Intrusion Detection System in Wireless Sensor Networks: A Comprehensive Review

Sonu Duhan
Dept. of Computer Science and Engineering
PEC University of Technology
Chandigarh, India
duhansonu66@gmail.com

Padmavati khandnor
Dept. of Computer Science and Engineering
PEC University of Technology
Chandigarh, India
padmavati@pec.ac.in

***Abstract*—In today's era security is one of the main concern in every field also in wireless sensor networks. Resource limitation is main concern of sensor nodes in wireless sensor networks. There are many security threats which are affecting the, functionality, security and network life time of and wireless sensor networks. In this paper security threats, security goals, various attacks, classification of these attacks are presented along with the comparison of different intrusion detection systems in wireless sensor networks. Detailed information about intrusion detection systems is provided then, intrusion detection methodologies are compared based on different schemes. Intrusion detection schemes are categorized based on techniques used in the scheme: Specification based scheme, computational intelligence and data mining based scheme, game theory approach based intrusion detection scheme, probability distribution based detection scheme. At the end of paper advantages and disadvantages of each scheme is also presented.**

Keywords—Wireless Sensor Networks; Intrusion Detection Systems; Open System Interconnect; Base station; Computational Intelligence and Data Mining.

I. INTRODUCTION

Wireless sensor network (WSN) is becoming the important area of research because of its vital use in various fields. Wireless sensor networks consist of sensors which may be thousands in numbers and work cooperatively based on the local decision process. WSN can work both in structured and non-structured manner. Sensor nodes are small in size and low power nodes. The main properties of WSN include flexibility, self-organization capacity, fault tolerance, high sensing power, rapid deployment and lower in cost. Due to its promising properties WSNs has wide application in various areas like military, power plants, industries, home (smart home), and in the field of health are important application of WSN [1].

Among their applications critical application includes military and health. So security of sensor networks is the main concern. It can prove to be very dangerous in the field of military and health if security is not considered as the main issue. As WSNs are scalable and infrastructure-less these characteristics make WSNs more promising in the area of its application. But security threats are to be considered as malicious node can enter into the system. WSN faces various security attacks which can affect the overall performance and security of the system. So, it is necessary to detect and prevent the attacks on WSN. For more security critical system like military both prevention and detection based techniques are used altogether. Considering the security as main issue various IDS have been proposed in recent years for WSN [2-3].

The paper is organised as follows: Section II gives an overview of security in WSN with security goals and security attacks in WSNs. Section III gives brief introduction of IDS and its techniques. Classification of intrusion detection scheme and its comparison is given in Section IV. Section V finally concludes the paper on the bases of analysis.

II. OVERVIEW OF SECURITY IN WSN

A. *Security Goals*

Information and resources should be protected over the network. As security is one of the main issues in WSN. Also misbehavior of the nodes should be handled. Below are the main security goals or services [3]:

- Confidentiality: Confidentiality means that the information is available or accessible to the authorized users only. It is the most important security goal. To achieve confidentiality Encryption with security key is used.
- Availability: Data should be available to the authorized user whenever needed despite of any internal or external attacks i.e. DoS attack.
- Integrity: Data should not be altered or manipulated by adversary as it travels from sender to the recipient.
- Authentication: Data originates from the identified sender with which the node is communicating in the network.
- Non-repudiation: Non-repudiation means a previously send message cannot be denied by a node in a WSN.
- Authorization: Network services or resources can only be accessed by authorized nodes.
- Freshness: Data should be recent it is very important goal for WSNs it ensures that only new messages are received but not the replayed messages of the adversary.

B. *Security Attacks*

Figure 1 provides classification of attacks in WSN: Attacker type, Result of impact, Attackers ability.

978-1-4673-9939-5/16/$31.00 ©2016 IEEE

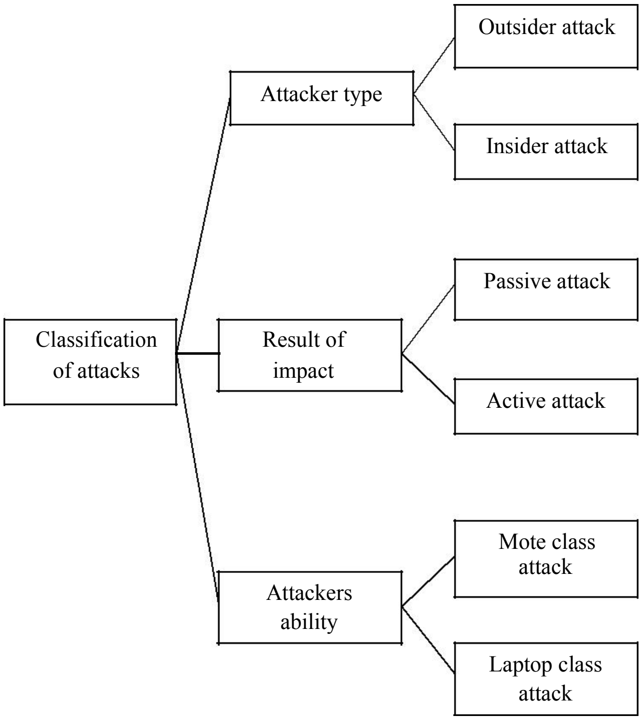

Fig.1. Classification of attacks in WSN.

Possible security attacks in WSN [3-4]:

1) Passive Information Gathering

Information is gathered by adversary if the information is not in encrypted format with the help of powerful resource.

2) Subversion of node

Captured node reveals all information including cryptographic keys of the whole sensor network.

3) False Node

False malicious data is injected with the help of malicious node by an adversary.

4) Node Malfunction

Inaccurate data is generated by malfunction node which would affect the integrity of sensor network it would be more dangerous if node is cluster head.

5) Node Outage

If a cluster leader node is not working or dead then alternate route should be provided for the proper and secure function of the network.

6) Message Corruption

Message integrity is compromised when a message is modified by an attacker.

7) Traffic Analysis

Traffic is analyzed on the bases of communication pattern. Encrypted messages are analyzed.

8) Routing loops

In this type of attack the data exchanged between nodes is the main target when the attacker replays or alters the routing data and false error messages are generated. Latency is increased because data move between the loops.

9) Selective forwarding

In this attack, attacker node simply drops some of the messages i.e. it does not forward all the messages received by it. Its Effectiveness depends upon two factors: Malicious node location more traffic it will attract if it is closer to the base station and second is percentage of messages dropped by it.

10) Sinkhole attacks

In this attack adversary node attracts most of the network traffic. Sinkhole is created by placing the compromised node closer to the base station, where it attracts most of the traffic.

11) Sybil attacks

In this attack, malicious node creates multiple identities by stealing the identities of legitimate nodes or by fabricating it. Topology maintenance and routing algorithms are affected by Sybil attacks.

12) Wormholes

In this type of attack a tunnel is created with low latency by the adversary near the base station creating a sinkhole.

13) Hello flood attacks

In this type of attack a HELLO message is broadcasted pretending the message is coming from base station with stronger transmission power. Nodes receiving HELLO message send their messages through adversary node. A lot of energy is wasted by the nodes.

15) DoS attacks

In Denial of service is physical layer attack includes battery exhaustion, radio jamming, interfering network protocol occur at physical level.

C. Layering Based Security Approach [3]

1) *Application layer:* At application layer manages data collection. So the reliability of the data should be ensured at application layer.
2) *Transport Layer:* Establishment of communication for external networks is the main objective of transport layer.
3) *Network Layer:* Network layer performs routing of messages from cluster head to base station, cluster head to cluster head, node to node, node to cluster head, cluster head to the base station and vice versa.
4) *Data Link layer:* Data link layer performs multiplexing of data stream, the error detection and correction, medium access control, and encryption of data.
5) *Physical Layer:* Physical layer focuses on Signal detection, frequency selection, carrier frequency generation, signal strength, encrypting data, media of transmission between sending and receiving nodes.

Table I below summarizes the attacks and countermeasures in a layering model in sensor networks. of the current designations [5].

TABLE I
LAYERING APPROACH TO SECURITY ATTACKS AND COUNTERMEASURES

Layers	Attacks	Countermeasures

Application Layer	Subversion Malicious Nodes	Malicious Node Detection Isolation
Transport Layer	Flooding De-synchronization	Client puzzles Authentication
Network Layer	Spoofed routing information selective forwarding Wormholes Sinkholes Sybil Routing loops Hello Flood Ack. flooding	Key Management authentication Secure Routing Egress filtering Monitoring Redundancy checking Packet leashes Probing bi-directional link authentication verification
Data Link Layer	Collision Exhaustion Unfairness Link layer Jamming	Link layer encryption Rate limitation Error-correction code Small frames
Physical Layer	DoS Node capture attacks Jamming	Adaptive antennas priority messages region mapping mode change

III. INTRUSION DETECTION SYSTEM

An Intrusion Detection System (IDS) is used for the detection of intrusions in the network using various methods and tools. It cannot be considered as standalone protection system in fact it is one of the part of protection system. [4] [6].

Requirements of IDSs:

- It should not introduce new weakness in the system
- Requirement of resources should be less and overhead of the system should not be increased resulting degrade overall system performance
- Run continuously and transparent
- Standards should be cooperative
- Standards should be open
- False negative and false positive rate should be low in detection phase
- It should be reliable.

Broadly speaking, IDS has three main components these are defined below and in Figure 2:

(i) Monitoring component: Traffic is monitored using patterns of traffic.

(ii) Analysis and detection: Based on algorithm of modelling behaviour and different activities are analysed and detects the misbehaviour.

(iii) Alarm component: Whenever intrusion is detected alarm is raised by alarm component

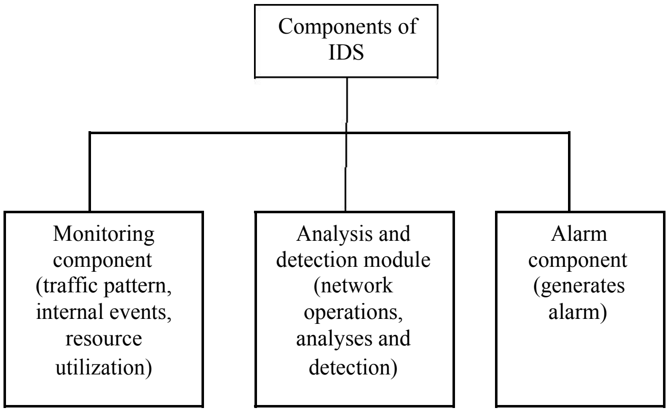
Components of IDS
Monitoring component (traffic pattern, internal events, resource utilization)
Analysis and detection module (network operations, analyses and detection)
Alarm component (generates alarm)

Fig .2. Components of IDS

WSNs works on three broad categories of IDSs detection methodologies that is, signature-based and anomaly-based IDSs, Hybrid.

Signature-Based /Rule based IDS: Consist of predefined set of rules considering different security attacks. In this system sensor network behaviour is analyzed based on set of predefined rules [7].

Anomaly-Based IDS: In this heuristic approach is used to analyze network activities and classified as either malicious or normal. Intrusion is identified using threshold value i.e. activity above threshold value [8-9].

Hybrid IDS: Hybrid IDS is a combination of both anomaly and signature-based methodologies. It contains two modules for detection; that is, one module uses signatures to detect known attacks other responsible for detecting new attacks by learning malicious and normal patterns and monitoring network behaviour deviating from normal [10].

Table II provide comparison of these three techniques based on different characteristics.

TABLE II.
COMPARISON OF DETECTION METHODOLOGIES IN WSN BASED ON DIFFERENT CHARECTERISTICS

Characteristics	**Anomaly based**	**Signature based**	**Hybrid based**
Memory/ Utilization	Lower	Lower	Medium
Energy consumption	Lower	Lower	Medium

978-1-4673-9939-5/16/$31.00 ©2016 IEEE

Detection rate	Medium	Medium	Higher
False alarm	Medium	Medium	Lower
Strength	Capable of detecting new attacks	Detects all those attacks having signatures	Can detect both existing and new attacks
Weakness	Misses well known Attack	Cannot detect new Attacks	Requires more computation and resources

IV. Intrusion detection schemes

A. *Specification based intrusion detection scheme*

This scheme is also known as rule based intrusion detection scheme. In these schemes, we have set of rules defining the attacks [7] [11-15].

Advantages:

Detection is fast
Simple rules for detecting attacks
Less complexity
Higher accuracy for
detection. Disadvantages:
Generality
Collaborative voting
Assumptions made.

B. *Computational intelligence and Data mining based scheme*

Intelligent IDS uses Data mining and Computational Intelligence (DM/CI) techniques in computer networks because of unknown attacks detection ability of this scheme. WSN faces challenges because of limited resources [16-17] [18-21].

Advantages:

Communication overhead is less
Generality
Scalability
guaranteed. Disadvantages:
Detection is Slow
Computational complexity is high
False alarms are high.

C. *Game theory based intrusion detection scheme*

This theory represented scientifically by a game between players. In these different strategies is used by the ID agent to defend against the strategies that attackers always uses [22-23].

Advantages:

Do Not need extra data
Lightweight
Depend on
strategies. Disadvantages:
Need to be experimented so time consuming in beginning
Scope is limited.

D. *Statistical based intrusion detection scheme*

Statistical based techniques are commonly used detection schemes designed for WSN. Probability distribution is used in these schemes for normal and abnormal data as evidence behaviour [10] [24].

Advantages:

Mathematically proven
Used effectively with accurate probability distribution.

Disadvantages:

Difficulties in getting probability
Not suitable for multivariate data.
Difficulty in keeping the model up to date.

V. PROPOSED SYSTEMS FOR WSN

Group-based intrusion detection system in wireless sensor networks: In group based scheme sensor network is partitioned in groups. Sensor nodes in each group are physically close to each other. Attacker is detected using multiple attribute of the sensor nodes [10].

Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks: Network traffic is analyzed and a mechanism is defined for detecting attacks [13].

A Global Hybrid Intrusion Detection System for Wireless Sensor Networks: Support vector machine (SVM) algorithm for anomaly detection and set of signature for malicious behaviour detection is used in this method [14].

An Energy-Efficient Routing Method with Intrusion Detection and Prevention for Wireless Sensor Networks: Both intrusion detection and prevention scheme are implemented with less communication overhead and low energy consumption [15].

An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks: It is a cluster based scheme. Intrusion detection systems are implemented at different levels in cluster. Misuse Intrusion detection technique has applied at sensor nodes, Hybrid IDS at cluster-head and integrated HIDS at sink node [16].

*Using artificial intelligence in routing schemes for wireless networks: A*rtificial neural network is used at every sensor node which provides self learning capability to system [17].

Intrusion Detection System In wireless Sensor network Based On Mobile Agent: Mobile agent is used for detecting the intrusion. Three main mobile agents are used: Collector agent, Misuse detection agent and anomaly detection agent which uses SVM [18].

978-1-4673-9939-5/16/$31.00 ©2016 IEEE

D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks: In this scheme, Hybrid clustering method is introduced. Imperialist competitive algorithm is enhanced with fuzzy logic controller and density based algorithm is used to form arbitrary shape clusters and for handling noise. [19].

Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks: This scheme is bio-inspired method i.e fuzzy system and cooperative decision making approach has applied [20].

Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling: In this scheme, fuzzy c-mean clustering is used and anomaly detection is performed based on fuzzy evaluation and inter cluster distance [21].

Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks: In this game theory method is used along with fuzzy Q-learning. Attacker, base station and sink nodes are three players in the game. Base station and sink nodes are decision maker players for detection DOS attack [23].

An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks: Algorithm for detecting the sinkhole attack is proposed. Firstly list of suspected nodes is generated checking data consistency, and than using data flow information intruder is identified [24].

Table III presents comparison of IDS proposed for WSNs by other researchers based on architecture, detection techniques used and highlighted the features.

TABLE III.
COMPARISON OF THE IDSS PROPOSED FOR WSNS

Proposed system	Architecture	Detection technique	Highlighting features
[10]	Hierarchical	Statistical based	Decrease the false alarm rate Increase detection Accuracy lower computation & transmission power consumption.
[13]	Hierarchical	Rule based	Reduced Overhead Effective The false negative rates are lower
[14]	Hierarchical	Rule based	lower the false positive rate High Detection Rate
[15]	Hierarchical	Rule based	Reduced communication overhead Reduced energy consumption
[16]	Hierarchical	Data mining and computational intelligence	Raised detection Rate lower the false positive rate Efficient with a higher accuracy rate
[17]	Flat based	Data mining and computational intelligence	QoS-driven routing algorithm Enhanced scalability
[18]	Hierarchical	Data mining and computational intelligence	redundant and fault-tolerant Efficient Scalability
[19]	Hierarchical	Data mining and computational intelligence	Avoid possible errors Enhanced accuracy clustering quality
[20]	Hierarchical	Data mining and computational intelligence	Detection accuracy Defence rate performance

978-1-4673-9939-5/16/$31.00 ©2016 IEEE

[21]	Hierarchical	Data mining and computational intelligence	High detection accuracy Less communication overheads
[23]	Hierarchical	Game theory based	do not need extra data benefits from routing information lightweight since no training
[24]	Hierarchical	Statistical based	Robust to deal with multiple malicious nodes Effective Accurate Communication and computation overheads are reasonably low

VI. Conclusion

Security is a major concern for WSN researchers and designers because of its critical application like in military and health. In this paper we discussed the security issues, various security attacks and their countermeasures. Various detection schemes and methodologies are also discussed. At the end of paper comparison of these schemes are also presented based on architecture followed, detection technique used and also highlighted their features.

References

[1] Mitchell, Robert, and Ray Chen. "A survey of intrusion detection in wireless network applications." *Computer Communications* 42 (2014): 1-23.

[2] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." *Computer networks* 52.12 (2008): 2292-2330.

[3] Chen, Xiangqian, Kia Makki, Kang Yen, and Niki Pissinou. "Sensor network security: a survey." *Communications Surveys & Tutorials, IEEE* 11.2 (2009): 52-73.

[4] Can, Okan, and Ozgur Koray Sahingoz. "A survey of intrusion detection systems in wireless sensor networks." *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on*. IEEE, 2015.

[5] Maleh, Yassine, and Abdellah Ezzati. "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks." *arXiv preprint arXiv:1401.1982* (2014).

[6] Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review."*Journal of Network and Computer Applications* 36.1 (2013): 16-24.

[7] Huo, Guangcheng, and Xiaodong Wang. "DIDS: A dynamic model of intrusion detection system in wireless sensor networks." *Information and Automation, 2008. ICIA 2008. International Conference on*. IEEE, 2008.

[8] Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges." *computers & security* 28.1 (2009): 18-28.

[9] Rajasegarar, Sutharshan, Christopher Leckie, and Marimuthu Palaniswami. "Anomaly detection in wireless sensor networks." *Wireless Communications, IEEE* 15.4 (2008): 34-40

[10] Li, Guorui, Jingsha He, and Yingfang Fu. "Group-based intrusion detection system in wireless sensor networks." *Computer Communications* 31.18 (2008): 4324-4332.

[11] Stetsko, Andriy, Lukáš Folkman, and Vashek Matyáš. "Neighbor-based intrusion detection for wireless sensor networks." *Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on*. IEEE, 2010.

[12] de Sousa Lemos, Marcus Vinícius, Líliam Barroso Leal, and Raimir Holanda Filho. "A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks." *Novel Algorithms and Techniques in Telecommunications and Networking*. Springer Netherlands, 2010. 239-244.

[13] Baig, Zubair A. "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks." *Computer Communications* 34.3 (2011): 468-484.

[14] Maleh, Yassine, et al. "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks." *Procedia Computer Science* 52 (2015): 1047-1052.

[15] Moon, Soo Young, Ji Won Kim, and Tae Ho Cho. "An energy-efficient routing method with intrusion detection and prevention for wireless sensor networks."*Advanced Communication Technology (ICACT), 2014 16th International Conference on*. IEEE, 2014.

[16] Wang, Shun-Sheng, et al. "An integrated intrusion detection system for cluster-based wireless sensor networks." *Expert Systems with Applications* 38.12 (2011): 15234-15243.

[17] Barbancho, Julio, et al. "Using artificial intelligence in routing schemes for wireless networks." *Computer Communications* 30.14 (2007): 2802-2811.

[18] El Mourabit, Yousef, et al. "Intrusion detection system in Wireless Sensor Network based on mobile agent." *Complex Systems (WCCS), 2014 Second World Conference on*. IEEE, 2014.

[19] Shamshirband, Shahaboddin, et al. "D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks." *Measurement* 55 (2014): 212-226.

[20] Shamshirband, Shahaboddin, et al. "Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks." *Journal of Network and Computer Applications* 42 (2014): 102-117.

[21] Kumarage, Heshan, et al. "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling." *Journal of Parallel and Distributed Computing* 73.6 (2013): 790-806.

[22] Reddy, Yenumula B., and S. Srivathsan. "Game theory model for selective forward attacks in wireless sensor networks." *Control and Automation, 2009. MED'09. 17th Mediterranean Conference on*. IEEE, 2009.

[23] Shamshirband, Shahaboddin, et al. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." *Engineering Applications of Artificial Intelligence* 32 (2014): 228-241.

[24] Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu. "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks."*Computer Communications* 30.11 (2007): 2353-2364.