International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

REVIEW ARTICLE

ISSN: 2321-7758

A SURVEY ON INTRUSION DETECTION SYSTEM IN WIRELESS SENSOR NETWORK

NEHA R. JAISWAL[1], Prof. H. M. BARADKAR[2]

[1]PG scholar, Electronics & Telecommunication Dept. Jagadambha College of Engineering & Technology Yavatmal, India.

[2]Associate Professor & HOD,

Electronics & Telecommunication Dept.Jagadambha College of Engineering & Technology, Yavatmal, India.

Article Received: 20/04/2015 | Article Revised on:26/04/2015 | Article Accepted on:29/04/2015

ABSTRACT

Wireless sensor network (WSN) is a promising technology with number of application in various fields. Because of their unique nature like resource limitation, limited memory storage & limited battery power, they are susceptible to many attacks or intrusions. Now to detect this attack in order to protect WSN many intrusion detection system (IDS) are proposed .This paper aims to present survey on IDS in context of WSN. Firstly, Security attacks are described. Secondly information about IDS is provided. Thirdly IDSs proposed for WSN are discussed along with their advantage and disadvantage. This paper will be beneficial for researchers in conducting their research.

Key Words—intrusion detection, IDS, wireless sensor network, WSN, security.

INTRODUCTION

Wireless sensor networks extend people's ability to explore, monitor, and control the physical world. Owing to their easy and cheap deployment features, Wireless Sensor Networks (WSNs) are applied to various fields of science and technology. The wireless sensor network (WSN) is an infrastructure that senses environmental information such as temperature, humidity, sound and image, collects and provides the information to users

A WSN is composed of hundreds or even thousands of tiny, cheap sensors nodes which communicate with one another wirelessly and one or more sink nodes .When a WSN is deployed in a sensing field, these sensor nodes will be responsible for sensing abnormal events (e.g., a fire in a forest) or for collecting the sensed data (temperature or humidity) of the environment & it will send the message hop-by-hop to a special node, called a sink node.

Limitation & challenges of WSN :

1. Bandwidth, memory, battery power are scarce resources that need to be used with great consideration.
2. The lack of fix infrastructure (i.e., routers, base station, regenerator, etc.) makes the design of security related models & systems for WSNs more difficult.
3. Nodes are prone to a failure which adds hurdles in network operations.

4. Compromised nodes may leak information to the rest of the WSN thereby disrupting the network operation.
5. Wireless communication is susceptible to eavesdropping, which would reveal important data to adversaries and/or to jamming/interfering, which would cause DoS in the WSN.
6. There is no trusted authority; decisions have to be concluded in a collaborative manner.
7. Functions in unattended manner.

Owing to above specific nature of WSN and their limitations, it is necessary to protect it from various sorts of intrusions. There are numbers of intrusion detection systems developed for this reason. This paper gives information about few IDS in brief along with their benefits and drawbacks, which might help other researcher in preparing their work.

Security attacks

1. may listen to requests for routes, and then reply to the requesting node with messages containing a bogus route with the shortest path to the requested *Spoofed, Altered, or Replayed Routing Information :*

While sending the data, the information in transition may be spoofed, altered, replayed, or destroyed. Due to the short range transmission of the sensor nodes, an attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

2. *Selective forwarding :*

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

3. *Sinkhole attack:*

In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the compromised node destination.

4. *Black hole attack:*

The attack involves inserting a malicious node in the network. This node, by various means, will modify the routing tables to force the maximum neighboring nodes passing the information through him. Then like a black hole in space, all the information that will go in it will never be retransmitted

5. *Sybil Attacks:*

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

6. *Wormholes:*

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

7. *HELLO Flood Attacks:*

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

8. *Acknowledgement spoofing :*

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

9. *Sleep deprivation attack :*

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

10. *Denial of Service:*

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor

networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The table 1 shows layer wise DoS attack.

Taxonomy of IDS in WSNs

IDS in WSN are basically classified into three classes 1) Misuse Detection 2) Anomaly based detection 3)Specification based Detection as shown in fig 2. These three classes are then further classified into sub categories. The watchdog approach and spontaneous Watchdog approach comes under Misuse based detection. Anomaly based detection include statistical based, knowledge based, machine learning based ,game theory based, clustering algorithm based, centralize approach and artificial immune system based detection methods. Decentralize approach, Pre-define approach & hybrid system detection methods are defined under specification based detection.

TABLE 1 LAYER WISE DOS ATTACK

Layer	Attack
Physical	Jamming
Link	Exhaustion
	Collision
	Unfairness
Network	Spoofed routing information, and selective forwarding
	Sinkhole
	Sybil
	Wormhole
	Hello Flood
Transport	Session Hijacking.
	SYN flooding
Application	Data Corruption. Repudiation

1. *Misuse detection:*

It is also known as signature based or rule based. The signatures (profiles) of the previously known attacks are generated and are used as a reference to detect future attacks. The advantage of this type of detection is that it can accurately and efficiently detect known attacks; hence they have a low false positive rate. The disadvantage is that if the attack is a new kind (that was not profiled before), then the misuse detection would not be able to catch it.

2. *Anomaly based detection:*

This is based on statistical behavior modeling. Normal operations of the members are profiled and a certain amount of deviation from the normal behavior is flagged as an anomaly. The advantage of this detection type is that it is well suited to detect unknown or previously not encountered attacks. The disadvantage of this detection type is that the normal profiles must be updated periodically, since the network behavior may change rapidly. This may increase the load on the resource constrained sensor nodes.

3. *Specification based detection:*

A set of specification and constraints that describe the correct operation of a program or protocol is defined. Then execution of the program with respect to the defined specifications and constraints is monitored. Specification based intrusion detection techniques combine the advantages of both misuse and anomaly based detection techniques by using manually developed specifications and constraints to characterize legitimate system behavior. Specification based intrusion detection techniques are similar to anomaly based detection techniques, in that both of them detect attacks as the deviations from a normal profile. Since specification based detection techniques are based on manually developed specifications and constraints, they have low false alarm rate compared to the high false alarm rated anomaly based detection techniques. On the other hand, the cost to achieve the mentioned low false alarm rate is that the development of detailed specifications and constraints would be very time consuming.

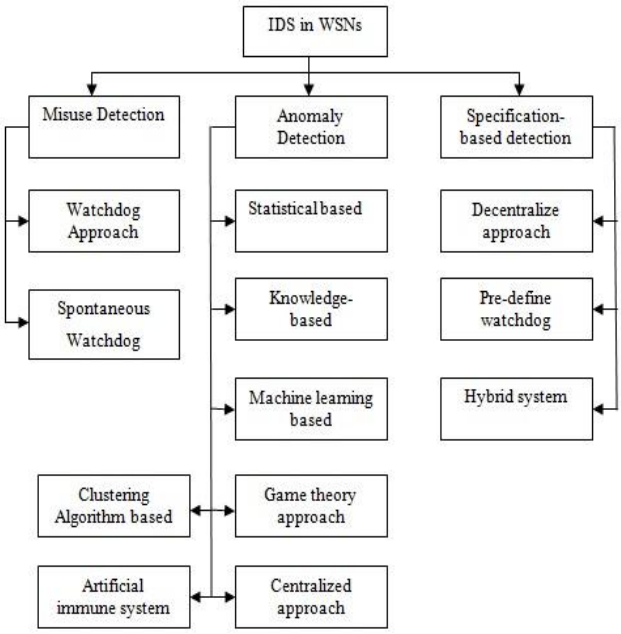

Fig. 1. Taxonomy of IDS in WSNs

IDSs Proposed For WSNs

1. Cluster-Based IDS :

In [1] by S. Shin et al. a hierarchical framework for intrusion detection as well as data processing is proposed. Throughout the experiments on the proposed framework, they stressed the significance of one hop clustering. Authors have constructed logical protocols which are an intrusion detection protocol and intrusion prevention protocol .The authors believed that their hierarchical framework was useful for securing industrial applications of WSNs with regard to two lines of defense.

The [2] C.C. Su et al., has proposed two line of defense to improve the security of WSNs. The first line of defense is intrusion prevention, which uses a model-based on authentication, which can resist to external attacks. Its basic technique is to add a message authentication code (MAC) for each message. Whenever a node wants to send a message, it adds to it a timestamp and a MAC is generated by a key-pair or individually depending on the key role of the sender (cluster-head, member - node, or base station). So that the receiver can verify the sender massage, the security mechanism used is LEAP (Localized Encryption and Authentication). In second line of defense the energy-saving intrusion detection approach is proposed to detect and revoke the compromised nodes with energy-saving consideration This approach focuses on the detection of misbehavior both in Member nodes (MN) and cluster-head nodes (CH) by monitoring each other, When misbehavior is detected, the CH broadcasts a warning message encrypted with the cluster key to restrain this specific node.

Advantage- From their experiment result, node energy is efficiently saved and network lifetime is extended when WSN is under attacks.

Disadvantage-The problem with this approach is its key management mechanism. Sensor nodes cannot move and new sensor nodes cannot be added after the pair wise keys are established.

In S. Rajasegarar [3], a distributed cluster based anomaly detection algorithm was proposed. They minimized the communication overhead by clustering the sensor measurements and merging clusters before sending a description of the clusters to the other nodes. The authors implemented their proposed model in a real-world project.

Advantage- They demonstrated that their scheme achieves comparable accuracy when compared to centralized schemes with a significant reduction in communication overhead.

Disadvantage- All kind of attacks is not tested.

In [4], 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 isolation table detects anomalies in table & If the node is anomalous, it will be isolated and recorded in the isolation table and Base station will be updated.

Advantages- The authors claim through primary experiment that their ITIDS can prevent attacks effectively.

Disadvantage- 1.The results of simulations show that the method has disadvantages in terms of high energy consumption whenever the number of nodes is increased.

2. When the remaining nodes decrease, the intruders can infiltrate WSN more easily

3. Statistical detection based IDSs:

In the proposed algorithm of S.S. Doumit et al. [5] the sensor network adapts to the norm of the dynamics in its natural surroundings so that any unusual activities can be singled out. In order to achieve this, they employ a hidden Markov model (HMM). 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.

Advantages- The authors claimed that

1. Their proposed algorithm is easy to employ, requiring minimal processing and data storage.

2. Robustness with low false-alarm rate as it adapts well to the surrounding phenomena, and flexible to modified task requirements.

Disadvantages- .mainly focused on the accuracy of the data gathered rather than the security of the nodes or the links.

4. Game theory based IDSs:

In [6] and [7], Agah et al. considered attack and detection as both participants of the game and formulated strategies for both parties. In order to increase detection probability, strategies were normalized into a non-cooperative, non-zero game model. The three different proposals put forward to protect the network nodes. The first method is used in non-cooperation to determine the invasion between ordinary nodes and the attacker. The second method is to use a Markov Decision Process to determine the cluster head node intrusion detection mechanisms. The third method is in each time slot by the largest traffic node protection mechanism to protect the cluster head.

Advantage- The authors claimed that the evaluation of their schemes reveals its effectiveness of successful defense against attacks.

Disadvantage- Only one of the clusters of the network is monitored at a time. This leaves the rest of the network un-protected.

5. Anomaly detection based IDSs:

In [8], S. Rajasegarar et al. proposed a solution to the problem of minimizing the communication overhead in the network while performing in-network computation when detecting anomalies. Their approach to this problem is based on a formulation that uses distributed one-class quarter-sphere support vector machines to identify anomalous measurements in the data. Data vectors are mapped from the input space to a higher-dimensional space for further investigations.

Advantage- The authors implemented their proposal in a real-world project and they claimed that their model was energy efficient in terms of communication overhead while achieving comparable accuracy to a centralized scheme

Disadvantage- Lacks in Periodical adjustments of parameter in system based on statistics from previous time window

6. Reputation (Trust) based IDS:

F. Bao et al. [9] proposed a hierarchical trust management for WSNs to detect selfish and malicious nodes. Authors developed a probability model utilizing stochastic Petri nets technique to analyze the protocol performance and validated subjective trust against objective trust obtained based on ground truth node status.

Advantages- Their trust-based IDS algorithm outperforms anomaly-based IDS algorithms in the detection probability percentage while maintaining sufficiently low false positive rates.

Disadvantage- the impact of the cluster size and the trust update interval to the protocol performance are not considered in this work.

For Other work refer [10].

7. Centralize IDS-

In [11] authors have compared related IDS solutions, they claim that their proposition is very simple and suitable for resource constrained sensor nodes. It doesn't use complex security mechanisms such as multipath routing, localization based or authentication and key distribution strategies. They propose a centralized based detection architecture, where base station is charged of analyzing and detecting anomalies behaviors. That reduces significantly the computation load on network sensor nodes.

Advantage- 1. Reduces the computation load on network sensor nodes.

2. Useful for Black hole & selecting forwarding attacks which represent a particular type of black hole attacks.

Disadvantage-authors don't claim that the proposed mechanism can prevent definitively all black hole attacks; however our proposal mitigates significantly the impact of the attacks

8. Decentralized Approach

V. Bhuse et al. [12] 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 labeled by the authors as SRP,

and consists of the verification of the number of packets sent and received by a certain node.

Disadvantage- 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.

In [13] authors consider two WSN models: homogeneous and heterogeneous WSN. They derive the detection probability by considering two sensing models: single-sensing detection and multiple-sensing detection. In addition, they discuss the network connectivity and broadcast reach ability, which are necessary conditions to ensure the corresponding detection probability in a WSN. Their simulation results validate the analytical values for both homogeneous and heterogeneous WSNs.

Disadvantage- The method relies on sensing range of nodes, so whether it is single-sensing detection or multiple-sensing detection, the method will utilize more energy than required.

There are many other works in this topic [1], [14] that use different techniques to specify intrusion detection patterns and attack signatures.

9. Machine Learning Based IDSs-

There are some IDSs that rely on various machine learning techniques. For example [15], [5] introduce machine learning and automata-based learning approaches as an anomaly detection tool for wireless sensor networks. [15] Provides theoretical framework without experimental results

[16] Propose an energy-aware protocol for intrusion detection in wireless sensor networks (WSNs).Detection system is implemented based on learning automata concept.

Proposed protocol is performed in three phases, Zoning and Initializing, Gathering Information and Learning and Intrusion Detection phase. The method used the energy level of nodes in the network to determine the feedback of the environment to the automaton in partially favorable or partially unfavorable cases.

Disadvantage- Their simulation has shown that

1. In detecting Gray-hole, Back-hole, DoS and the Flooding attacks, the detection rate has decreased with increasing number of nodes in the network
2. In networks with high densities, the false positive rate is high.
3. Need to adjust zone number with variation in node numbers.

10. Pre-defined watchdog:

I. Krontiris et al. [17] proposed distributed IDS for WSNs based on collaborative neighborhood watching. In a simulation environment, the authors evaluated the effectiveness of their IDS scheme against blackhole and selective forwarding attacks. Their approach is based on watchdogs, which have pre-defined rules for raising intrusion alerts. The method has three common modules: 1) local monitoring and detection engine, for collecting and analyzing 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.

Advantage- The method produces very low false-negative and false-positive rates, which is a good thing.

Disadvantage- Detects only blackhole and selective forwarding attacks. Besides, proposed solution works only when there is one attacker.

11. Watchdog approach:

In [18], Roman et al. proposed a novel technique for optimal monitoring of neighbors called spontaneous watchdog, which extends the watchdog monitoring mechanism proposed in [19].They provided guidelines about application of IDSs (that are designed for MANETs) to static WSNs. Then, they propose an IDS for WSNs called 'spontaneous watchdogs' in which the neighbors are optimally monitored and where some nodes choose to independently monitor the communications in their neighborhood.

Advantage- takes advantage of the high density of sensors being deployed in the field.

Disadvantage- 1. Relies on the broadcast nature of sensor communications.

2. There is scope for further investigation which has not been covered in this work & left for future work.

12. Hybrid IDSs-

[20] Propose a hybrid, lightweight, distributed Intrusion Detection System (IDS) for wireless sensor networks. This IDS uses both misuse-based and anomaly-based detection techniques. It is composed of a Central Agent, which performs highly accurate intrusion detection by using data mining techniques, and a number of Local Agents running lighter

anomaly-based detection techniques on the motes. Decision trees have been adopted as classification algorithm in the detection process of the Central Agent and their behavior has been analyzed in selected attacks scenarios.

Advantage- The experimental results obtained show that high detection accuracy is obtained while keeping an acceptable, but not negligible false positives rate.

Disadvantage- Need to focus on the configuration of alert thresholds.

Comparison and Analysis

Comparative analysis of advantages and disadvantages of different methods:

1. Cluster-based: Low consumption, high safety

Disadvantage: Whenever number of nodes is increased energy consumption also increase.

2. Game theory based: Can help managers to weigh the detection efficiency and network resources.

Disadvantage: it is non-adaptive and requires human intervention for a stable operation.

3. Anomaly based: it is well suited to detect unknown or previously not encountered attacks.

Disadvantage: the normal profiles must be updated periodically, since the network behavior may change rapidly increasing the load on the resource constrained sensor nodes.

4. Misuse based: Simple, clear levels, easy to operate

Disadvantage: they need continuous rule updates in order to cope with the new released attacks.

5. Specification based: .they have low false alarm rate

Disadvantage: the cost to achieve the low false alarm rate is that the development of detailed specifications and constraints would be very time consuming.

Conclusion

In this survey paper, security attacks are described then brief information about IDS is presented. Various IDSs proposed for WSNs are discussed thereby providing their advantage and disadvantage. At last comparisons between different IDS is provided. This survey paper might help other researchers in constructing IDS for WSN.

References

[1] S. Shin, T. Kwon, G.Y. Jo, Y. Park, H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks", IEEE Trans. Ind. Informat., volume 6, number 4, pages 744-757, 2010.

[2] C.C. Su, K.M. Chang, Y.H. Kuo and M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in Proc. IEEE Wireless Communications and Networking Conference, 2005.

[3] S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, "DistributedAnomaly Detection in Wireless Sensor Networks", 10th IEEE Singapore International Conference on Communication systems, 2006.

[4] R.C. Chen, C.F. Hsieh, and Y.F. Haung," An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Networks", Journal of Networks, vol. 5, no. 3, 2010, pp. 335-342.

[5] S.S. Doumit and D.P. Agrawal, "Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks", in Proc. IEEE Military Communications Conference (MILCOM'03), 2003.

[6] A. Agah, S.K. Das, K. Basu and M. Asadi, "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach," Proc. 3rd IEEE International Symposium on Network Computing and Applications (NCA'04), pp. 343-346, 2004.

[7] A. Agah, K. Basu, S.K. Das, "Preventing DoS attacks in wireless sensor networks: A game theory approach", International Journal of Network Security, volume 5, number 2, pages 145-153, 2005.

[8] S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, "Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks", IEEE ICC '07, Glasgow, U.K., June 2007.

[9] F. Bao, R. Chen, M.J. Chang and J.H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trustbased routing and intrusion detection", IEEE Trans. Network Service Management, vol. 9, num. 2, pp. 169–183, 2012.

[10] C. Wang, T. Feng, J. Kim, G. Wang and W. Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", IEEE Trans. Parallel Distrib. Syst., vol. 23, num. 5, pp. 835–843, 2012.

[11] Athmani, S. ; Boubiche, D.E. ; Bilami, A.,"Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs",IEEE 2013,Computer and Information Technology (WCCIT), 2013 World Congress on

[12] V. Bhuse, A. Gupta, and A. Al-Fuqaha, "Detection of Masquerade Attacks on Wireless Sensor Networks", in ICC'07, 2007, pp. 1142- 1147.

[13] Y. Wang, X. Wang, B. Xie, D. Wang, and P. Agrawal," Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks", IEEE Trans. Mobile Computing, vol. 8, no. 6, pp. 698-711, 2008.

[14] A.P.R. da Silva, M.H.T. Martins, B.P.S. Rocha, A.A.F. Loureiro, L.B. Ruiz, and H.C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks", in 1st ACM International Workshop on Quality of service and security in wireless and mobile networks, Montreal, Quebec, Canada, October 2005.

[15] Z. Yu and J. Tsai, "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks", in SUTC'08, 2008, pp. 272- 279

[16] FathiNavid, A.H., Aghababa, A.B., "A Protocol for Intrusion Detection based on Learning Automata in Forwarding Packets for Distributed Wireless Sensor Networks", 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC),IEEE Conference Publications

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

[18] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in Proc. IEEE Consumer Communications and Networking Conference, 2006.

[19] 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.

[20] Coppolino, L. ; D'Antonio, S. ; Garofalo, A. ; Romano, L., "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks", 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), IEEE Conference Publications .