A Comprehensive Survey on Intrusion Detection Systems in Wireless Sensor Network

Amol R. Dhakne(✉) and P.N. Chatur

Department of CSE, Government College of Engineering, Amravati, India
dhakne.amol5@gmail.com, prashant_chatur@rediffmail.com

Abstract. Wireless sensor network is of prime importance because of its applicability in various domains ranging from healthcare applications to military applications. Security of such networks is important as these carry confidential information. Security of Wireless Sensor Network is divided in three phases, prevention, detection and mitigation. In Prevention phase, care is taken so that attack should not occur. But most of the times it is not possible to prevent attacks, so it is very important to detect them as early as possible so that these will not harm a lot to wireless sensor network and that phase is called as intrusion detection. Once Intrusion has been detected we have to take actions to cure from it and it is called as mitigation. So, Intrusion detection is most important phase as far as security of wireless sensor network is concerned. This paper discusses about various detection methodologies such as Anomaly based, Misuse based and Specification based IDS, various decision making schemes for intrusion. Major focus of this paper is to understand various Intrusion Detection Systems that are proposed for wireless sensor network. These are discussed with different issues with advantages and disadvantages. Finally paper gives future directions for selection of Intrusion Detection System.

Keywords: Intrusion · Intrusion detection · Wireless sensor network (WSN) · Mobile ad hoc network (MANET) · Security

1 Introduction

Wireless Sensor Network is widely used in various fields of Science and Technology as they are capable to gather information about human beings and environment. Now days WSN is used for various applications including highway traffic, health care and military surveillance, also in earthquake prediction, water quality analysis, building safety, pollution, ocean and wildlife, manufacturing machinery performance, and so on [1]. So, Security of WSN is of utmost importance as we need to keep patient health records confidential so that it can be secured from third parties in healthcare application. Also in military applications we need to tackle security gap in the network. More Information on Security can be found in [2–4].

Security attacks in WSNs are mainly partitioned in two types: Active attacks and Passive attacks. Passive attacks are not visible or hidden and they can tap communication channel to gather data; or they can harm the networking elements that are working. Node

A. Unal et al. (Eds.): SmartCom 2016, CCIS 628, pp. 541–549, 2016.
DOI: 10.1007/978-981-10-3433-6_65

malfunctioning, traffic analysis and eavesdropping are some examples of passive attack. Active attacks affect the operations in network. Networking services can degraded because of these attacks. Black hole, Sinkhole, wormhole attacks, jamming and Denial-of-Service (DoS) are some examples of active attack [3–5].

Securing WSN from these attacks works in 3 phases, Prevention step is aimed to prevent attack before it should happen and it is called as defense against attack. In Detection phase we need to know presence of attack and identify the nodes that are being harmful. If first phase fails then it is always important to find the attacks quickly so that it can harm less to network. Most of the time it is not possible to defend attack from happening so Detection phase is very important as far as security of WSNs is concerned. Mitigation (reacting to the attack) is last phase and is aimed to mitigate any attack after its proper detection and in this phase affected nodes are removed to secure the network.

Intrusions are any unauthorized (unwanted) behaviors in network. Intrusion detection is detection of any malicious activity in a network carried out by any network member. Intrusion detection systems provide following information to supportive system such as identification of intruder, time of intrusion, activity, type and layer where intrusion occurs. This information is useful in third line of defense as specific information is available to mitigate the attacks. Therefore, IDSs are of utmost importance for security of network.

WSNs are limited by various factors such as small memory size, limited battery etc. IDS that are applicable to traditional networks are not applicable to WSN [6]. So, developing effective IDS for WSNs is very important task which lead us to do some survey on existing IDSs in WSN.

2 Intrusion Detection System Methodologies

IDS are equivalent of burglar alarms that notify the presence of intrusion if any. IDSs are majorly categorized in three categories according to their functionality as follows:

2.1 Anomaly Based Detection

In this normal operations are recorded and deviation is from normal behavior is considered as anomaly. The drawback of this type is that normal operations need to be recorded and updated regularly. The benefit of this methodology is that it detects previously unencountered or unknown attacks. Anomaly based IDSs are divided into three types based on nature of processing such as Statistical based, Knowledge based and Machine learning based Intrusion detection methodologies [7, 8].

Statistical based IDSs work by analyzing network traffic and then it generates profile reflecting its operating nature. Reference profile is created when network is functioning in normal condition in absence of any attack. Then after, profiles are created periodically and network is monitored. By comparing profiles to reference profile, anomaly Score is generated. If deviation is above certain threshold, IDS will indicate existence of intrusion.

Knowledge based anomaly IDSs depends on pre information or knowledge of network parameters at normal conditions and at different attacks. These can be

dependent on expert systems based on rules of classification for audit data, finite state machine or any data clustering and outlier detection techniques.

Machine learning based anomaly IDSs generate model of some analyzed pattern. These can be updated periodically, for improvement in performance of intrusion detection based on previous results. These can make use of different techniques such as fuzzy logic, Marrow models, Bayesian networks, neural networks or genetic algorithms.

2.2 Misuse Based Detection

This can be called as Rule based or Signature based detection as signatures of already known attacks are generated to detect future attacks. If suppose there are 3 wrong login attempts, we can consider it as intrusion and whenever next time such attempts/signatures are recorded it is considered as Intrusion. Benefit of this method is that it can detect known attacks very effectively and so these have low false positive rate. Drawback of this technique is that by these methods it is not possible to detect the new types of attacks. These can be considered similar to Anti-Virus systems as these detect mostly known attack patterns [9]. In rule based IDSs the behaviors that attempt to break the rules of networking are considered as anomalies. In [10], author presented some rules to detect network anomalies, such as Interval, Retransmission, Integrity, Delay rule.

2.3 Specification Based Detection

In this technique, specifications and limits about the correct execution of some program is already described. Operation of program with respect to described specifications is checked [11]. These kinds of methods are capable of detecting the previously unknown attacks. Also, these incur low false positive rate.

Major difference between Anomaly based and Misuse based detection method is that, first tries to detect effects of bad behavior and second tries to detect already known bad behaviors [9].

Specification based technique take advantage of both techniques to characterize illegal behavior. In this method, attacks are detected as deviations from specifications about execution of program similar to anomaly based approach. These have low false alarm rate as compared to anomaly based method as specifications are selected manually. Disadvantage of this technique is that cost and time associated with development of specifications and constraints is high relative to low false alarm rate [12].

3 Decision Making in IDS

There are two ways of making a decision about the intrusion in a system.

3.1 Collaborative Decision Making

In this method, decisions about events are taken by considering the collaboration and interaction among all (or some) network members. In this, event is decided as intrusion if majority of voting is against the normality of event.

3.2 Independent Decision Making

In this, each and every member of network (sensor node) takes decision about the events around them.

According to [8], decisions about particular event are divided in four categories such as False Negative, False Positive, True Negative and True Positive.

Some of the events such as limited transmission power, collisions, fading battery supply, and packet drop etc. lead to false positives due to wireless nature of communication for IDSs in WSNs [13].

- After alert from IDS about any intrusion IDS doesn't try to prevent because prevention part is left with IPS. After alert from IDS following actions should be taken.
- It should generate audit records.
- Network members, system administrator and base station should get notification of intrusion.
- Location of intrusion and its identity should be provided with notification of intrusion.
- If intrusion exists, in order to stop the intrusion, mitigation method should be induced. For example, there should be collaborative system where all network members are able to take corrective action. Especially, network members which are near to location of incident should start taking corrective actions.

4 IDS Proposed for WSNs

In this section, IDS proposed for WSNs are summarized. Applying traditional IDSs directly to WSN is difficult, so first in Sect. 4.1, limitations of WSN and challenges of WSN are presented. Section 4.2 presents the overview on major IDSs for WSNs.

4.1 Limitations and Research Challenges in WSNs

WSNs are lacking in infrastructure (i.e. gateways, routers, base stations, etc.) which makes designing algorithms and WSNs are limited by resources such as bandwidth, throughput, which need to be used wisely. Following are some of the major limitations and related challenges that need to be considered while designing IDSs for WSN.

- WSNs are lacking in Infrastructure to support the operations of communication, routing, encryption, traffic analysis etc.
- There is always chance of physical capture, tampering or hijacking of sensor node which can compromise network operation.
- Nodes which are compromised are prone to various attacks such as black hole, wormhole, sinkhole etc., which can halt the operation of network.
- Decisions need to be taken in collaborative fashion. There is lack of trusted authority in WSNs.
- There is possibility of eavesdropping as communication is wireless which can reveal important data to adversaries.

Whenever there is need to design IDS for WSN, above limitations and challenges should be considered.

4.2 Proposed Schemes

IDSs that are proposed for Wireless Sensor Network are as follows.

4.2.1 Clustering (Hierarchical) Based IDSs

In [14], author proposed hierarchical framework for intrusion detection and processing in WSN. For the experiments they gave the importance to one hop clustering and believed that IDS is helpful for securing industrial applications which is carried out through two lines of defense.

In [15], Method is used to detect intrusion in energy efficient way based on isolation table. They proposed IDS with two- level of clustering. According to the experiments they have conducted isolation table helps them to detect intrusions in efficient manner. The problem with this approach is that, each level need to monitor the other level and it should report abnormal behaviors to base station. But if higher level does not report intrusion to the base station then there can be problem to deal with intrusion. In this case, higher level nodes can just block the alert messages generated by lower level nodes.

In [16], IDS based on clustering approach focuses on security of CHs. In this approach, CH is monitored by members of cluster in time scheduled manner so that energy for cluster members will be saved. And at same time, cluster head monitors the cluster members by not taking help of them which also saves energy of cluster members. Even though this approach saves energy of cluster members, it has problem with its key management which is part of IDS that establishes pairwise keys among nodes. IDS make use of keys to authenticate the messages. In WSN new nodes need to be deployed with time, so key management approach is not that much appropriate for IDS.

In [17], hierarchical IDS model is considered where network is divided into different groups called cluster with cluster head for each. In this model centralized routing is used where packets are forwarded to CH first and then base station. Intruder detectors are placed at CH so that minimum number of detectors will be required. This work doesn't have any simulation result and it not clear whether this approach works as promised.

4.2.2 Distributed and Collaborative IDS

In [18], Distributed approach is proposed as solution to cooperative intrusion detection, where nodes are equipped with local detection mechanism and they are supposed to identify intrusion in distributed way. Detector modules get triggered when they identify any intrusion in neighborhood sensor node. In [10], Specification based intrusion detection algorithm is proposed, where decentralized approach is used in which intrusion detector were placed in entire network. Whatever information is collected and its processing is carried out in distributed fashion. Authors claim that their distributed approach is far better than centralized approach as intrusion detector at different places had different views of network being distributed throughout network.

4.2.3 Statistical Model Based Approach

In [19], authors presented algorithm which first identified the suspected nodes and then it start identifying intruder in list by making use of network flow graph. This algorithm helps to detect sinkhole attacks. Algorithm implemented the parametric technique of statistical approach based on chi-square test. According to author's observation, this approach is reasonable as far as communication and computational loads are concerned.

4.2.4 Game Theory Based Approaches

Maximum times these approaches are provided as solutions of security for wired networks. But, it is little bit difficult to implement it in Wireless sensor network as these are having some limitations of energy. Also performance of Wireless sensor network decreases as new node is added. In [20], non-co-operative approach was proposed for detecting misbehaving nodes in clustered sensor network. A non-co-operative game approach, which formulates attack defense game as non-co-operative two players non zero sum game, achieves Nash equilibrium whenever defense player finds and protects most vulnerable cluster.

In [21, 22], authors considered participants of game as attack and detection and strategies for both parties have been formulated. Non cooperative, non-zero game model approach has been considered as a normal strategy. Both of these approaches focus on finding out the weakest node in network and then strategy has been provided to defend that node. Drawback of these schemes is that only one of intrusion can be detected by leaving others not detected.

4.2.5 Anomaly Detection Based IDSs

In [23], authors have presented the survey article on anomaly based intrusion detection schemes. Authors have suggested considering energy consumption factor whenever one is going to design intrusion detection system so as to minimize energy consumption.

In [24], lightweight method has been proposed to detect the intrusion that is anomalous. In this approach, information from OSI layers of protocol stack such as routing tables, list of neighbors sleep/wake up schedules, strength of received signal, MAC layer transmission schedules has been considered as main idea to detect anomalous behavior. Multiple detectors have been placed to monitor different layers of OSI stack, so that detection rate will be increased. This approach considers only outsider attack by forgiving the outsider attack only.

4.3 Drawbacks of Existing IDS

(a) ***Simulation***

No proper simulation has been proposed till now for anomaly based or misuse-based intrusion detection scheme. It is cumbersome to analyze IDS mechanism effectively as there is lack of real network.

(b) ***Real world implementation***

As per today's knowledge, only some real world implementations of IDS schemes are available. In [13], author has shown some real world implementation of Cooperative intrusion detection scheme in wireless sensor network. Even though some simulations and some statistical analysis are available, these implementations are important to check applicability of IDS in real world.

(c) ***Lightweight modules***

Sensor nodes in Wireless Sensor Networks are battery operated and these batteries are limited in power. So while designing any IDS one should consider energy factor so that IDS should consume less energy as much as possible.

(d) ***Attack Specific***

Most existing IDS detect only one or two attacks by using different network and hardware considerations. It is hard to combine all methods in universal platform.

4.4 Issues Concerning the Proposed Schemes

Following issues are drawn in various proposed IDS in WSNs:

In Clustering based IDS, clustering algorithms may consume energy for formation of clusters. After creation of cluster, Cluster heads are elected and they can fail at some point so they need to be secured. If cluster head is not a powerful node then overhead of CH makes network to utilize resources very quickly.

In agent based IDS, network load and latency have been reduced, but they cause very high energy consumption of nodes. Communication in agents or in agent and coordinator can become reason for bottle neck or congestion in network.

Rule based IDSs need continuous updating of rules so as to deal with new attacks.

In game theory based IDSs, network security administrator can change the parameters to adjust the intrusion detection rate. Drawback of these IDSs is that, it is not-adaptive and it requires interference of people for stable operation.

4.5 Future Directions for Selecting the IDS for WSNs

Today, energy consumption is the biggest issue in wireless sensor network. WSN needs to sense surrounding phenomenon, process that information and then transmit the resultant data. For all these operations to be carried out WSN consumes a lot of energy. That's why, design of IDS should be such that it should consume least energy and should make WSN to utilize its energy for important operations. Hierarchical model of IDS is best suited as a solution of requirement of least consumption of energy. In this, network will be divided into different clusters and each cluster will have a CH. In this model, CH is responsible to do communication with Base Station (BS) and there is no need for all nodes to send data directly to BS, which ultimately reduces energy consumption and increases lifetime of WSN.

Apart from all these IDS that have been surveyed, we have to consider trust factor of sensor nodes to find out the malicious activities in WSN. To the best of our knowledge, there are no proper IDS that consider the trust factor to design IDS for WSN that consider the benefits of hierarchical approach. In future, this will be a good topic of research.

5 Conclusion

This paper gives introduction about various intrusion detection methodologies such as anomaly based, Misuse based, specification based intrusion detection methodologies. Also, this paper focuses on decision making methodologies that help to decide whether particular sensor node is malicious or not. Thirdly, the difference between MANET and WSN has been described with limitations of WSN and the IDSs proposed for WSN have been discussed with their important aspects. Finally, the drawbacks and issues concerning existing IDS have been discussed and future directions have been suggested in order to help researchers to select IDS.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)
2. Zhou, Y., Fang, Y., Zhang, Y.: Securing wireless sensor networks: a survey. IEEE Commun. Surv. Tutorials **10**(3), 6–28 (2008)
3. Cayirci, E., Rong, C.: Security in Wireless Ad Hoc and Sensor Networks. Wiley, New York (2009)
4. Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutorials **8**(2), 2–23 (2006)
5. Padmavathi, G., Shanmugapriya, D.: A survey of attacks, security mechanisms and challenges in wireless sensor networks. Int. J. Comput. Sci. (IJCS) **4**(1), 1–9 (2009)
6. Butun, I., Sankar, R.: A brief survey of access control in wireless sensor networks. In: Proceedings of IEEE Consumer Communications and Networking Conference, Las Vegas, Nevada (2011)
7. Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., Vazquez, E.: Anomaly-based network intrusion detection: techniques, systems and challenges. J. Comput. Secur. **28**(1–2), 18–28 (2009). Elsevier
8. Patcha, A., Park, J.M.: An overview of anomaly detection techniques: existing solutions and latest technological trends. J. Comput. Netw. **51**(12), 3448–3470 (2007). Elsevier
9. Sobh, T.S.: Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art. J. Comput. Stand. Interfaces **6**, 670–694 (2006). Elsevier
10. da Silva, A.P., Martins, M., Rocha, B., Loureiro, A., Ruiz, L., Wong, H.C.: Decentralized intrusion detection in wireless sensor networks. In: Proceedings of 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet 2005), pp. 16–23. ACM Press (2005)
11. Anantvalee, T., Wu, J.: A survey on intrusion detection in mobile ad hoc networks. In: Xiao, Y., Shen, X.S., Du, D.-Z. (eds.) Wireless Network Security, pp. 159–180. Springer, New York (2007)

12. Sun, B., Osborne, L., Xiao, Y., Guizani, S.: Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Trans. Wirel. Commun. **14**(5), 63 (2007)
13. Michiardi, P., Molva, R.: Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Jerman-Blažič, B., Klobučar, T. (eds.) Advanced Communications and Multimedia Security. ITIFIP, vol. 100, pp. 107–121. Springer, Boston (2002). doi:10.1007/978-0-387-35612-9_9
14. Crossbow MICAz mote data sheet. http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/MICAz_Datasheet.pdf
15. Chen, R.C., Hsieh, C.F., Huang, Y.F.: A new method for intrusion detection on hierarchical wireless sensor networks. In: Proceedings of ACM ICUIMC-09 (2009)
16. Su, C.C., Chang, K.M., Kuo, Y.H., Horng, M.F.: The new intrusion prevention and detection approaches for clustering-based sensor networks. In: Proceedings of IEEE Wireless communications and Networking Conference (2005)
17. Strikos, A.A.: A full approach for intrusion detection in wireless sensor networks. School of Information and Communication Technology (2007)
18. Krontiris, I., Benenson, Z., Giannetsos, T., Freiling, F.C., Dimitriou, T.: Cooperative intrusion detection in wireless sensor networks. In: Roedig, U., Sreenan, Cormac, J. (eds.) EWSN 2009. LNCS, vol. 5432, pp. 263–278. Springer, Heidelberg (2009). doi:10.1007/978-3-642-00224-3_17
19. Ngai, E., Liu, J., Lyu, M.: On the intruder detection for sinkhole attack in wireless sensor networks. In: ICC 2006, Istanbul, Turkey (2006)
20. Agah, A., Das, S.K., Basu, K., Asadi, M.: Intrusion detection in sensor networks: a non-cooperative game approach. In: 3rd IEEE International Symposium on Network Computing and Applications, pp. 343–346 (2004)
21. Agah, A., Das, S.K., Basu, K. Asadi, M.: Intrusion detection in sensor networks: a non-cooperative game approach. In: Proceedings of 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004), pp. 343–346 (2004)
22. Agah, A., Das, S.K.: Preventing DoS attacks in wireless sensor networks: a repeated game theory approach. Int. J. Netw. Secur. **5**(2), 145–153 (2007)
23. Rajasegarar, S., Leckie, C., Palaniswami, M.: Anomaly detection in wireless sensor networks. IEEE Trans. Wirel. Commun. **15**(4), 34–40 (2008)
24. Bhuse, V., Gupta, A.: Anomaly intrusion detection in wireless sensor networks. J. High Speed Netw. **15**(1), 33–51 (2006)