Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Security Enhancement Using IDT in Wireless Sensor Network

[1]M.C.Charumathi, [2]P.Divya and [3]D.Nagapriya
[1,2,3]B.Tech Information Technology
[1,2,3]Velammal Institute of Technology, panchetti, Chennai-601203, Tamil Nadu, India
Guided by:Mr.S.Jegadeesan

***Abstract*—** Wireless Sensor Network is one of the most prominent technologies that have wide range of applications. Even though WSN has a lot of innovative features it has a huge concern towards security. This might be mainly due to the absence of a physical line of defence between the sensor nodes. But there are also other issues mounting the security concerns in a WSN. In order to make a WSN secure and confidential there should be 100% defence against any kind of intrusions in the network before it can harm any node. Therefore Intrusion Detection Techniques have their own vital importance in the area of WSN. This article proposes a detailed survey of various Intrusion Detection Techniques with a comparative study highlighting the advantages and disadvantages of various schemes.

I. INTRODUCTION

With respect to their top-notch features, Wireless Sensor Networks (WSN) are applied in various fields of science and technology. They are mainly used to gather data's regarding human activities and behaviour in many streams like health care industries, Roads, Parking lots, Public places etc… They are also used to monitor physical and environmental development such as Wildlife, Earthquake, landslide detection, Pollution, Sea life, water quality, Wild fire etc… They are also used for commercial purposes in building safety, manufacturing machines performance and so on . WSNs are deployed in physical harsh and hostile environments where nodes are always exposed to physical security risks damages. Further its self-organizing nature, low battery power supply, limited bandwidth support, distributed operations using open wireless medium, multi hop traffic forwarding, and dependency on other nodes expose it to many security attacks at all layers of the OSI model. Readers who are interested more on security in WSNs, may refer to [3], [4], [5] and [6] for further information. Security solutions like authentication, cryptography or key management can enhance the security of WSNs. Nevertheless, these solutions alone cannot prevent all possible attacks. As a wide range of attacks can be launched by compromised nodes in a WSN, a second line of defence like Intrusion Detection [23] is needed.

Intrusion Detection Techniques have already been implemented in wired networks and they are used to detect the misbehaviour of participating modes and notify other nodes in the network to take appropriate remedial steps. This scheme cannot be incorporated in WSN because of some of their unique characteristics like limited processing power, memory and battery. This is a significant security system against both inbound and outbound threats [20]. In recent past many Intrusion Detection Techniques have be incorporated for Wireless Sensor Networks. Still there is an immense need for a global survey on modern progress in this area. Despite the presence of some works like [20],[10],[11] and [12] till date there is no survey paper that compile all the compelling Intrusion Detection Techniques along with the approaches proposed by them. The primary task of any research would be conducting a comprehensive literature review, which led us to the preparation of this survey as the initial outcome of our research.

II. OVERVIEW OF SECURITY IN WSN

WSN's are sensitive to various security threats due to open wireless medium, multi hop distributed communication and deployment in alienated and physically unprotected areas [13]. Different attacks are discussed in [5] and [14] such as mote-class attacks and laptop-class attacks. In mote-class attacks, the attacker compromises few of the sensor nodes inside a WSN. In laptop-class attacks, the attacker has more powerful device(s) to launch more intense attack against WSNs. Security attacks against WSNs can be classified as active and passive [15]. Passive attacks are hush in nature and are deployed to extract crucial data from a node however they do not harm any network resource. Active attacks are used to harm, temper or drop packets. Physical layer of WSN is responsible for radio and signals management. Radio jamming is one of the severe attacks against WSN [5]. Another physical layer attack is the battery exhaustion attack. In a WSN battery plays a vital role and determines the lifetime of the network. Considering the limitations it's essential to develop power efficient mechanism for sustainable WSN. Unlike in the active mode the nodes consume less energy in the sleep mode. So in energy exhaustion attack the attacker never allows the nodes to go to sleep mode by sending unnecessary beacons to the nodes there by keeping them busy. Most of the WSNs use contention based Carrier Sense Multiple Access with Collision Avoidance mechanism (CSMA/CA). This mechanism tries to avoid collision; however it adds more complications in the form of hidden-node problem, MAC selfishness, and unfairness [14] and [15]. Possible remedies for such kind of attacks are small frames and rate limitations [14].

Network layer is responsible for relevant route selection from source to destination. In WSN, the multi hop route from source to destination is vulnerable to many active and passive attacks [15]. Active attacks include packet dropping attacks, packet-misdirecting attacks, rushing attack, Sybil attack, byzantine attack, routing table overflow attack, spoofed routing information, hello flood, and acknowledgement spoofing.

III. INTRUSION DETECTION TECHNIQUES

In reality it's difficult to design a network that is intrusion proof and cannot be bypassed by an attacker.

In fact, networks should seriously consider integration of self-awareness and fault tolerance capabilities i.e. not only to assume that problems will appear in one way or another, but also to provide some mechanisms that will detect and reduce the impact of a particular threat. In a network or a system, any kind of unauthorized or unapproved activities are called intrusions. An Intrusion Detection Techniques (IDT) is a collection of the tools, methods, and resources to help identify, assess, and report intrusions. Intrusion detection is typically one

part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure [16]. In [17], intrusion is defined as: "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" and intrusion prevention techniques are presented as the first line of defence against intrusions. A single perfect defence is neither feasible nor possible in wireless networks, as there always exist some architectural weaknesses, software bugs, or design flaws which may be compromised by intruders. The best practice to secure wireless networks is to implement multi lines of security mechanisms; that is why IDT is more critical in wireless networks. It is viewed as a passive defence, as it is not intended to prevent attacks; instead it alerts network administrators about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms) and false negatives (attacks not detected), where the IDTs attempt to minimize both these terms [18]. The actual detection mechanisms are implemented in specific elements known as IDT agents. The intrusion and compromise of a node leads to confidential information such as security keys being revealed to the intruders which results in the failure of the preventive security mechanism. Therefore, IDTs are designed to reveal intrusions, before they can disclose the secured system resources. The IDT that is being designed should satisfy the following requirements:

1. Should not introduce new weaknesses to the system.
2. Need little system resources and should not degrade overall system performance by introducing overheads.
3. Run continuously and remain transparent to the system and the users.
4. Use standards to be cooperative and open.
5. Be reliable and minimize false positives and false negatives in the detection phase.

There are three main approaches that an IDT can use to classify the attacks;

A. Misuse detection

In misuse detection approach, we initially define abnormal system behaviour, and then define any other behaviour. These actions of nodes are compared with well-known attack patterns. In this case, these patterns must be defined and given to the system. In misuse detection, the IDT analyses the data's it gathers and compares it to the available databases of attack signatures. Substantially, the IDT looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets are updated periodically. The disadvantages are that this technique needs knowledge to build attack patterns and they are not able to detect novel attacks. In addition, always someone has to update the database of attack patterns. These drawbacks significantly reduce the efficiency of this approach in terms of system management, as the administrator of the network always has to provide IDT agents with an up-to-date database.

B. Anomaly detection

It is the search for items or events which do not conform to an expected pattern but rather it checks whether the behaviour of the nodes can be considered as normal or anomalous. This approach initially describes the substantial attributes of a 'normal behaviour', which are established by using automated training. Later, any activity that deviates from these behaviours are triggered as intrusion . If a sensor node doesn't operate with regards to the predefined conditions of a distinct protocol then the IDT would decide that its a malicious node. Sometimes false alarms induce the IDT to make wrong decisions there by affecting the accuracy of detection. The main drawbacks of this system is that a legal node showing unseen behaviour might trigger false alarms and also sometimes illegal nodes that doesn't exhibit abnormal behaviour would be left unnoticed.

C. Specification-based detection

Specification-based techniques have been shown to produce a low rate of false alarms [19]. In certain cases misuse detection and anomaly detection schemes are merged giving birth to hybrid detection mechanisms. It mainly concentrate on diversion of nodes from normal behaviour which are not detected by using alarms or other techniques. The conditions that describes normal behaviour are defined manually so that any behaviour of the node is monitored with respect to these conditions. Manual updation of these specifications are a major drawback for this technique as it consumes more time. Another drawback is that it cannot reveal an abnormal behaviour which do not breach the defined specifications.

IV. TAXONOMY OF IDT APPROACHES INWSN

Till now we have discussed several security threats in WSNs and we also discussed about some IDTs. These security threats can be defended using certain remedial steps like IDT mechanisms that make use of numerous underlying principles. Majority of these principles are based on the expectation that there is a distinct contradiction between behaviour of a normal node and an attacker. Considering these assumptions it's clear that IDTs can be categorised with regards to the particular detection technique used for studying the audit data. Therefore IDTs can be organised into 3 groups: (a) misuse, (b) anomaly, and (c) specification based. Misuse detection is used to detect predefined patterns of intrusions while anomaly detection techniques are utilized to find unknown or new intrusions. Specification based detection is based on some deviations from normal behaviour

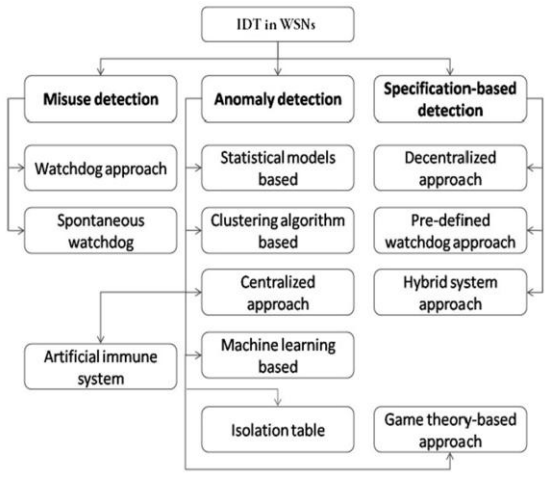

Fig 1 Taxonomy of IDT in WSNs

A. Misuse Detection Schemes

Misuse Detection in the context of WSN is a complex task. Practically its difficult to think exactly like an attacker or to know the motive of the attacker. The network administrator should design the attack patterns according to the threats happened in the past. Additionally the relentless memory constraints of WSNs make Misuse Detection based IDTs to work effectively as they need to store attack signatures approximately [20]. There are few research works that study Misuse Detection technique for WSNs, most of them follow the

watchdog approach, where packet monitoring takes place in several specific nodes in the network [21].

a. Watchdog approach

This technique mostly depends on the broadcast nature of the wireless communications and on the hypothesis that sensors are usually densely deployed. Every packet that is broadcasted in the network is not just simply received by the destination node but also by its neighbouring nodes that are present within the radio range of the sender node. Generally at these kind of situations the neighbour nodes should discard the packets since they are not the actual receivers, but for Intrusion Detection this can be used as a valuable audit data. Therefore a node can stimulate its IDT agent and supervise the packets sent by its neighbours by spying them. To detect attacks with high accuracy it's enough to supervise only one node as the system involves more information from other neighbour nodes as well. To detect the selective forwarding attack, a watchdog must spy on the packets arriving at a node and transmitted by that node. For example let's consider two nodes A and B. If we have to investigate whether B forwards packets sent by A then we have to stimulate watchdogs C and E within the radio range of A and B .

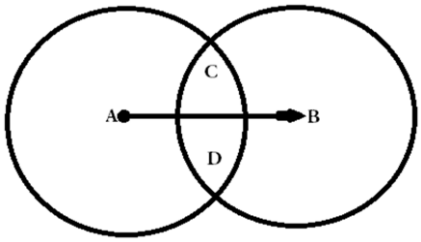

Fig 2 C and D are watchdogs for A and B

Drawbacks: The problem with this approach is that not all packets can be overheard by a global agent, due to the randomness of the selection process. Another drawback of the work is that it does not deal with the collision of packets, which is high likely due to the high density of nodes in various wireless sensor networks applications.

B. Anomaly Detection Schemes

There are many IDT mechanisms that use anomaly detection techniques. These systems usually depend upon the analysis of whether the behaviour of these sensor nodes can be normal or abnormal according to certain metrics. Many Anomaly Detection techniques have inherited some of the strategies that are used in Misuse Detection Techniques such as watchdog approach. To define what can be considered as normal behaviour, most Anomaly Detection Techniques employ simple assumptions [22] such as:

1. Payload of a packet should not be altered or modified.
2. Retransmission of a packet must occur in a certain time threshold.
3. Same packet can be resubmitted a limited number of times.
4. Packet sending rate must be within some limits, etc.

There are several Anomaly Detection Techniques, they are explained briefly as follows;

a. Statistical Model-Based Approach

[23] proposes an Anomaly Detection based security scheme for WSNs. In that method, each sensor node builds a simple statistical model of its neighbour's behaviour, and these statistics are used to detect various attacks such as node impersonation and resource depletion changes. The system features that are used to detect anomalies are the average of the received power and the packet arrival rate. At every node, only the last N packets received from each neighbour are used to calculate the statistics for that neighbour node and each arriving packet is then compared with those values. If the packet conforms to the statistics of the neighbour, it is accepted as a normal behaviour. Drawbacks: The system cannot detect selective forwarding and wormhole attacks due to the use of simple statistics. In [2], the same authors present the same main idea of anomaly detection but with different evaluation metrics. Instead of the previously implemented inter-arrival times, the new scheme uses mean and standard deviation metrics in the buffers. A packet is identified as anomalous if the absolute value of the difference between the mean of the received packet buffer and the mean of the intrusion buffer is greater than the standard deviation of the received packet buffer. Drawbacks: Again, no information is given about the number of nodes, how nodes were tested, and the analysis of the communications and computational costs.

b. Clustering Algorithm Based Approach

In [7], Loo et al. developed an intrusion detection scheme for

routing attacks that uses a fixed-width clustering algorithm to build a model of normal behaviour. Note that here we refer to clustering algorithm as unsupervised learning algorithms, not cluster based network structure (although this approach can be used in clustered networks). They use this model to detect anomalous traffic patterns. The IDT module is implemented on each sensor node and twelve network traffic patterns are identified. These features are used in the training and testing stages. In the training stage, a fixed-width clustering algorithm is used to build a set of clusters in the feature space. Clusters that contain less training traffic samples than a specific threshold are identified as anomalous. During the testing stage, each traffic sample is compared to the cluster set to determine whether it is anomalous or not. Drawbacks: Their method put too much computation on sensor node. The authors claim that Since the proposed IDT do not require communication between sensor nodes, it significantly reduces the power consumption.

c. Centralized Approach

A centralized, active Anomaly Detection system called ANDES was proposed by Gupta et al. in [9]. In this IDT the detection agent is located in the base station, collecting application data, management information (e.g. node's ID, hops towards the sink, total transmitted packets, total number of failures to route a packet), and node status information (e.g. normal, unavailable, duplicated and abnormal state), amongst others. All this information can then be combined and analysed in order to identify possible anomalies. Benefits: This system was implemented in Tiny OS [24] on Tmote sky sensor nodes. While the management information might impose a certain overhead as additional management traffic must be acquired, the results obtained from experiments are shown to be positive.

d. Artificial Immune System

In a departure from traditional Anomaly Detection Techniques, the necessity of Artificial Immune Systems (AIS) was discussed in [25]. In this work, Shaust et al. address these biologically inspired algorithms as a possible solution to detect misbehaviour in WSNs. They conclude in the paper that AIS is actually a good choice for misbehaviour detection in WSNs. In fact, various researchers have used this approach as part of their experiments. For example, Kim et al. [26] showed the similarities between the properties of WSNs and biological immune systems, and introduced a specific AIS, the Dendritic

Cell algorithm (DCA), which was used to detect interest cache poisoning attacks in directed diffusion routing. A sensor node that uses directed diffusion for routing packets maintains an interest cache table and a data cache table. When a node receives a packet, directed diffusion updates both caches and extracts the signals and antigens (e.g. bogus interest packets) from the received packets and caches. Such information is then passed to the DCA, which evaluates whether the antigens are benign or malicious. The algorithm was implemented in J-Sim and also was tested in TOSSIM, a WSN simulator [27]. Drawbacks: There is no information available about the performance of the DCA, and there are also no statistical analyses that might prove the effectiveness of the approach.

Another approach based on immunology theory was proposed by Liu and Yu [50], and an overview of its architecture can be seen in Fig. 3. Their algorithm is divided into four phases: (i) self-acquisition, (ii) generation, (iii) detection, and (iv) clonal selection. The novelty of this approach lies mainly in the clonal selection phase, which increases the response time of the detection system by accelerating the underlying mechanisms (detectors). Besides, a feedback system is used to reduce false-positive rates. This algorithm was also tested in TOSSIM.

e. Isolation table

In [28], Chen et al. proposed an Anomaly Detection method for three-level hierarchical WSNs (base station - primary cluster heads - secondary cluster heads) based on an isolation table. In this method the isolation table records the anomaly information, and the detection agents use it to isolate nodes from the network. Note that these tables can be generated by all cluster heads (secondary cluster heads monitor sensor nodes and primary cluster heads, while primary cluster heads monitor secondary cluster heads), and all tables are forwarded to the base station. As a result, isolation tables can be provided to any node that needs them (e.g. a newly elected cluster head that needs to know the actual state of the network). The applicability of this method was analysed using the ns-2 simulator. Drawbacks: The results of these simulations show that the method has disadvantages in terms of high energy consumption whenever the number of nodes is increased. In addition, the authors did not consider the influence of node failure and node tampering, which can lead to a growth of the false negative rate. The authors extended their work and provided more insightful details on [29] and [30], but the energy consumption problem is still present.

f. Machine Learning Based Approaches

There are some IDTs that rely on various machine learning techniques. For example, [31-34] introduce machine learning and automata-based learning approaches as an anomaly detection tool for wireless sensor networks. In [31], Misra et al. used a learning automata based approach (which is commonly used in optimization problems) to detect misbehaving nodes. This approach relies on packet sampling, where a proportion of the packets traversing the network are sampled to identify whether they are malicious nodes or not. Decisions are made depending on the feedback of the environment to the automaton in partially favourable or partially unfavourable cases. Benefits: Results obtained from analytical analysis show that the detection rate is high and the energy consumption is low for WSNs. The extended version of the work is presented in [35]. Doumit and Aggarwal [33] introduced an anomaly approach based on the structure of naturally occurring events. This approach makes use of hidden Markov models (HMM), which have been applied in IDT for wired networks. It also makes use of the concept of self-organized criticality (SOC), which links complex phenomena to simplistic underlying laws. In particular, SOC provides a prediction on the most probable event (e.g. expected temperature value). If the HMM finds that the event is out of bounds, it raises an alarm. Recent work by Rajasegarar et al. [36] used one class support vector machines (SVM) in order to detect network anomalies. The paper proposes two SVM based approaches that are called cantered hyper ellipsoidal support vector machine (CESVM) and quarter-sphere support vector machine (QSSVM), respectively. CESVM has advantages in terms of parameter selection flexibility and the computational complexity, but it faces certain limitations in distributed WSNs, as it uses a centralized approach. On the other hand, QSSVM works well in a distributed environment. Benefits: The results from real and simulated data sets show that both approaches achieve high detection accuracy.

g. Game Theory-Based Approaches

Other researchers have applied game theory-based models in intrusion detection mechanisms [8], [37-41]. Game theory based models can be excellent solutions for wired networks in terms of level of security, but for WSNs, it is necessary to prove their applicability. Sensors are equipped with constrained energy sources, and the performance of these models seems to decrease when the number of nodes is large. As an example of these approaches, we can mention the IDT developed by Agah et al. [38], which introduced a non-cooperative game approach to detect misbehaving nodes in clustered sensor networks. This non-cooperative game approach, which formulates an attack-defence game as a non-cooperative two-player nonzero-sum game, achieves Nash equilibrium (i.e. best results for both players) whenever the defence player (i.e. the IDT system) finds and protects the most vulnerable cluster. Consequently, clusters are classified according to their utility and the cost of defending them. Note that the authors also introduced two more techniques (intuitive metric technique and Markov decision process) that could be used to predict the future behaviour of the attacker. Drawbacks: The authors claim that this IDT approach can improve the detection rate. However, as every node is provided with a heavy IDT module and learning mechanism, the problem of high energy consumption and communication overhead arises.

C. Specification-Based Schemes

Some specification-based schemes have been proposed as IDT solutions for WSNs. As noted earlier, the main drawback of this approach is that the development of attack or protocol specifications is done by human beings. In this case, the administrator or the designer of the network has to manually define the specifications that describe what a correct operation is and monitor any behaviour with respect to those constraints.

a. Decentralized Approach:

One of the first works in this research track was introduced by Silva et al. in [42]. They proposed a decentralized IDT that is based on several predefined rules. The method has three phases: (i) data acquisition, where packets are collected in a promiscuous mode in order to filter out the important data before storing it, (ii) rule application, where the rules are applied to the stored data, and (iii) detection phase, where the number of raised failures are compared with the expected amount of occasional failures that defines whether an intrusion has occurred or not. Fig. 4 illustrates the architecture of a monitor node which has an IDT function in addition to sensing and message transmission capabilities. The results obtained from simulations, which tested attacks such as jamming, black

hole and wormhole, show that the method performs well in a simulation environment.

Drawbacks: The algorithm is simulated using a WSN simulator made by the authors, whose technical details are unknown. This makes it difficult to rely on the results presented by the authors, as a simplified WSN model may not be something that could be used in practice. Besides, other types of analyses (numerical or probabilistic or logical) should have been added alongside the presented outputs. Moreover, the algorithm has no information about how to select the actual location of the IDT agents in the application. There are many other works in this topic [43-51] that use different techniques (e.g. group-based and collaborative) to specify intrusion detection patterns and attack signatures. For instance, Bhuse et al. [46] introduced a specification-based approach for detecting masquerade (Sybil) attacks. They propose two techniques which complement each other when used concurrently. The first one is mutual guarding, where the sensor nodes check the source id of received packets for intrusion. The second technique was labelled by the authors as SRP, and consists of the verification of the number of packets sent and received by a certain node. Drawbacks: Simulation results show that the mutual guard method has considerable overhead and it fails to protect nodes when the attacker has a shorter communication range than the sensor nodes.

b. Pre-defined Watchdog Approach

Krontiris et al. have proposed various specification-based IDT in order to detect black hole [15], selective forwarding [15], and sinkhole [11] attacks in WSNs. Their approach is based on watchdogs, which have pre-defined rules for raising intrusion alerts. An example of one of those rules is as follows: "If more than half of the watchdog nodes have raised an alert, then the target node is considered compromised and should be revoked, or the base station should be notified". In defining a threshold value, the authors also take into consideration the loss of messages caused by network anomalies (e.g. wireless noise). The method has three common modules:

1. Local monitoring and detection engine, for collecting and analysing Data according to the rules;
2. Cooperative detection engine, for making accurate decisions collaboratively; and
3. Local response module, for taking appropriate actions if an intrusion is verified by the network.

Drawbacks: The method produces very low false-negative and false-positive rates, which is a

Good thing. However, the actual simulator and experimental settings, which are used to calculate the rates, are not clear. In a more recent work [16], the above authors proposed a cooperative IDT scheme which has been tested in a real environment. The method inherits various extended modules from the authors' previous works. The algorithm is based on defined intrusion detection conditions (IDC), and the authors argue that these conditions are necessary and sufficient to solve the problem of detecting the most important WSN threats. Benefits: In fact, to the best of our knowledge, this paper is one of the few works that give details on a practical implementation of IDT agents in a real environment. The results show that the proposed algorithm is lightweight enough to run on resource constrained sensor nodes such as telosb.

c. Hybrid System Approach

As stated earlier, the specification-based approach integrates the aims of misuse and anomaly detection techniques. However, some specific IDTs allow both detection techniques to coexist and interact in one single detection agent. That is, such agents will make use of automated training-based anomaly detection techniques and human-made rule-based misuse detection techniques. These approaches are known as hybrid systems. Hai et al. [53] proposed a hybrid intrusion detection system that integrates both anomaly and misuse techniques. The specific goal of this method is to detect routing attacks in WSNs. For energy efficiency, they use hierarchical WSNs. In the misuse detection module, the authors use pre-defined rules such as packet interval rule, integrity rule, packet delay rule, and radio transmission range rule. Drawbacks: Unfortunately, there is no proper and full explanation of the anomaly detection techniques used in this paper, that is, how to effectively analyse the collected data and how to make decision on the existence of intrusions. Later, the extended versions of the above work have been published by the same leading author (along with others) in [54-56]. The methods use two-hop neighbour knowledge in order to prevent routing attacks. Two-hop neighbour knowledge is basically used in broadcasting protocols to reduce the number of packet transmissions such as Source based Protocol and Dominant Pruning [57]. The two-hop neighbour list is established in each sensor node via a single phase, by modifying the Hello packet. Other parts of this work consist of local and global agents and pre-defined rules. The global agents use the two-hop neighbours' list and predefined rules to monitor transmissions in their neighbourhood. The method performs well for routing attacks. However, it needs to be tested in different attack scenarios in order to check the effectiveness of the method. Yan et al. [58] introduce a similar hybrid approach. The algorithm contains a misuse detection model, an anomaly detection model, and a decision making model. The novelty of their method is the use of a Back Propagation Network (BPN) for the anomaly detection module. First, the packet records are given to the anomaly detection model, so as to check for abnormal activities. If activity is determined as 'abnormal', then it will be forwarded to both the misuse detection model and the decision making model. Then, the misuse detection model analyses the received data with the help of BPN and sends them to the decision making model. Finally, the decision making model combines the outputs of both models to determine whether or not an output can be considered as an intrusion, and the category of attack. In case of intrusion, the model reports to the base station. Benefits: This approach has been tested by providing comprehensive and detailed simulation results, which can be accessed in [59]. Finally, a dynamic IDT labelled as DIDT was proposed by Huo and Wang in [60]. Drawbacks: The distributed mechanisms implemented in DIDT can be able to detect multiple intruders, although at the cost of increasing the energy consumption. Besides, these mechanisms are not tested in a real environment.

CONCLUSION

In this work, we have provided a detailed and comprehensive study on IDSs in wireless sensor networks, classifying them according to their underlying mechanisms. In addition, we have briefly introduced the existing security attacks in WSNs and their respective countermeasures. Furthermore, we have provided a critical analysis of the IDS mechanisms with respect to network structure, highlighting various vital areas that are currently underdeveloped. Based on our observations and findings we can conclude that, while the field of IDS for WSN has advanced significantly in these last years, there are still various research areas (e.g. IDS architectures, balance between accuracy and consumption of resources, novel scenarios, better integration of underlying mechanisms) that need to be further

developed. We hope that our results will be beneficial for both beginners and active researchers in this area.

References

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

[2] I. Onat, and A. Miri, A Real-Time Node-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks, in ICW 2005, pp. 422-427.

[3] Y. Zhou, Y. Fang and Y. Zhang, "Securing wireless sensor networks: a survey", IEEE Commun. Surveys Tutorials, vol. 10, num. 3, pp. 6-28, 2008.

[4] E. Cayirci and C. Rong, "Security in Wireless Ad Hoc and Sensor Networks", book published by Wiley, 2009.

[5] K.Venkatraman, J.Vijay Daniel, G.Muugabhoopathi, "Various Attacks in Wireless Sensor Network: Survey" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013

[6] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Commun. Surveys and Tutorials, vol. 8, num. 2, pp. 2–23, 2006.

[7] CE. Loo, MY. Ng, C. Leckie, and M. Palaniswami, Intrusion Detection for Routing Attacks in Sensor Networks, International Journal of Distributed Sensor Networks, vol. 2, pp. 313-332, 2006.

[8] A. Agah, S.K. Das, K. Basu, and M. Asadi, Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach, in 3rd IEEE International Symposium on Network Computing and Applications, September. 2004, pp. 343-346.

[9] S. Gupta, R. Zheng, and A. Cheng, ANDES: an Anomaly Detection System for Wireless Sensor Networks, in MASS 2007, pp. 1-9, 2007

[10] A.H. Farooqi and F.A. Khan, Intrusion Detection Systems for Wireless Sensor Networks: A Survey, in FGCN/ACN 2009, CCIS, vol. 56, pp. 234-241.

[11] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier Detection Techniques for Wireless Sensor Networks: A Survey", IEEE Commun. Surveys Tutorials, vol. 12, no. 2, 2010.

[12] T. Bhattasali, and R. Chaki, A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network, in 4th International Conference on Network Security and Applications (CNSA-2011), Springer, 2011, pp. 268- 280.

[13] Nabil Ali Alrajeh, S. Khan, and Bilal Shams, Intrusion Detection Systems in Wireless Sensor Networks: A Review, International Journal of Distributed Sensor Networks Volume 2013 (2013), Article ID 167575

[14] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks," in, vol. 1, pp. 529– 536, Hanoi, Vietnam, 2006.

[15] S. Khan, N. Mast, and J. Loo, "Denial of service attacks and mitigation techniques in IEEE 802.11 Wireless mesh networks," , vol. 12, pp. 1–8, 2009.

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

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

[18] S. Khan, K. K. Loo, and Z. U. Din, "Framework for intrusion detection in IEEE 802.11 wireless mesh networks," , vol. 7, no. 4, pp. 435–440, 2010.

[19] 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" Department of Computer Science, Stony Brook University, Stony Brook, NY 11794.

[20] I. Krontiris, T. Dimitriou, and F.C. Freiling, Towards Intrusion Detection in Wireless Sensor Networks, in 13th European Wireless Conference, Paris, France, 2007.

[21] S. Marti, T.J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad hoc Networks, in MobiCom'00, 2000, pp. 255-265.

[22] M.S. Islam, and S. AshiqurRahman, Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches, in Int. J. Advanced Science and Technology, vol. 36, November 2011.

[23] I. Onat and A. Miri, An Intrusion Detection System for Wireless Sensor Networks, Wireless and Mobile Computing, Networking And Communications, vol. 3, 2005, pp. 253-259.

[24] TinyOS, http://www.tinyos.net

[25] S. Shaust and H. Szczerbicka, Misbehavior Detection for Wireless Sensor Networks – Necessary or Not?, in 6th Fachgespr¨ach "Drahtlose Sensornetze" der GI/ITG-Fachgruppe "Kommunikation und Verteilte Systeme", Germany, 2007, pp. 51-54.