wjert, 2020, Vol. 6, Issue 6, 180-192. Original Article ISSN 2454-695X

World Journal of Engineering Research and Technology

WJERT

www.wjert.org

Impact Factor Value: 5.924

SURVEY ON INTRUSION DETECTION APPROACHES FOR WIRELESS SENSOR NETWORKS

Sumalatha M. S.*[1], Dr. V. Nandalal[2], C. Santhoshkumar[3]

[1]PhD Scholar Anna University Chennai.

[2]Professor, Department of ECE, Sri Krishna College of Engineering and Technology, Coimbatore-641008.

[3] Demonstrator, Department of Electrical and Electronics Engg., NSS Polytechnic College Pandalam, Kerala.

Article Received on 11/10/2020 **Article Revised on 01/11/2020** **Article Accepted on 22/11/2020**

***Corresponding Author**
Sumalatha M. S.
PhD Scholar Anna University Chennai.

ABSTRACT

Wireless sensor network (WSN) has emerged as one of the most promising technologies for the future. This has been enabled by advances in technology and availability of small, inexpensive, and smart sensors resulting in cost effective and easily deployable WSNs. However, researchers must address a variety of challenges to facilitate the widespread deployment of WSN technology in real-world domains. In this survey, give an overview of wireless sensor networks and their application domains including the challenges that should be addressed in order to push the technology further. In this work, the WSNs are generally deployed in an unattended area, they are prone to various types of attacks. In this scenario, legitimate node shares data to the malicious node and the data are lost. So that it becomes necessary to secure the network from this type of attack. The Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. This paper aims to study, discuss and analyze the various techniques for detection of security attack in Wireless Sensor Networks. Also various protocols affected by security attack are studied and analyzed. The existing research methodologies are discussed with their merits and demerits, so that the further research works can be concentrated more.

KEYWORDS: Wireless Sensor Networks, Intrusion Detection System, Sybil attack, Routing.

INTRODUCTION

Wireless Sensor Network consists of a large number of small and low cost sensor nodes which are randomly deployed in an area. The sensor nodes have computational capability to carry out simple computations and transmit the required information.[1] These nodes transmit information to the sink node that aggregates the entire information received from other nodes and generates a summary data to be transmitted to another network. These sensor nodes can collectively monitor physical and environmental conditions like pressure, temperature, humidity and sound vibrations. Such features ensure a wide range of applications for wireless sensor network such as military, medical, industrial, disaster relief operations, environmental monitoring, traffic surveillance, agriculture, infrastructure monitoring.[2,3]

Despite the innumerable applications of WSNs, these networks have several restrictions, e.g., limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSNs is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. The design of routing protocols in WSNs is influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs.[4]

In general, routing in WSNs can be divided into flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, however, nodes will play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network. A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels.[5] Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation. In addition to the above, routing protocols can be classified into three categories, namely, proactive, reactive, and hybrid protocols depending on how the source finds a route to the destination. In proactive protocols, all routes are computed before they are really needed, while in reactive protocols, routes are computed on demand. Hybrid protocols use a combination of these two ideas.

When sensor nodes are static, it is preferable to have table driven routing protocols rather than using reactive protocols. A significant amount of energy is used in route discovery and setup of reactive protocols.[6]

The interesting feature of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks, while the routing criteria and wireless sensor network modeling are getting much precedence, the security concerns are yet to get pervasive focus.[7] The security requirement of WSN must include attributes such as confidentiality, integrity, data freshness, availability, and authentication. All network models allow provisions for implementing above said properties in order to assure protection against attacks to which these types of networks are vulnerable.[8] The majority of sensor nodes are deployed in dangerous environment, they are susceptible to various attacks that are caused by malicious or compromised nodes in the network. The malicious nodes can alter the normal behaviour of the network, tamper with the node's hardware and software, transmit false information, or drop the required information. Hence, security of wireless sensor network becomes a critical issue. Security in wireless sensor networks is an imperative, significant issue, required and very important requirement, due to: 1) WSNs are susceptible against security attacks (Broadcast and wireless environment of transmission medium); 2) Nodes installed on hostile environments (insecure physically) 3) Unattended nature of WSNs.[9]

Wireless sensor networks are very weak and susceptible to many types of security attacks cause to the broadcast. Also, the other reason is put the sensor nodes in a dangerous environment whether in public area or battlefield. The security threats and attacks in wireless sensor networks as follows: Sybil attacks, Wormhole attacks, Denial of service attacks, Hello flooding attacks and sinkhole attacks can be present in a sensor networks while communication takes place among the nodes.[13]

Sybil attack.[10] definite this attack by: "malevolent device, taking multiple identities in an illegitimate way", attacker can use the identities of the others nodes in order to take part in distributed algorithms such as the election. Wormhole attack: attackers here are strategically placed at different ends of a network. They can receive messages and replays them in different parts by means of a tunnel.[11] Denial of service attacks: Denial of service attacks can disrupt wireless transmission and occur either unintentionally in the form of interference, noise or collision at the receiver side or at the context of attacks. HELLO flood attack: many routing protocols use "HELLO" packet to discover neighboring nodes and thus to establish a

topology of the network. The simplest attack for an attacker consists in sending a flood of such messages to flood the network and to prevent other messages from being exchanged.[13] Sink hole attack: a node falsifies routing information to force the passage of the data by itself, later on; its only mission is then, nothing to transfer, creating a sink or black hole in the network.[12]

A variety of attacks are possible in Wireless Sensor Network (WSN). These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. The security attack detection is a complex issue which is analyzed and evaluated by the various researchers using different methodologies. In this research work, those research methodologies are discussed in terms of their working procedure and their functionalities along with various performance measures. The benefits and drawbacks that arise in those methodologies also discussed in the detailed manner.

EXISTING RESEARCH METHODOLOGIES

Jun Wu et al[14] (2016) designed a hierarchical framework based on chance discovery and usage control (UCON) technologies to improve the security of WSNs while still taking the low-complexity and high security requirements of WSNs into account. The features of continuous decision and dynamic attributes in UCON can address ongoing attacks using advanced persistent threat detection. In addition, author used a dynamic adaptive chance discovery mechanism to detect unknown attacks. To design and implement a system using the mechanism described above, a unified framework is proposed in which low level attack detection with simple rules is performed in sensors, and high level attack detection with complex rules is performed in sinks and at the base station. Moreover, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies are used to perform attack mitigation when either low level or high level attacks are detected. An experiment was performed to acquire an attack data set for evaluation.

Yuxin Liu et al[15] (2016) designed an active detection-based security and trust routing scheme named ActiveTrust is proposed for WSNs. The most important innovation of ActiveTrust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security. More importantly, the generation and distribution of detection routes are given in the ActiveTrust scheme, which can fully use the energy in non-hotspots to create as many detection routes as needed to achieve the desired security and energy efficiency. Both comprehensive theoretical

analysis and experimental results indicate that the performance of the ActiveTrust scheme is better than that of previous studies. ActiveTrust can significantly improve the data route success probability and ability against black hole attacks and can optimize network lifetime.

Nina Skorin-Kapov et al[16] (2010) designed a novel approach to help deal with these issues in the network planning and provisioning process as a prevention mechanism. Namely, author proposed to route lightpaths in such a way as to minimize the potential damage caused by various physical-layer attacks. It present a new objective criterion for the routing and wavelength assignment (RWA) problem, which is called as the maximum Lightpath Attack Radius (maxLAR) and formulate the routing sub problem as an integer linear program (ILP). Author test it on small networks to get an insight into its complexity and compare it to a formulation that minimizes congestion. Results indicate that our formulation achieves significantly better results for the maxLAR while obtaining near-optimal or optimal congestion in all cases. For larger networks, author proposed a tabu search algorithm for attack-aware light path routing, in combination with an existing graph-coloring algorithm for wavelength assignment.

Wei Wei et al[17] (2010) presented SybilDefender, a sybil defense mechanism that leverages the network topologies to defend against sybil attacks in social networks. Based on performing a limited number of random walks within the social graphs, SybilDefender is efficient and scalable to large social networks. Author experimented on two 3,000,000 node real-world social topologies show that SybilDefender outperforms the state of the art by more than 10 times in both accuracy and running time. SybilDefender can effectively identify the sybil nodes and detect the sybil community around a sybil node, even when the number of sybil nodes introduced by each attack edge is close to the theoretically detectable lower bound. Also, proposed two approaches to limiting the number of attack edges in online social networks.

Guojun Wang et al[18] (2015) presented how to address Sybil attack, an active attack, in which peers can have bogus and multiple identities to fake their owns. Peer to peer (P2P) e-commerce applications exist at the edge of the Internet with vulnerabilities to passive and active attacks. These attacks have pushed away potential business firms and individuals whose aim is to get the best benefit in ecommerce with minimal losses. The attacks occur during interactions between the trading peers as a transaction takes place. Most existing

work, which concentrates on social networks and trusted certification, has not been able to prevent Sybil attack peers from doing transactions. This work exploits the neighbour similarity trust relationship to address Sybil attack. In this approach, duplicated Sybil attack peers can be identified as the neighbour peers become acquainted and hence more trusted to each other.

Yue Liu et al[19] (2015) designed two efficient methods for separating the valid RSSI observations of behaving nodes from those falsified by malicious participants. Further, author note that prior signal print methods are easily defeated by mobile attackers and develop an appropriate challenge-response defense. Finally, we present the Mason test, the first implementation of these techniques for ad hoc and delay-tolerant networks of commodity 802.11 devices. Illustrated the performance in several real-world scenarios.

Guoxing Zhan et al[20] (2012) designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. Further, we have implemented a low-overhead TARF module in TinyOS; as demonstrated, this implementation can be incorporated into existing routing protocols with the least effort.

John Felix Charles Joseph et al[21] (2018) presented the detection system maximizes the detection accuracy by using cross-layer features to define a routing behaviour. For learning and adaptation to new attack scenarios and network environments, two machine learning techniques are utilized. Support Vector Machines (SVMs) and Fisher Discriminant Analysis (FDA) are used together to exploit the better accuracy of SVM and faster speed of FDA. Instead of using all cross-layer features, features from MAC layer are associated/correlated with features from other layers, thereby reducing the feature set without reducing the information content. Various experiments are conducted with varying network conditions and malicious node behavior. The effects of factors such as mobility, traffic density, and the packet drop ratios of the malicious nodes are analyzed.

Ju Ren et al[22] (2016) presented a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. The CRS-A evaluates the data forwarding behaviors of sensor nodes, according to the deviation of the monitored packet loss and the estimated normal loss. To optimize the detection accuracy of CRS-A, author theoretically derive the optimal threshold for forwarding evaluation, which is adaptive to the timevaried channel condition and the estimated attack probabilities of compromised nodes. Furthermore, an attack-tolerant data forwarding scheme is developed to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network.

Li, et al[23] (2008) presented a distributed group-based intrusion detection scheme that meets all the above requirements by partitioning the sensor networks into many groups in which the sensors in each group are physically close to each other and are equipped with the same sensing capability. In this work, intrusion detection algorithm takes simultaneously into consideration of multiple attributes of the sensor nodes to detect malicious attackers precisely. The experiments with real data that algorithm can decrease the false alarm rate and increase the detection accuracy compared with existing intrusion detection schemes while lowering the computation and transmission power consumption. Thus the experiment results show that this scheme can achieve a lower false alarm rate and a higher detection accuracy rate than the existing detection schemes. At the same time, it can also reduce the monitoring power consumption with the requirement of grouping the sensor nodes in the network only once.

Tao Shu et al[24] (2015) observed a sequence of packet losses in the network, interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. Also interested in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, author proposed to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, developde a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information

reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-blockbased mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity.

Shiyu Ji et al[25] (2015) desinged a centralized algorithm to detect wormholes and shown its correctness rigorously. For the distributed wireless network, we propose DAWN, a Distributed detection Algorithm against Wormhole in wireless Network coding systems, by exploring the change of the flow directions of the innovative packets caused by wormholes. We rigorously prove that DAWN guarantees a good lower bound of successful detection rate. We perform analysis on the resistance of DAWN against collusion attacks. Author find that the robustness depends on the node density in the network, and proved a necessary condition to achieve collusion-resistance. DAWN does not rely on any location information, global synchronization assumptions or special hardware/middleware.

Comparative Analysis

S.no	Reference	Method	Merits	Demerits	Result
1.	Jun Wu et al[14] (2016)	Usage control (UCON)	It is capable of continuous decision making, is used to address the ongoing attacks.	High security performance is needed.	the result of attack experiment and simulation shown. it is feasible for WSNs and offers a significant improvement over current attack detection accuracy
2.	Yuxin Liu et al[15](2016)	ActiveTrust scheme,	The ActiveTrust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly to successful routing probability.		The theoretical analysis and experimental results have shown that our scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases.
3.	Nina Skorin-Kapov et al[16](2010)	Novel approach and Tabu search algorithm	Fast detection and Efficient for Testing on a larger network.	Careful power equalization placement in order to thwart jamming attack.	Testing and comparing with existing approaches from literature indicate its superiority with respect to the

					maxLAR and average lightpath load, However, this is justified with the obtained improvement in network security
4.	Wei Wei et al[17] (2010)	SybilDefender and Combo algorithm	This algorithm is Highly accurate	Need to improve the security	The results are tabulated by using proposed method.
5.	Guojun Wang et al[18] (2015)	SybilTrust and distributed structured approach	This ensures that the group detection algorithms to identify Sybil attack peers to be efficient and scalable in large P2P e-commerce networks.	It is only suitable for detect the Sybil attack	Security and performance analysis shows that Sybil attack can be minimized by the proposed neighbour similarity trust.
6.	Yue Liu et al[19](2015)	Mason test	The proposed system is highly efficient for office environment.	It is only acheives 61% of Sybil identitfication in the outdoor environment.	It eliminates 99.6%–100% of Sybil identities in office environments, 91% in a crowded high motion cafeteria, and 96% in a high-motion open outdoor environment.
7.	Guoxing Zhan et al[20] (2012)	Trust-Aware Routing Framework (TARF)	Steady improvement in network performance	The system needs to improve in routing path	The effectiveness of TARF is verified through extensive evaluation with simulation and empirical experiments on large-scale WSNs
8.	John Felix Charles Joseph et al[21] (2018)	Cross layer apporoach.	It increases the reliability of global IDS and knowledge sharing.	Designed methodology is analyzed only for sinking behaviour.	Experiments based on simulation show that the proposed cross-layer approach aided by a combination of SVM and FDA performs significantly better than other existing approaches.
9.	Ju Ren et al[22]	Channel-aware	Can achieve a high detection accuracy	This method is little	simulation results show that the

	(2016)	Reputation System with adaptive detection threshold (CRS-A)	with both of false and missed detection probabilities close to 0, and improve more than 10% data delivery ratio for the network.	difficult to applying with mobile sensor node.	proposed CRS-A can achieve a high detection accuracy with low false and missed detection probabilities, and the proposed attack tolerant data forwarding scheme can improve more than 10% data delivery ratio for the network.
10.	Li, et al.,[23](2008)	Group-based Intrusion Detection Scheme	The proposed system decrease the false alarm rate and increase the detection accuracy	Need to improve the security of cluster-based sensor networks.	The false alarm ratios and the detection accuracy ratios of the refined group-based intrusion detection scheme with alpha-quantile of the chi-squared distribution 0.99, 0.95 and 0.90, respectively.
11.	Tao Shu et al[24] (2015)	Homomorphic Linear Authenticator (HLA) based public auditing architecture	Packet-loss reporting by individual nodes are easy by proposed method.	This technique is limited to static or quasistatic wireless ad hoc networks.	Verified the proposed mechanisms achieve significantly better detection accuracy than conventional methods.
12.	Shiyu Ji et al[25] (2015)	Distributed detection Algorithm against Wormhole in wireless Network (DAWN)	Proposed algorithm is efficient and practical. It also very effective.	It is only based on the local information that can be obtained from regular network coding protocols	Extensive experimental results have verified the effectiveness and the efficiency of DAWN.

CONCLUSION

In this work, various techniques to defend against security attack are surveyed. Also various protocols affected by security attack are studied and discussed. From the study, it can be concluded that, these various approaches of Intrusion detection system help to detect and prevent the security attack for Wireless Sensor Networks (WSNs). This research work

analyses the various Intrusion detection system methodologies by different authors has been discussed. Those research methodologies are discussed along with their benefits and drawbacks in the detailed manner to find the effectiveness of every algorithm.

REFERENCE

1. Virmani, D., Soni, A., Chandel, S., & Hemrajani, M. Routing attacks in wireless sensor networks: A survey. *arXiv preprint arXiv*, 2014; *1407.3987*.
2. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey, Computer Networks", 2000; 393- 422.
3. A.S.K. Pathan, H.W. Lee, C.S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Communications, IEEE Transaction, Feb 2006.
4. Al-Karaki, J. N., & Kamal, A. E. Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications*, 2004; *11*(6): 6-28.
5. Manjeshwar and D. P. Agarwal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001.
6. D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.
7. Sharma, P. Survey on Orthogonal Dimensions of Sybil Attack in Wireless Sensor Network, 2004.
8. Manisha, G. G. Attacks on Wireless Sensor Networks: A Survey. *International Journal*, 2013; *3*(10).
9. S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks,DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited, 2009.
10. John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, 2006.
11. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", In First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
12. Fei Hu and Neeraj K. Sharma, "Security considerations in ad hoc sensor networks", Ad Hoc Networks, Published by Elsevier Science, 2005; 69–89.

13. Messai, M. L. Classification of attacks in wireless sensor networks. *arXiv preprint arXiv:1406.4516*, 2014.
14. Wu, J., Ota, K., Dong, M., & Li, C. A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities. IEEE Access, 2016; 4(4): 416-424.
15. Liu, Y., Dong, M., Ota, K., & Liu, A. ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 2016; 11(9): 2013-2027.
16. Skorin-Kapov, N., Chen, J., & Wosinska, L. A new approach to optical networks security: Attack-aware routing and wavelength assignment. IEEE/ACM Transactions on Networking (TON), 2010; 18(3): 750-760.
17. Wei, W., Xu, F., Tan, C. C., & Li, Q. SybilDefender: A defense mechanism for sybil attacks in large social networks. IEEE transactions on parallel and distributed systems, 2013; 24(12): 2492-2502.
18. Wang, G., Musau, F., Guo, S., & Abdullahi, M. B. Neighbor similarity trust against sybil attack in P2P e-commerce. IEEE transactions on parallel and distributed systems, 2015; 26(3): 824-833.
19. Liu, Y., Bild, D. R., Dick, R. P., Mao, Z. M., & Wallach, D. S. The Mason test: A defense against Sybil attacks in wireless networks without trusted authorities. IEEE Transactions on Mobile Computing, 2015; 14(11): 2376-2391.
20. Zhan, G., Shi, W., & Deng, J. Design and implementation of TARF: A trust-aware routing framework for WSNs. IEEE Transactions on dependable and secure computing, 2012; 9(2): 184-1.
21. Joseph, J. F. C., Lee, B. S., Das, A., & Seet, B. C. Cross-layer detection of sinking behavior in wireless ad hoc networks using SVM and FDA. IEEE Transactions on Dependable and Secure Computing, 2011; 8(2): 233-245.
22. Ren, J., Zhang, Y., Zhang, K., & Shen, X. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. IEEE Transactions on Wireless Communications, 2016; 15(5): 3718-3731.
23. Li, G., He, J., & Fu, Y. Group-based intrusion detection system in wireless sensor networks. Computer Communications, 2008; 31(18): 4324-4332.
24. Shu, T., & Krunz, M. Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. IEEE Transactions on mobile computing, 2015**;** 14(4): 813-828.

25. Ji, S., Chen, T., & Zhong, S. Wormhole attack detection algorithms in wireless network coding systems. IEEE transactions on mobile computing, 2015; 14(3): 660-674.