International Journal of Engineering & Technology, 7 (2.21) (2018) 405-409

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Comparison and detail study of attacks and detection methods for wireless sensor network

T. Karthik Krishnan[1], S. Sridevi[2*], G. Bindu[3], R. Anandan[4]

[1]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
[2]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
[3]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
[4]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
**Corresponding author E-mail: sridevi.se@velsuniv.ac.in*

Abstract

Wireless sensor network is emanating technology in the field of telecommunications. WSNs can be applied in many fields like machine surveillance, precision agriculture, home automation and intelligent building environments. However the major aspect of WSN is the security as the sensor nodes are limited because of these facing several security threats such as black hole attack, worm hole attack, flooding etc. which is finally affecting the functioning of the whole network. These attacks are maximizing the consumption of power in the node and also it decreases life of the battery. In this paper, we discuss several types of security attacks in wireless sensor networks and also it introduces various intrusion detection systems to detect these attacks and prevent the compromised nodes in the WSN. And also we discuss about the different intrusion detection methods with the help of machine learning algorithms. In future these techniques can be helpful to create a safe and sophisticated network.

Keywords: *WSN, security, malicious node, machine learning, black hole attack.*

1. Introduction

A small, light, weight and portable device equipped with transducer, micro computer, transceiver and power source called sensors are grouped together to form wireless sensor devices. These Sensors are positioned in the different places in the field. And also it collects the information from the field, summative them and forward them to a sink node, which is answerable for data fusion. Transducer generates the electrical signal. The data is processed in Microcomputer and sensor output is stored in microcomputer. Central computer sends the commands to the Transceiver and the data is sent to the computer. The sensor node power is based on a battery. Depending upon the requirements wireless sensor network classified in to [2]

Category 1 the wireless sensor networks in this uses multi hop packet routing using radioactive waves. The network setup is Mesh Topology. Category 2 wireless sensor networks in this uses single hop routing which is also known as Peer to Peer Communication. The nature of WSN makes us to use in Critical situations like Disasters, operations, Medical field.

2. Security goals for WSN

Wireless sensor networks have the two main goals for security such as primary and subsidiary [1] [3] [4] Primary security consists.

A. Data confidentiality

The major issue in network security is data confidentiality. It is the way of protecting data from unauthorized user. It hides the data from a passive attacker. In WSN, each and every sensor nodes exchange information with each other and also sends the sensitive data such as public key, private key and key distribution in secure channel.

B. Data integrity and authentication

Data integrity refers to the overall accuracy, consistency and completeness of data. It also confirms the message has not been altered during the transfer of data in the network.

Data authentication allows a receiver checks that the data comes from the claimed sender.

C. Data availability

Data Availability is the capability of node to use the maximum available resources all the time.

D. Data freshness

It says that data available is recently updated and therefore there is no repetition of old data existence. Subsidiary Security consists.

E. Self-organization

In WSN the nodes keep moving leading often changes in network topologies. Therefore management of WSN is a challenging issue. Because of this, the sensor nodes should be always self organizing and self healing natured to handle different situations.

F. Time synchronization

Time synchronization among the executions is the one of the major task in WSN applications.

G. Secure localization

In WSN, the sensor nodes are automatically located and accurately deployed in wireless environment when there is displacement in sensors.

3. Security attacks in WSN

An attacker in WSNs can be classified based on the following characteristics: targets, performance, and layers based technology.

A. Target-oriented attacks

We classified passive and active attacks [3] [4] [5].

Passive attacks

These attacks are generally opposition to confidentiality of data. An attacker looks for sensitive information and also monitors the traffic.
It analyzes the data packets, travelling and decrypts it. It also observes the authentication information. This types of attacks allows attacker to use the information of data file, without the knowledge of the user.

Active attacks

These attacks takes active measures to control over the network. It changes the content of the data in the network. Some of the active attacks are replay, sink hole, spoofing, flooding, black hole, DoS attack, worm hole, Hello flood, lack of cooperation, man in middle attack, selective forwarding and false node.

B. Performance oriented attacks

There are two types of performance oriented attacks outside attack and inside attack. [6] [7] [8].

Outside attacks

It attacks using eaves dropping when there is a transmission of data and this data is transformed in to the network.
It consumes the resources of the network causing Denial of Service attack.

Inside attacks

In military surveillance system inside attackers silently damages the network without knowledge of others. The attacks like change of data, eavesdropping, misrouting, dropping of packets are of inside attacks.

C. Layer-based technology attacks

WSNs follows in layered based architecture. This layered form creates many types of attacks which is vulnerable to network.

Physical layer attacks

Physical layer attacks on WSNs to jam the entire radio channel[9][10][11].It is more difficult to prevent .In which attacker send very high energy signals to block the radio channel and prevent sensor nodes from communicating.

Data link layer attacks

In data link layer, the wireless channel can be accessed and shared by multiple adjacent nodes. so that it affords abstraction of link to the above layer. The predefined protocol behavior can be purposely violated by the attacker such as drain out of source energy of packet, collision of packets occurs due to repeated retransmission of data packet[8] [11] [12].

Network layer attacks

The network layer of WSNs is exposed to the many types of attacks, such as Dos attack, spoofing, sinkhole attack. DoS attacks completely disturb the routing information of the whole network. A sinkhole attack, compromise node produces a fake routes to attract the network and tries to create network traffic. It launches selective forwarding attack, acknowledge spoofing attack. In spoofing attack malicious node exactly behaves like legitimate node [13] [12] [16].

Transport layer attacks

In this attacker try to over utilize the resources available .It loads to severe resource limitation for trusted nodes[9][16]

Application layer attacks

In this types of attack, the attacker tries to transfer large volumes of data to the base station. In this way it consumes more network bandwidth and finally energy of the node will be reduced. So that malicious node can be easily enter [14] [17].

4. Intrusion detection systems in WSN

In 1980, Intrusion Detection (ID) was established to detect the malicious nodes, two important types of intrusion detection systems (IDS) are Host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) [17]. Intrusion detection monitors the entire network and generates alarm when there is an intrusion in the network. In this section we describe the architecture of IDS in WSNs. Intrusion Detection System only detect the intrusion in WSN, it does not make any preventive action.
There are two distinct technologies of IDS:

Network Intrusion Detection System (NIDS)

These systems are designed to capture and analyze the entire packets circulating around the network. Therefore, the nodes can mutually check the network traffic.

Host Intrusion Detection Systems (HIDS)

In this type of detection system follows one node and can observe the entire network. This system uses two types of informations in that individual node. First it observes all the ongoing tasks in the system and data traffic in that system.
In these systems it can only monitor the individual node in the network not an entire network. The IDS utilize two varieties of files which records activities in the system and data flow in and out of the particular node.

5. Design of IDS in wireless sensor network

Wireless sensor networks are vulnerable to attack. The sensor nodes are randomly distributed and data are captured in all directions and attacks come at any time and target any node. So to detect this attack is major task in the network. There are several possible IDS architectures such as standalone IDS, distributed and cooperative IDS and hierarchical IDS [27].

5.1. Adaptive IDS

In this system, each individual node acts as standalone IDS and each node identifies intruder. There will not be any interaction between two nodes and hence not allowed to share information. In this system each node relays the duties of IDS.

5.2. Distributed and cooperative IDS

In this design of IDS each node detects and takes decision by itself. The entire node communicates each other to create a unique detection system. This type of IDS design is more convenient to work with flat network configuration than multilayer networks.

5.3. Hierarchical IDS

In this network nodes are divided in to clusters. A leader (header) places an important role. The header is responsible for transfering data packets in the cluster. All the cluster head interact with base station for global IDS.

6. Related works

1. Weighted trust evaluation approach

The basing of forwarding behavior of a node trust on that node has been decided. If node sends wrong information that means its trust value is decreased. If the attacker compromise the base station it is very difficult to track the node. So that it is easy to identify the node unless it compromises the base station. This is possible by assuming base station is trusted. In fact, if the opponent gains control over base station, the intruder can attack easily.

The main critical problem is that assuming the sensor nodes functioning appropriately. If the number of compromising nodes is more than normal nodes, other malicious nodes are normal nodes, intermediate nodes are considered as malicious nodes. In this paper we try to identify the correct scheme for verifying efficiency of detection scheme.

2. Ant colony based approach

In this approach it is classified into two types. The first is to configuring the network and second is to identify the attacks and finding out the path of the data to reach the destination. In trust it consists four stages, cluster formation, Wireless sensor network is divided into different regions.

In a region G and node N is chosen and L indicates the parameters level of neighbor in the cluster. To avoid the flooding effect, only up to L level it's allowed to send hello messages. Only M neighbor list starts from N to L level.

After this cluster level identification starts first randomly, H1,H2,H3 are selected.

The resource of H1,H2,H3 are they compared with threshold value of resource. Hence a node with highest resource is then selected as head. The process repeated to identify the heads for the remaining clusters. Finally after this ant phenomenon is deployed in all clusters.

3. Data mining based approach

In this approach intrusion detection system based on online mining is anticipated in [20]. It takes wireless network data and applies the concept of data mining clustering technique, for the detection of peculiar manners in wireless data packets. Before reaching access points they capture network packets using hardware sensors, further analyzed to detect attacks. This explains how to detect intrusion without any training and detection rate.

4. Agent based approach

In the agent based approach [4] the author proposed a model to identify the abnormal behavior of a node by using Bayesian technique. It identifies the abnormal event pattern of sensors nodes in a large wireless distributed sensor networks.

5. Trust based approach

In this paper author used intrusion detection based on trust based value [22]. In this method each and every sensor node calculates serial trust and QOS trust values. These trust values are evaluated based on peer to peer communication are collected from sensor nodes. The trust of a node are calculated by header of each cluster. Finally, clusters are evaluated by base station. In this method stochastic petri nets model is developed for finding the trust values.

6. Weak Hidden Markov Model Based Approach [WHMM]

In this proposed approach, uses learning and training phase for identifying intrusion. It also uses scheme based on scoring and deviation alarm mechanism to find accuracy of WHMM.

7. Neighbor based approach

The intrusion dection method based on the neighbors proposed in[6], in this he explores that the behavior of neighbor nodes as the same because they are spatially closed to each other. The author implemented IDS, a small OS users packet delivery ratio and packet dropping ratio. To detect flooding attacks, they used TOSSIM simulator for implementation.

8. Game theory based approach

In this approach, a gaming theory based model is proposed for identifying intruder in wireless sensor network. Here the nodes are communicated using signaling game theory in wireless sensor networks. A Bayesian game is considered when there is an interaction between attacker and an independent node with the clear information.

9. Swarm intelligence based method

A network based on theoretical alerting game model used for finding intrusion in WSN is proposed in [8], in this method Dijikstra algorithm used to find the shortest path between the nodes.

10. Artificial neural network method

ANN consist of two stages training and generalization in the first stage values of the inputs are read until an error is occurred or after specific number of times hence, learning, discussion boundaries in the network neural networks have the capability of reading the human brain behavior using unprocessed and simple expectations of human neurons. In generalization stage unprocessed input values are used to find out the out the output

using the processed ANN. This methodology is famous for it's efficiency, parallelism and noise tolerance [15].

11. Fuzzy logic system

Challenges can intrude through DOS attacks which disturbs the service of wireless sensor network.DOS can be identified in any layer of wireless network [3][4]. Hence this is considered as an important issue in aspects of security for ad-hoc sensors network[5].Even after introducing strength cryptographic authentication methods DOS attacks may happens.[4] but these methods cannot be implemented in wireless sensor network due to lack of resource.DOS attacks however can be identified in wireless sensor networks using MAC protocol which is designed by using fuzzy logic system[6].and HIIDS(hybrid intrusion detection system)[7].This system can easily identified attacks.

12. SVM approach

This approach explains the use of complex algorithm like neural networks implementing in real time not only theoretically and mathematically.

13. GSA: An algorithm based on newton theory of gravitation

Gravitational search algorithm is based on law of neutron in physics. In this method masses are compared as agents. The gravitational force is responsible agent for which the mass value is high and hence considered as the best global solution.

14. IWD: Intelligent water drops algorithm

IWD is an optimized approach swarm based algorithm .This algorithm works according to the behavior of water drops and soil of river bed.
This implementation in many problems like travelling salesman problem, n-queen puzzle, multiple knapsack etc.

15.Adapative neuro fuzzy interference system

The adaptive Neuro Fuzzy Interference System[ANFIS] classifier is used to detect the dropping of packets in wireless sensor networks. This Adaptive neuro fuzzy classifier used to detect the normal and abnormal activities in wireless sensor network in a binary form. In adaptive neuro fuzzy classifier is a kind of neural network based on sujeno fuzzy interference system.
It is an efficient and optimal way of detecting abnormal nodes.

16. Radial bias fuzzy interference system

This paper contributes a individual node based on a Radial Basis Function neural network. This function helps to detect compromised node in an effective manner. It uses the trained data for detecting malicious nodes. These data further tested experimentally on different types of attacks. These results propose that IDS training on data is not only effective in detecting intrusions, but also predict the malicious node accurately.

VII Comparative study of Recent ID Schemes

Existing IDS	Strength	Flaws	Future Extent
Semantic IDS[28]	1) Agent is capable of storing all the domain information in memory	1) Mapping of security details, will sensors data is unclear. 2) Decision making is not clear	Algorithms can be developed with complex security ontology.
Simple Learning Automata based IDS [29]	1) Distributed nature effecting the remaining nodes, if a node has been effected	Increase the computational complexity because often changing in network topology.	S-LAID can be tested in all the domains of sensor network.
Location Aware Trust based IDS [30]	1) Ranking -based monitoring levels to detect and isolated malicious nodes. 2) Identifying location increases integrity	It consumes more energy.	Location verification can be explained in detail
Isolation Table based IDS	It works efficiently in terms of live nodes to prevent attacks and accuracy in transmission	The intruder passes easily when there is less number of nodes.	Abnormal node detection technique can be extended.
Ranger based IDS [35]	1) Using unique nodes it is not possible to attack by an intruder. 2) Energy-efficient manner.	It mainly based on Sybil attack.	To improve the performance further it is implemented through standard protocols (e.g. Zigbee)
Hierarchical Overlay Design based IDS [31]	1) For a large geographical area the values of Reliability, efficiency and effectiveness are high	1) Intruder can reach route area where the nodes are not subjected to capturing.	Nodes can identified by using election procedure algorithm.
Hybrid IDS [32]	1)Detection rate is high 2)Accuracy is high 3)Decision making is simple 2)By electing cluster head it reduces the energy consumption and increases the lifetime of a network.	In anomaly detection the performance can be detected only through manually	For better performance and flexibility it uses feature selection and rule based approach in data mining.
Weighted Trust Evaluation based IDS [33]	1)It detects malicious nodes accurately with a short time.	It increases misdetection rate	To improve the performance of the system the detailed analysis further to be done.
Dynamic Model of IDS[34]	1) It increases life time of the network stability and robustness 2)It increases the flexibility of the entire system	1)It takes more time for detecting intrusions. 2) It consumes more energy	To guarantee the perfectness of the model it can be tested with real life applications

7. Conclusions

This paper describes how protect a wireless sensor networks and it challenges to secure the data. This paper focuses on the different types of security attacks in WSN, description of intrusion detection systems (IDS), and examines different methods of intrusion detection in WSN. The detection of intrusion in a wireless sensor network automatically reduces the consumption of energy in nodes and unwanted transmissions, thereby increasing

the network lifetime. This paper discussed various techniques of protecting the nodes in WSNs against malicious nodes using different intrusion detection algorithms.

References

[1] Kahina CHELLI, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", *Proceedings of the World Congress on Engineering*, Vol.1, (2015).

[2] Sumathi K & Dr. Venkatesan M, "A Survey on Detecting Compromised Nodes in Wireless Sensor networks", *International Journal of Computer Science and Information Technologies*, Vol.5, No.6, (2014), pp.7720-7722.

[3] Qusay I.S, "Security Attacks and Countermeasures for Wireless Sensor Networks: Survey", *International Journal of Current Engineering and Technology*, (2013).

[4] Benenson Z, Cholewinski M & Freiling C, "Vulnerabilities and Attacks in Wireless Sensor Networks", *Laboratory for Dependable Distributed Systems, University of Mannheim*, (2010).

[5] David M & Herve G, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", *13th International Conference on Network-Based Information Systems (NBiS)*, (2010).

[6] Anitha SS, Shazia S & Dr. Vagdevi S, "Security Threats in Wireless Sensor Networks in Each Layer", *International Journal of Advanced Networking and Applications*, Vol.4 No.4, (2013), pp.1657-1661.

[7] Kaplantzis S, Mani N, Palaniswanmi M & Egan G, "Security models for wireless sensor networks", *Conversion report, Monash University*, Vol.20, (2006).

[8] Chris K & David W, "Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Networks Journal*, Vol.1, No.2-3, (2003), pp.293-315.

[9] Yan S, Zhu H & Ray Liu KJ, "Defense of Trust Management Vulnerabilities in Distributed Networks", *IEEE Communications Magazine*, Vol.46, No.2, (2008), pp.112-119.

[10] Yanli Y, Keqiu L, Wanlei Z & Ping L, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures", *Journal of Network and Computer Applications*, *Elsevier*, (2011).

[11] Xu W, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", *Mobi Hoc '05: Proc. 6th ACM Int. Symp. Mobile Ad Hoc Net. and Comp.*, (2005), pp.46–57.

[12] Xu W, Trappe W & Zhang Y, "Channel Surfing: Defending Wireless Sensor Networks from Interference", *Information Processing in Sensor Networks*, (2007).

[13] Shih E, Cho S, Ickes N, Min R, Sinha A, Wang A & Chandrakasan A, "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, (2013), pp.272-287.

[14] Woo A & Culler D, "A Transmission Control Scheme for Media Access in Sensor Networks", *Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom*, (2001).

[15] Sohrabi K, Gao J, Ailawadhi V & Pottie GJ, "Protocols for Self-Organization of a Wireless Sensor Network", *IEEE Personal Communications*, (2000), pp.16-27.

[16] David RR & Scott FM, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", *IEEE Pervasive Computing*, Vol.7, No.1, (2008), pp.74-81.

[17] Parno B, Perrig A & Gligor V, "Distributed Detection of Node Replication Attacks in Sensor Networks", *IEEE Symposium on Security and Privacy (S&P'05)*, (2005).

[18] Atakli IM, Hu H, Chen Y, Ku WS & Su Z, "Malicious node detection in wireless sensor networks using weighted trust evaluation", *Proceedings of the Spring simulation multi conference, Society for Computer Simulation*, (2008), pp.836-843.

[19] Arolkar HA, Sheth SP & Tamhane VP, "Ant colony based approach for intrusion detection on cluster heads in WSN", *Proceedings of the International Conference on Communication, Computing & Security* (2011), pp.523-526.

[20] Ezeife CI, Ejelike M & Aggarwal, AK, "WIDS: a sensor-based online mining wireless intrusion detection system", *Proceedings of the international symposium on Database engineering & applications*, (2008), pp.255-261.

[21] Sa M & Rath AK, "A simple agent based model for detecting abnormal event patterns in distributed wireless sensor networks", *Proceedings of the International Conference on Communication, Computing & Security*, (2011), pp.67-70.

[22] Bao F, Chen R, Chang M & Cho JH, "Trust-based intrusion detection in wireless sensor networks", *IEEE International Conference on Communications (ICC)*, (2011), pp.1-6.

[23] Song X, Chen G & Li X, "A weak hidden Markov model based intrusion detection method for wireless sensor networks", *International Conference on Intelligent Computing and Integrated Systems (ICISS)*, (2010), pp.887-889.

[24] Stetsko A, Folkman L & Matyas V, "Neighbor-based intrusion detection for wireless sensor networks", *IEEE 6th International Conference on Wireless and Mobile Communications (ICWMC)*, (2010), pp.420-425.

[25] Estiri M & Khademzadeh A, "A theoretical signaling game model for intrusion detection in wireless sensor networks", *14th International conference on Telecommunications Network Strategy and Planning Symposium (NETWORKS)*, (2010), pp.1-6.

[26] Yan KQ, Wang SC, Wang SS & Liu CW, "Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network", *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, Vol.1, (2010), pp.114-118.

[27] Strikos AA, "A full approach for intrusion detection in wireless sensor networks", *School of Information and Communication Technology*, (2007).

[28] Mao Y, "A semantic-based intrusion detection framework for wireless sensor network", *IEEE 6th International Conference on Networked Computing (INC)*, (2010), pp.1-5.

[29] Misra S, Krishna PV & Abraham KI, "Energy efficient learning solution for intrusion detection in wireless sensor networks", *IEEE Second International Conference on Communication Systems and Networks (COMSNETS)*, (2010), pp.1-6.

[30] Crosby GV, Hester L & Pissinou N, "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks", *IJ Network Security* Vol.12, No.2, (2011), pp.107-117.

[31] Chen RC, Hsieh CF & Huang YF, "An isolation intrusion detection system for hierarchical wireless sensor networks", *JNW*, Vol.5, No.3, (2010), pp.335-342.

[32] Yan KQ, Wang SC & Liu CW, "A hybrid intrusion detection system of cluster-based wireless sensor networks. In *Proceedings of the International Multi Conference of Engineers and Computer Scientists*, Vol.1, (2009), pp.18-20.

[33] Idris MA, Hongbing H, Yu C, Wei SK & Zhou S, "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", *The Symposium on Simulation of Systems Security (SSSS'08)*, (2008).

[34] Huo G & Wang X, "DIDS: A dynamic model of intrusion detection system in wireless sensor networks", *IEEE International Conference on Information and Automation*, (2008), pp.374-378.

[35] Chen RC, Haung YF & Hsieh CF, "Ranger intrusion detection system for wireless sensor networks with Sybil attack based on ontology", *New Aspects of Applied Informatics, Biomedical Electronics and Informatics and Communications*, (2010).