless sensor networks, Ad Hoc Netw., 3: 325-349.

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Netw., 38: 393-422. DOI: 10.1016/S1389-1286(01)00302-4

Al-Karaki, J.N. and A.E. Kamal, 2004. Routing techniques in wireless sensor networks: A survey, IEEE Wireless Commun., 11: 6-28. DOI: 10.1109/MWC.2004.1368893

Alpcan, T. and T. Basar, 2006. An intrusion detection game with limited observations. Proceedings of the 12th International Symposium on Dynamic Games and Applications, (DGA’ 26), pp: 1-9.

Baig, Z.A., 2011. Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks. Comput. Commun., 34: 468-484. DOI: 10.1016/j.comcom.2010.04.008

Banerjee, S., C. Grosan and A. Abraham, 2005. IDEAS: Intrusion detection based on emotional ants for sensors. Proceedings of the 5th International Conference on Intelligent Systems Design and Applications, Sept. 8-10, IEEE Xpore Press, pp: 344-349. DOI: 10.1109/ISDA.2005.53

Buttyán, L., L. Dóra and I. Vajda, 2005. Statistical Wormhole Detection in Sensor Networks. In: Security and Privacy in Ad-hoc and Sensor Networks, Molva, R., G. Tsudik and D. Westhoff (Eds.). Springer Berlin/Heidelberg, pp: 128-141.

Chandola, V., A. Banerjee and V. Kumar, 2009. Anomaly detection: A survey. ACM Comput. Surveys. DOI: 10.1145/1541880.1541882

Chen, X., K. Makki, K. Yen and N. Pissinou, 2009. Sensor network security: A survey. IEEE Commun. Surveys Tutorials, 11: 52-73. DOI: 10.1109/SURV.2009.090205

Chi, S.H. and T.H. Cho, 2006. Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks. Proceedings of the 3rd International Conference on Fuzzy Systems and Knowledge Discovery, (FSKD’ 26), Springer-Verlag Berlin, Heidelberg, pp: 725-734. DOI: 10.1007/11881599_88

Christin, D., P.S. Mogre and M. Hollick, 2010. Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives. Future Internet, 2: 96-125. DOI: 10.3390/fi2020096

Curiac, D.I., O. Banias, F. Dragan, C. Volosencu and O. Dranga, 2007. Malicious node detection in wireless sensor networks using an autoregression technique. Proceedings of the 3rd International Conference on Networking and Services, IEEE Computer Society, June 19-25, IEEE Xplore Press, Athens, pp: 83. DOI: 10.1109/ICNS.2007.79

Debar, H., M. Dacier and A. Wespi, 1999. Towards a taxonomy of intrusion-detection systems. Comput. Netw., 31: 805-822.

Doumit, S.S. and D.P. Agrawal, 2003. Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks. Proceedings of the Conference on IEEE Military Communications, Oct. 13-16, IEEE Xplore Press, pp: 609-614. DOI: 10.1109/MILCOM.2003.1290173

Farooqi, A.H. and F.A. Khan, 2009. Intrusion detection systems for wireless sensor networks: A survey. Commun. Comput. Inform. Sci., 56: 234-241. DOI: 10.1007/978-3-642-10844-0_29

Heady, R., 1990. The Architecture of a Network-level Intrusion Detection System. 1st Edn., Department of Computer Science, Mexico, pp: 18.

Huai-Bin, W., Y. Zheng and W. Chun-Dong, 2009. Intrusion detection for wireless sensor networks based on multi-agent and refined clustering. Proceedings of the International Conference on Communications and Mobile Computing, WRI, Jan. 6-8, IEEE Xplore Press, Yunnan, pp: 450-454. DOI: 10.1109/CMC.2009.172

Juneja, D. and N. Arora, 2010. An Ant based framework for preventing DDoS attack in wireless sensor networks. Int. J. Adv. Technol., 1: 1-11.

Juneja, D., S. Bansal, G. Kaur and N. Arora, 2010. Design and implementation of EAR algorithm for detecting routing attacks in WSN. Int. J. Eng. Sci. Technol., 2: 1677-1683.

Kaplantzis, S., A. Shilton, N. Mani and Y.A. Sekercioglu, 2007. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. Proceedings of the 3rd International Conference on Intelligent Sensors, Sensor Networks and Information Dec. 3-6, IEEE Xplore Press, Melbourne, Qld., pp: 335-340. DOI: 10.1109/ISSNIP.2007.4496866

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 11-11, IEEE Xplore Press, pp: 113-127. DOI: 10.1109/SNPA.2003.1203362

Khanna, R., L. Huaping and C. Hsiao-Hwa, 2009. Reduced complexity intrusion detection in sensor networks using genetic algorithm. Proceedings of the IEEE International Conference on Communications, , Jun. 14-18, IEEE Xplore Press, Dresden, pp: 1-5. DOI: 10.1109/ICC.2009.5199399

Krontiris, I., 2008. Intrusion Prevention and Detection in Wireless Sensor Networks, PhD dissertation, in, University of Mannheim, Mannheim,Germany,

Krontiris, I., T. Dimitriou and F.C. Freiling, 2007. Towards intrusion detection in wireless sensor networks. Proceeding of the 13th European Wireless Conference, (EW' 07), CiteSeer.

Krontiris, I., T. Dimitriou, T. Giannetsos and M. Mpasoukos, 2008. Intrusion detection of sinkhole attacks in wireless sensor networks. Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks, (AAWSN' 28), Springer-Verlag Berlin, Heidelberg, pp: 150-161.

Lemos, M.V.D.S., L.B. Leal and R.H. Filho, 2010. A new collaborative approach for intrusion detection system on wireless sensor networks. Novel Algorithms Techniques Telecommun. Netw. DOI: 10.1007/978-90-481-3662-9_41

Li, G., J. He and Y. Fu, 2008. Group-based intrusion detection system in wireless sensor networks. Comput. Commun., 31: 4324-4332. DOI: 10.1016/j.comcom.2008.06.020

Loo, C., M. Ng, C. Leckie and M. Palaniswami, 2006. Intrusion detection for routing attacks in sensor networks. Int. J. Distributed Sensor Netw., 2: 313-332. DOI: 10.1080/15501320600692044

McCune, J.M., E. Shi, A. Perrig and M.K. Reiter, 2005. Detection of denial-of-message attacks on sensor network broadcasts. Proceedings of the IEEE Symposium on Security and Privacy, May 8-11, IEEE Xplore Press, pp: 64-78. DOI: 10.1109/SP.2005.7

Moon, S.Y. and T.H. Cho, 2009. Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. Int. J. Comput. Sci. Netw. Security, 9: 118-122.

Muraleedharan, R. and L.A. Osadciw, 2009. An intrusion detection framework for sensor networks using ant colony. Proceedings of the 43rd Asilomar Conference on Signals, Systems and Computers, IEEE Xplore Press, Pacific Grove, California, USA, pp: 275-278. DOI: 10.1109/ACSSC.2009.5470103

Murali, K. and T.V. Lakshman, 2003. Detecting network intrusions via sampling: a game theoretic approach. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, Mar. 30-Apr. 3, IEEE Xplore Press, pp: 1880-1889. DOI: 10.1109/INFCOM.2003.1209210

Onat, I. and A. Miri, 2005. An intrusion detection system for wireless sensor networks. Proceedings of the IEEE International Conference on, Wireless And Mobile Computing, Networking And Communications, Aug. 22-24, IEEE Xplore Press, pp: 253-259. DOI: 10.1109/WIMOB.2005.1512911

Phuong, T.V., L. Hung, S. Cho, Y.K. Lee and S. Lee, 2006. An Anomaly detection algorithm for detecting attacks in wireless sensor networks. Proceedings of the 4th IEEE International Conference on Intelligence and Security Informatics, (ISI' 06), Springer-Verlag Berlin, Heidelberg, pp: 735-736. DOI: 10.1007/11760146_111

Pires, W.R., T.H. De Paula Figueiredo, H.C. Wong and A.A.F. Loureiro, 2004. Malicious node detection in wireless sensor networks. Proceedings. 18th International, Parallel and Distributed Processing Symposium, (PDS' 04), pp: 1-7.

Ponomarchuk, Y.A. and Seo D.W., 2010. Intrusion detection based on traffic analysis and fuzzy inference system in wireless sensor networks. J. Convergence, 1: 35-42.

Rajasegarar, S., C. Leckie and M. Palaniswami, 2008. Anomaly detection in wireless sensor networks. IEEE Wireless Commun., 15: 34-40. DOI: 10.1109/MWC.2008.4599219

Rajasegarar, S., C. Leckie, M. Palaniswami and J.C. Bezdek, 2007. Quarter sphere based distributed anomaly detection in wireless sensor networks. Proceedings of the IEEE International Conference on Communications, June 24-28, IEEE Xplore Press, Glasgow, pp: 3864-3869. DOI: 10.1109/ICC.2007.637

Reddy, Y.B. and S. Srivathsan, 2009. Game theory model for selective forward attacks in wireless sensor networks, Proceedings of the 17th Mediterranean Conference on Control and Automation, Jun. 24-26, IEEE Xplore Press, Thessaloniki, pp: 458-463. DOI: 10.1109/MED.2009.5164584

Shi, E. and A. Perrig, 2006. Designing secure sensor networks. IEEE Wireless Commun., 11: 38-43. DOI: 10.1109/MWC.2004.1368895

Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A.A.F. Loureiro and L.B. Ruiz *et al*., 2005. 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), pp: 16-23. DOI: 10.1145/1089761.1089765

Stetsko, A., L. Folkman and V. Matyáš, 2010. Neighbor-based intrusion detection for wireless sensor networks. Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), Sept. 20-25, IEEE Xplore Press, Valencia, pp: 420-425. DOI: 10.1109/ICWMC.2010.61

Tan, P.N., 2007. Introduction To Data Mining. 1st Edn., Pearson Education India, ISBN-10: 8131714721, pp: 792.

Walters, J.P., Z. Liang, W. Shi and V. Chaudhary, 2007. Wireless sensor network security: A survey. Security in Distributed, Grid. Mobile Pervasive Comput.

Wang, S.S., K.Q. Yan, S.C. Wang and C.W. Liu, 2011. An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks, Expert Syst. Appli., 38: 15234-15243. DOI: 10.1016/j.eswa.2011.05.076

Wang, Y., G. Attebury and B. Ramamurthy, 2006. A survey of security issues in wireless sensor networks. IEEE Commun. Surveys Tutorials, 8: 2-23. DOI: 10.1109/COMST.2006.315852

Xie, M., S. Han, B. Tian and S. Parvin, 2011. Anomaly detection in wireless sensor networks: A survey. J. Network Comput. Appli., 34: 1302-1325. DOI: 10.1016/j.jnca.2011.03.004

Yang, Z., N. Meratnia and P. Havinga, 2010. Outlier detection techniques for wireless sensor networks: A survey. IEEE Commun. Surveys Tutorials, 12: 159-170. DOI: 10.1109/SURV.2010.021510.00088

Yick, J., B. Mukherjee and D. Ghosal, 2008. Wireless sensor network survey. Comput. Netw., 52: 2292-2330. DOI: 10.1016/j.comnet.2008.04.002

Yun, Z., F. Yuguang and Z. Yanchao, 2008. Securing wireless sensor networks: A survey. IEEE Commun. Surveys Tutorials, 10: 6-28. DOI: 10.1109/COMST.2008.4625802

Zamboni, D., 2001. Using internal sensors for computer intrusion detection. Purdue University.

Zhang, Y., N. Meratnia and P. Havinga, 2009. Adaptive and online one-class support vector machine-based outlier detection techniques for wireless sensor networks. Proceedings of the IEEE 23rd International Conference on Advanced Information Networking and Applications Workshops/Symposia, May 26-29, IEEE Xplore Press, Bradford, pp: 990-995. DOI: 10.1109/WAINA.2009.200