International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 10 Issue 6, November 2022

A Review on Evaluations of Malicious Node Detection in Wireless Sensor Network Environment

Pragati Nigam, Vivek Sharma
CSE Department, TIT Bhopal, India
priyanigam4795@gmail.com, Sharma.vivek95@yahoo.in

Abstract- Deployed in a hostile environment, the adversary could easily compromise individual wireless sensor network nodes due to constraints such as limited battery lifetime, memory space and computing capability. Wireless Sensor Network is broadly used today in various fields, such as environmental control, surveillance task, object tracking, military applications etc. As WSN is an ad-hoc network deployed in an environment that is physically insecure, intrusion detection has been one of the major areas of research in WSN. In order to achieve an appropriate level of security in WSNs, we cannot depend on cryptographic techniques, as these techniques fall prey to insider attacks. This paper discusses the watchdog mechanism, one of the intrusion detection techniques in Wireless Sensor Networks. Watchdog is a monitoring technique which detects the misbehaving nodes in the network. The main area of focus in this paper is being made to the problems with existing watchdog techniques for malicious node detection. A brief survey is presented on different trust-based models aimed at WSNs for malicious node detection and dealing with the security of wireless sensor networks, starting with a brief overview of the sensor networks and discussing the current state of the security attacks in WSNs. Various types of attacks are discussed, and their countermeasures are presented. A brief discussion on future research directions in WSN security is also included. Malicious node detection causing attacks, packet loss causes, and data modifications are the challenges to overcome due to the network's malicious nodes. Moreover, different sorts of malicious attacks on trust models are identified, and whether the existing trust models can withstand these attacks or not has been assessed.

Keywords: Wireless Sensor Networks; Fault Detection; Malicious Node Detection, Attacks, Security, Threats, filtering, Routing, flooding.

I. INTRODUCTION

Wireless sensor networks (WSNs) are innovative large-scale wireless networks consisting of distributed, autonomous, low-power, low-cost, small-size devices using sensors to collect information through infrastructure-less ad-hoc wireless networks. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian applications, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of their unique characteristics. First, sensor nodes are very sensitive to production costs since sensor networks consist of many sensor nodes. [1] the sensor node can be equipped with a range of mechanical, thermal, biological, chemical, optical, or magnetic sensors to monitor environmental characteristics. A radio is installed for wireless communication to convey the data to a base station since the sensor nodes often deploy in difficult-to-access areas and have limited memory (e.g., a laptop, a personal handheld device, or an access point to a fixed infrastructure). A sensor node's primary power supply is a battery. Depending on the suitability of the location where the sensor will be placed, a supplementary power supply that gathers electricity from the environment, such as solar panels, may be added to the node. Actuators could be integrated into the sensors, depending on their intended function and method. Typically, a WSN has very little or no infrastructure. It comprises several sensor nodes (from a few tens to thousands) cooperating to monitor an area and gather environmental data. WSNs come in two flavours: structured and unstructured. A dense cluster of sensor nodes constitutes an unstructured WSN. Sensor nodes may be set up in the field on a whim [2]. The network is deployed and then left unattended to carry out monitoring and reporting tasks. Because there are so many nodes in an unstructured WSN, it is challenging to manage the connection and identify faults. In a structured WSN, the placement of the sensor nodes follows a predetermined pattern. ([3] A structured network allows for the deployment of fewer nodes with cheaper network administration and maintenance expenses. Since nodes are now positioned at particular places to provide coverage, fewer nodes may be deployed, whereas ad hoc deployment could leave regions unattended. The article consists of VII section, in section describes the introduction to WSN, section II elaborates on existing work on the security issue and their prevention, section III describes the proposed MDP-AODV technique, in section IV discuss the proposed MDP-AODV working architecture, section V describe the simulation environment, in section VI describe the simulation analysis result and in section, VII describe conclusion and future approach on WSN network.

1.1 Summary of Various Compromised Nodes Detection Techniques

Many techniques have been proposed till now for detecting and recovering compromised nodes. This paper gives some idea regarding various compromised node detection and recovery schemes and their pros and cons.

1. **Weighted Trust Evaluation Scheme: The author introduced a weighted trust evaluation scheme in hierarchical network architecture, consisting** of three different sensors at three different layers. The trailing position of the architecture contains low-power Sensor Nodes (SN), which gather information about various sensors at this lower layer level. The middle layer contains the Forwarding Node (FN), which assumes who is trustful and won't be compromised. The FN is responsible for collecting information from the lower layer, computing aggregation results, and committing the information to the Access point (AP). The FN is also responsible for verifying the correctness of the information gathered from the SN. The Access point or Base station is placed at the leading position of the architecture and assumes who is also trustworthy and who is responsible for transferring the output to the outside world.

2. **STL Approach** Generally, WSN consists of hundreds or thousands of sensor nodes and creating effective topology and protecting all nodes from vulnerable attacks is impractical. To overcome this situation, the author introduced Stop Transmission and Listened to approach, one of the simple and effective techniques for detecting a malicious node. This number of sensor nodes is deployed in an environment, each with a built-in time limit to stop their transmission. Each node starts its sensing process within its sensing region, and each node can detect the malicious node. After sensing, the sensed data is forwarded to the sink node, and each node has to stop its transmission every few seconds and listen to malicious behaviour. The malicious nodes transmit data during the non-transmission period because those nodes are unaware of this non-transmission built-in period. If malicious nodes are not transmitting any data during the non-transmission time, they will be caught during another frequent non-transmission time. This approach has some disadvantages, such as the whole network stopping its transmission at a time and suddenly starting, which will cause congestion and unwanted delay in the network operations. The simulation result shows the effectiveness of the approach.

3. **Auto regression technique** in this paper, the author considered the following assumption for detecting the maliciousness of the different sensor nodes in the same network. The sensor network is static, and each node passes a one-time authentication procedure. Every sensor node can store up to hundreds of bytes of keying material to secure the transfer of information through symmetric cryptography. The base station will not be compromised at any cost. Due to this assumption, the networks avoid eavesdropping, traffic analysis, spoofing, sinkhole, selective forward attack, wormhole attack, Sybil attacks and Hello flood attacks. The node-capturing attack is the biggest threat to the wireless sensor network, where an adversary gains full control over sensor nodes through direct physical access. The author introduced the Auto Regression model (AR model) to avoid these kinds of attacks. Each sensor node's time series of measured data relies on an autoregressive predictor placed in the base station. The basic principle is collecting past and present

values for each sensor node. It will be compared with the threshold and detect whether that sensor node behaves normally or abnormally. This scheme has some disadvantages. It follows symmetric key cryptography for information transmission, which causes key exchange problems and is an open issue in network security. Another important consideration is choosing an effective threshold for comparing the present and past behaviour of the sensor nodes. Through this study, the author shows the effective nests and efficiency of the AR model.

4. **Dual threshold** in this work, the author considered the following assumptions: The n numbers of sensors are deployed in the monitored area and have the transmission range RC. Each node knows its neighbours and their transmission range. Suppose two nodes are neighbours of each other if their distance is less than or equal to RC. The trust values of the neighbour are calculated based on the Weighted directed graph, and their lies between 0 and 1. If Wij=0 means node vi does not trust node VJ at all, Wij=1 means node vi trusts node VJ. In addition, vi also has a trust value ranging from 0 to 1. Once wii reaches 0, means node vi is faulty. The event region is assumed to be a circle with a radius re. If any event occurs in the region, nodes then alarm their neighbours. In event detection, each sensor node makes a local decision based on the sensor readings of its own and its neighbouring nodes. The malicious nodes are detected based on two thresholds, θ1 and θ2. The role of the θ1 is to minimize the false alarm rate. The role of the θ2 is to enhance the malicious node detection accuracy. For each node collecting binary reading of all its neighbours, compute U1 /U0+U1 to determine which group it belongs to. Generally, there are three groups: R1, R2 and R3. If a particular node vi at the region R1 if its computed value of U1 /U0+U1 is greater than θ1. A particular node vi at the region R2 if its computed value of U1 /U0+U1 lies between θ1 and θ2. All the remaining nodes are in group R3. After the division of the region, apply the hypothesis test and decide the behaviour of each node is normal or up normal. Through simulation results, the author evaluates the performance of the malicious node detection using a dual threshold scheme.

5. **SWATT**: Software-based Attestation for Embedded Devices Our environment is surrounded by several embedded devices ranging from a java enabled cell phones to sensor networks and smart appliances. Suppose an adversary can compromise one of our devices and modify the memory contents. To avoid this kind of maliciousness, the author introduced Software based Attestation (SWATT) to verify the memory contents of the embedded devices. SWATT can be applied in various fields, such as network printers, smart cell phones, electronic voting machines, smart cards etc. A verifier is used to verify the expected memory contents of the embedded device, which generates a random MAC key and sends this key to the embedded device. The device computes MAC on the entire memory using the key and returns the MAC value. The random keys are used to avoid replay attacks. The embedded device contains some empty memory filled with the number of zeros of an intruder.

II. RELATED WORK

In this section, we describe various existing WSN security techniques used to improve the WSN service, i.e., energy issues and security. Here those are working in the field of WSN service improvement. Dr. K. Sasi Kala Rani, *et.al.* [1] "Experimental Evaluations of Malicious Node Detection on Wireless Sensor Network Environment" utilizes the same logic of WSN in an enhanced way using adding some security metrics and associated communication strategies. A Modified Ad-hoc-On-Demand-Distance-Vector (mAODV) is introduced in this book to carry out the routing setups effectively. This suggested method of mAODV is derived from the logic of the conventional AODV model, but the metrics are improvised instead of employing the standard transmission and reception power ratio. Balakrishnan *et al.* [4] proposed a two-hop acknowledgement detection scheme (TWO PACK) based on the checkpoint node. The checkpoint node in the TWOACK technique is each node along the forwarding chain. An acknowledgement packet will be sent by node I, the receiving node, to node j, which is two hops distant. If node j does not receive the acknowledgement packet, it assumes that the link between nodes I and j is malicious and issues a warning to the source node. The TWOACK technique significantly increases the conflict and collision of network messages. Xiao et al. [5]

presented a multi-hop acknowledgement-based detection technique to address this issue (CHEMAS). The CHEMAS system randomly chooses certain nodes along the route from the source node to the base station to serve as checkpoint nodes. The acknowledgement packet is sent to the upstream node by the checkpoint node when it receives a packet. Liu. *et al.* [6] Novel system, based on a multi-hop acknowledgement mechanism, was presented to address Per-Hop acknowledgement (PHACK). In the Per-Hop acknowledgement system, each node in the forwarding path must transmit an acknowledgement packet for each packet to forward along with the regular packets to the originating node. However, these multi-hop acknowledgement-based techniques call for sending several confirmation packets, which will raise communication overhead and significantly shorten network life. To improve the effect of malicious node detection. Yang *et al.* [7] proposed a malicious node detection model based on reputation with enhanced low-energy adaptive clustering hierarchy in MNDREL. The cluster head nodes are chosen based on the upgraded routing protocol, and other nodes create various clusters by selecting the appropriate cluster head. The network's malicious nodes can be successfully discovered by analyzing the reputation value for the parent node as evaluated by the child node. The MNDREL model beat other WSN malware detection models with a decreased false alarm rate. However, the MNDREL model's real-time performance has to be enhanced. A reputation model for sensor networks based on a Gaussian distribution was developed by Xiao et al. (GRFSN). In this paradigm, each node's trust value is determined by summing its direct and indirect reputations, and then that value is compared to the trust threshold. A malicious node has a trust value lower than the trust threshold. This approach needs to establish a trust threshold, and however since the trust threshold is static, it frequently misjudges legitimate nodes as malevolent. Zheng *et al.* [9] proposed a network security mechanism based on trust management to deal with the threats faced by WSNs (DNSMTM). This mechanism is designed to rapidly and effectively detect un-trusted nodes in the network and ensure the dependable functioning of the network (DNSMTM). This mechanism derives the comprehensive trust degree of nodes, which can reflect the trust degree of nodes based on the trusted access of nodes. It detects malicious nodes per the comprehensive trust degree of nodes. It first calculates the local trust degree of nodes based on the interaction behaviour of the currently used nodes. The technique has a greater detection rate for rogue nodes and can efficiently stop them from using as much energy. [10] Suggested a hybrid monitoring-forwarding game detection technique to identify targeted forwarding assaults (MSGSFS). This system builds a set of techniques by including elements like packet loss, data corruption, and forwarding delay. To play the monitoring-forwarding game and gather the routing trust value of the suspicious node, the data transmitting node and its one-hop neighbour nodes choose strategies from a set. Zhou *et al.* [11] presented an enhanced trust evaluation model (ITEMBB). In this paradigm, the node's direct trust value is computed first. If the direct trust value is deemed insufficiently dependable, the indirect trust value of the node is determined. A complete trust value is created by combining the direct and indirect trust values, and entropy is employed to give highly trusted nodes more weight. The methodology somewhat gets over the drawbacks of subjective weighting, but it still can't deal with the issue of enduring reputation value. A cluster-based selective forwarding attack detection system was proposed by Zhou et al. [12] by combining the neighbour node monitoring and watchdog mechanism (SMCSF). This scheme divides the cluster nodes into cluster head nodes, monitoring nodes, and cluster member nodes. By choosing the monitoring node in the cluster, the monitoring node performs the calculation and adjustment of the overall reputation of the cluster head nodes and cluster member nodes. And in this scheme, the monitoring nodes are in charge of not only determining and adjusting a node's reputation as well as judging and spotting malicious nodes in the cluster but also keeping an eye out for any malicious behaviours on the part of the cluster head node, such as data tampering or packet loss during the data forwarding process. Even though this method may rapidly and precisely identify rogue nodes, it is too difficult to maintain track of all the nodes. Sheetal *et al.* [13] introduce a blockchain trust model (BTM) for malicious node detection in wireless sensor networks to address the issue that the fairness and traceability of the detection process cannot guarantee the current malicious node detection methods in wireless sensor networks. In BTM, it is realized through 3D space, blockchain intelligent contracts, and WSN quadrilateral measurement for the localization of the identification of rogue nodes. The consensus voting results are also recorded in the blockchain's distributed ledger. The model can successfully identify malicious nodes in WSNs and ensure that the discovery process can be tracked back. Although the model's consensus approach is the conventional POW workload-proof method, which demands a lot of energy and computer resources, it is not well suited for the operating environment of wireless sensor networks. Li *et al.* [14] suggested a distributed and randomized detection technique (IPAs). Each node in this system keeps a list of questionable nodes. All node neighbours are first put on a list of suspicious nodes; if the packets sent by its neighbours are invalid, the neighbour nodes that transmit valid packets are subsequently removed from the list of suspicious nodes. The nodes in the group of suspicious nodes are bad neighbours after n detection rounds. The system can detect rogue nodes in the network, but it requires n rounds, making network communication considerably more difficult. In conclusion, each type of current research strategy has unique characteristics. Comparing comparable tasks is examined by comparing each plan's benefits and drawbacks. High communication overhead will result from the multi-hop acknowledgement-based detection techniques [4–6] having to send many acknowledgement packets. The number of monitoring nodes required by the detection systems [7–12] based on trust evaluation substantially increases network overhead. Furthermore, the present methods for finding malicious nodes generally concentrate on finding them along a single path. No monitoring nodes or intricate assessment models are required for the HFDLMN technique described in this book to determine a node's trust value. Malicious nodes can also be found and located in many other methods.

III. PROBLEM FORMULATION

The wireless sensor network is a collection of sensor nodes with low processing, memory, and energy capacity to take special-purpose data from the atmosphere and send it to the Base Station using direct or indirect (with the help of other sensor nodes). Due to the device's limited capacity, it's incapable of processing itself. They want to transfer data to Base Station (BS) for further processing. The route between the sensor's node to the base station forms through a direct range of BS or a movable sensor treated as a router capable of making routing decisions. Due to the sensor network's nature and low capability, missing activity is more vulnerable. This paper aims to develop a security system to protect the sensor network from rushing or denial of service (DoS) attacks using a packet filtering mechanism.

IV.CONCLUSION

Intrusion detection is a crucial issue due to the nature of wireless sensor nodes. This paper first discusses the security issues in WSN, then various challenges associated with an intrusion detection system and the existing methods to detect the malicious node in the wireless sensor network. WSNs can set up networks in harsh environments where it may not be possible to deploy a traditional network infrastructure in areas humans cannot reach. Whether WSN has vast potential, there are many challenges left to overcome. Security is an important feature for the deployment of WSNs. Security is such an important feature that it could determine the success and wide deployment of WSNs. Malicious nodes either drop valuable data packets or inject useless packets into the network. A malicious node attack is a type of attack that performs malicious activity by flooding unwanted or useless packets into a network. The proposed Malicious Detection and Prevention scheme with AODV is applied to detect malicious attackers by packet filtering in a network. MDP-AODV aims to detect malicious nodes by the packets they flood the network. The packets sent by the attacker are completely different because they contain no message to misbehaving links to prevent them from communicating networks. This MDP-AODV protects against malicious node attacks and blocks the activities of attacker nodes.

In the case of an attack, almost all the network performance is completely down, but the proposed scheme improves performance to nearly equal normal routing. The routeing overhead is less than one as compared to MAODV. Security is becoming a major concern for energy-constrained wireless sensor networks because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted much attention in recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. This paper introduces sensor networks and their related security problems, threats, risks and characteristics. Network security for WSNs is still a fruitful research direction to explore further.

Reference

[1] Dr K. Sasi Kala Rani, Ms R. Vijayalakshmi "Experimental Evaluations of Malicious Node Detection on Wireless Sensor Network Environment" IEEE Xplore (ICICCS 2021).

[2] Christian Miranda, Georges Kaddoum, Elias Bou-Harb, Sahil Garg and Kuljeet Kaur, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, 2020.

[3] Muhammad Nawaz Khan, Haseeb Ur Rahman, Mohammed Amin Almaiah, Muhammad Zahid Khan and Ajab Khan, "Improving Energy Efficiency with Content - Based Adaptive and Dynamic Scheduling in Wireless Sensor Networks", IEEE Access, 2020.

[4] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," in Proceedings of the Wireless Communications & Networking Conference, pp. 2137–2142, IEEE, New Orleans, LA, USA, April 2005.

[5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: i," Journal of Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218–1230, 2007.

[6] A. Liu, M. Dong, K. Ota, and J. Long, "PHACK: an efficient scheme for selective forwarding attack detection in WSNs," Sensors, vol. 15, no. 12, pp. 30942–30963, 2015.

[7] H. Yang, X. Zhang, and F. Cheng, "A novel algorithm for improving malicious node detection effect in wireless sensor networks," Mobile Networks and Applications, vol. 2020, Article ID s11036-019-01492-4, 2020.

[8] D. Xiao, J. Feng, and Q. Zhou, "Gauss reputation framework for sensor networks," Journal on Communications, vol. 29, no. 3, pp. 47–53, 2008.

[9] G. Zheng, B. Gong, and Y. Zhang, "Dynamic network security mechanism based on trust management in wireless sensor networks," Wireless Communications and Mobile Computing, vol. 2021, Article ID 6667100, 10 pages, 2021.

[10] H. Liao and S. Ding, "Mixed and continuous strategy monitor-forward game based selective forwarding solution in WSN," International Journal of Distributed Sensor Networks, vol. 2015, no. 11, Article ID 359780, 13 pages, 2015.

[11] Z. Zhou and N. Shao, "An improved trust evaluation model based on Bayesian for WSNs," Chinese Journal of Sensors and Actuators, vol. 29, no. 6, pp. 927–933, 2016.

[12] H. Zhou, Y. Wu, L. Feng, and D. Liu, "A security mechanism for cluster-based WSN against selective forwarding," Sensors, vol. 16, no. 9, pp. 1537–1552, 2016.

[13] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," IEEE Access, vol. 7, pp. 38947–38956, 2019.

[14] Y. Li and J. C. S. Lui, "Identifying pollution attackers in network-coding enabled wireless mesh networks," in Proceedings of the 2011 20th International Conference on Computer Communications and Networks (ICCCN), pp. 1–6, Maui, HI, USA, August 2011.

[15] Douceur, "The Sybil attack", In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), February 2002

[16] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, "Search-based physical attacks in sensor networks: Modelling and defence, technical report, Department of Computer Science and Engineering, Ohio State University, February 2005

[17] H. Chan and A. Perrig, "Security and privacy in sensor networks", IEEE Computer Magazine, pp. 103-105, 2003

[18] Abror Abduvaliyev, Al-Sakib Khan Pathan, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks" in IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013.