Malicious Attack Detection and Prevention using Packet Filtration in Wireless Sensor Networks

Pushpendra Dwivedi, C. S. Raghuvanshi, Hari Om Sharan
Faculty of Engineering & Technology, Rama University, Uttar Pradesh, Kanpur, U.P, India

Corresponding Author: Email Id: drcsraghuvanshi@gmail.com

Abstract: **The usage of mobile devices and sensors-based Internet of Things communication technology is growing quickly nowadays; wireless communication is a key area of current study. Numerous application fields, including military surveillance, weather report forecasting, soil testing, crop forecasting, emergency medical treatment, etc., benefit from sensor communication. Lightweight nodes that make up wireless sensor networks receive environmental data such as air pressure, wetness, force, friction, location, sound, etc. and send that information to the base station (BS) for a specialized analysis. Because there is no one in charge of monitoring and controlling the whole sensor field, sensor nodes' limited power and processing capacity makes them more susceptible to network security breaches during communication. Numerous researchers have attempted to address the issue of sensor network security in the past using a variety of strategies, but the subject remains open since new attacks and other irregularities are discovered on a daily basis. We design a system to identify and prohibit wireless sensor networks using packet filtering approach to solve the security issue. To that end, the following objectives are defined to meet security requirements.**

Keywords: ***Wireless sensor network, Malicious attack, packet filtering, AODV***

I.INTRODUCTION

Due in large part to the growing usage of Micro-Electro-Mechanical Systems (MEMS) technology, which has made it easier to create smart sensors, interest in wireless sensor networks (WSNs) has increased recently. Although these sensors are less expensive, they are also smaller and have less processing and computing capability than conventional sensors. Depending on a local decision-making process, these sensor nodes may convey that data to the user after being able to detect, measure, and gather data from their surroundings. Smart sensor nodes are low-power devices that include one or more sensors, a radio, a power supply, a CPU, memory, and an actuator [1]. There are two types of WSNs: organized and unstructured. An unstructured WSN is made up of a substantial collection of sensor nodes. In the field, sensor nodes may be quickly installed. To perform monitoring and reporting duties, the network is deployed and then left unattended. An unstructured WSN has a large number of nodes, making connection management and problem detection difficult.

When it comes to sensor nodes, accumulator or cell are the most important source of power, yet they are a limited resource [2]. During the transmission of data packets, the sensor nodes use up the majority of their energy. As soon as a sensor node's battery is depleted, it ceases to function and ceases to cover the region on which it was installed. WBANs must thus prioritize energy saving above anything else [3].Numerous small sensor nodes in the WSN network capture data from the atmosphere and send it to the base station. The semi-ad hoc aspect of WSN communication implies that certain sensor nodes are viewed as routers and are dynamically mobile, enabling interlink between source sensors and destination Base Stations (BS) utilizing ad hoc routing techniques [4]. Trust [5], adaptability and scalability are the main concern in the WSN security. There has been an exponent evolution in the malwares that has become a major challenge [6].These distributed denial of service attacks is currently the Internet's most pressing security risk. Multiple safeguards have been set up to prevent denial-of-service (DDOS) attempts on the network [7]. A complete security assurance for WSN cannot be provided by passive protection methods. It is essential to develop preventative defensive technologies [8]. Durante et. al. [9] suggested overload scenarios, such as transient traffic surges or DoS assaults ad proposed a methodology for redistributing the filtering rules amongst cascaded firewalls in order to decrease the packet processing cost and prevent performance loss.

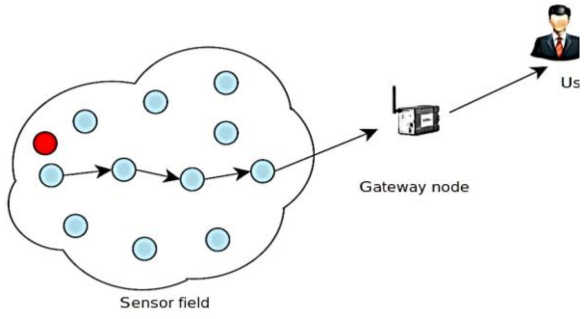

Figure 1: Structure of WSN

Due to the device's low processing power, data must be sent to the base station (BS) for additional processing [10]. The path from the sensor node to the base station can either be taken directly through the BS or by employing a mobile sensor that can act as a router and make routing decisions [11].

In this paper the scheme is proposed to design a security system to guard the sensor network against rushing or denial of service (DoS) attack using packet filtering mechanism because of the nature of sensor networks and their poor capability, which makes them more vulnerable to mis-activity.

II.PRIVIOUS WORK AND MOTIVATION

Numerous effective detection techniques for wireless sensor networks rogue nodes have been developed thanks to extensive research efforts. Plans may be broken down into three distinct groups: those that rely on multi-hop acknowledgments, those that rely on trust evaluations, and those that rely on statistical classifications. Manjuprasad et. al. [12] proposed for WSNs that are short on resources, the CIAWSNs prioritized offering a low-complexity security mechanism. Rules for the firewall are checked by the node with the most powerful packet filtering capabilities. Yang et. al. [13] introduced MNDREL, a malicious node detection model based on reputation and energy-efficient clustering. Nodes construct clusters by picking the appropriate cluster head depending on the improved routing protocol. Analyzing the parent node's reputation as evaluated by the child node reveals the network's harmful nodes. MNDREL outperformed other WSN malware detection algorithms by reducing false alarms. Real-time performance of MNDREL needs improvement.

She et. al. [14] offer a blockchain trust model (BTM) for malicious node detection in wireless sensor networks to ensure fairness and traceability of the detection process. In BTM, rogue nodes are localized using 3D space, blockchain smart contracts, and WSN quadrilateral measurement. The blockchain's distributed ledger records consensus voting outcomes. The model can identify malicious WSN nodes and trace their discovery. The model's consensus methodology is the typical POW workload proof method, however it's not well-suited for wireless sensor networks.

The research conducted by Ali et al. [15] revealed that AODV is a more dependable protocol than DSR in terms of delay and throughput, and that size of the network has no impact on AODV performance relative to delay. Srivastava et. al. [16]demonstrates the significance of the SEIQR model and the relationship between quarantine and recovery and the malicious nodes under various conditions, demonstrating that when the rate of recovery rises, the number of infected nodes decreases. The SLGBM suggested by Jiang et al [17]., an intrusion detection approach for wireless sensor networks, has a low false alarm rate, a little amount of computing effort, and a high detection rate. The detection rate is high, the computation time is short, and the false alarm rate is low with this technique. Fang et. al. [18] proposed a trust management schemes for protection in WSN. It is used to counter internal attacks, with various systems targeting various attacks by various applications. Nancy et. al. [19] implemented the principles acquired from deep learning algorithms, a novel intrusion detection system (IDS) is provided for more accurate detection of intruders, such as denial-of-service (DoS) assaults, user-to-user (U2U) attacks, probe (probing), and remote-to-local (R2L) attacks. Sahu et. al. Pat[20] proposed PPFS mechanism counteract attackers' efforts to saturate a WSN with packets for a DoS attack

III.PROPOSED PACKET FILTERING MDP-AODV SCHEME

During the transmission phase, several security concerns are considered. These include errant routing (blackholes and grayholes), undesired floods, DoS attacks, packet insertion, and so on. The author proposes several safety measures, some of which are based on indicators of inappropriate behavior [21]. In this study, we advocate for a packet filtering method for detecting and preventing malicious behavior in wireless sensor networks (MDP-AODV).

Table 1: Simulation Parameter for Deployment of WSN

Parameters	**Configuration Value**
Simulation Tool	NS-2.31
Routing Protocol	MAODV, MDP-AODV
Simulation Area	1000m*1000m
Network Type	WSN
Number of Nodes	100
Number of Base Station	4
Physical Medium	Wireless, 802.11
Simulation Time (Sec)	550Sec
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground
Energy (Initial)/J	Random

The planned MDP-AODV runs from the time the routes are established until after the data has been sent. While waiting for data to be sent, the source sensor node runs the network-wide MDP-AODV routing protocol to find the receiver, in this case the base station (BS). The suggested MDP-AODV based security system works constantly to keep an eye out for and shut down any potential threats to the network, while still keeping the lines of communication open and secure for legitimate users.

A. Proposed Architecture

The MDP-AODV module helps the base station make decisions concerning malicious behavior and node blocking by determining whether or not a packet is genuine and by determining the route's expiration time.

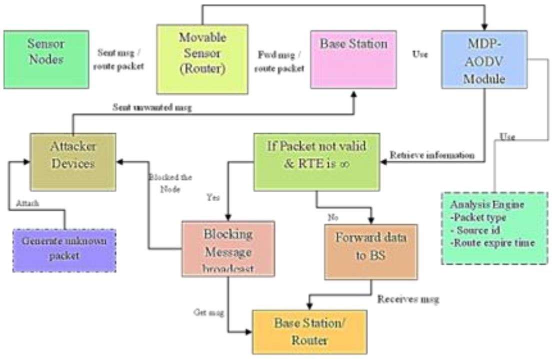

Figure 2: Malicious Detection/ Prevention AODV Security Block Architecture

B. Proposed Algorithm

Route Discovery Phase

```
Deploy $N_t$ in $\Psi$
$W_n$ want sent data to BS
$W_n$ generate $R_{req}(W_n$, BS, MDP-AODV)
If $W_n$ within $\Psi$ of BS then
    $W_n$ sent data to BS
    BS processes it and analyze
Else if $W_n$ not $\Psi$ of BS || $\Psi$ of $M_w$ then
    Sent $R_{req}$ to $M_w$
    $M_w$ receive $R_{req}$
    Check by $M_w$ next_hop is BS or not
        If next_hop == BS then
            Forward $R_{req}$ to BS
            BS receive $R_{req}$
            Sent ack to Sender $W_n$ by reverse path
            $W_n$ Call Data_Sent($W_{n,}$ BS, tcp/udp)
        Else if next_hop != BS && next_hop == $M_w$
        Then
            If $M_w$ is not visit then
                Goto Step 5
            Else
                BS not found
                Exit
            End if
Else
    BS not found
    Exit

End if
```

MDP-AODV Detection and Prevention Module

```
Mw || BS use MDP-AODV protocol for Attack Detection
While Mw || BS watch activity of Wn
Random Sample data take (Ptype, Source_id, RTE)
    If Ptype != tcp/udp & RTE == $\infty$ then
        Get Wn source_id
        Set node as Ad:
        Block Ad node
        Use MDP-AODV & Broadcast blocking message of Ad in Nt
        Wn receive information and block communication with Ad
    Else
        Wn treated as normal node
    End if
Analyze network performance
```

The table 1 simulation parameters are used to model common malicious attacks, MAODV, and MDAP-AODV methods. The dynamic topology is used to determine the values for these simulation parameters. When regular routing is being performed, all 100 nodes are taken into account, but when a malicious situation is being evaluated, only some of the nodes are attackers and the rest are normal nodes. Use packet filtering on every node in an MDAP-AODV network to identify and stop intrusion attempts.

IV. Simulation Result Analysis

A. PDR Analysis

Here, we see how the Packet Delivery Ratio (PDR) changes under typical AODV routing, wormhole assault, and the Multi-Domain Pseudo-AODV (MDP-AODV) protocol. In this situation, the performance of the network is compared to how it would have performed without the protection strategy solely. Here, the impact of malicious assaults on the network is graphically represented by measuring just roughly 71% of packet delivery. When an attacker is present, the packet-receiving rate drops below the level expected by the security system. When the MDP-AODV system is used, MAODV gains an additional 4 percentage points in PDR performance. After implementing a protection plan, the PDR increases in quality.

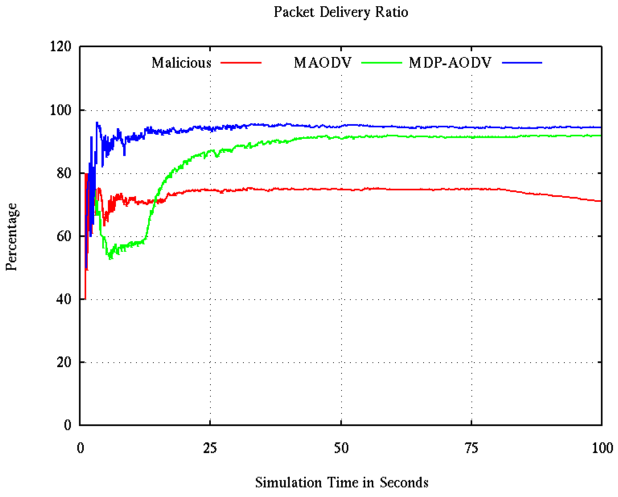

Figure.2 PDR Analysis

B. NRL Analysis

To calculate how many routing packets were sent and received across a given network, a routing load study must be performed. Essential information about the recipient may be found in the routing packets. This graph shows that MDP-AODV has the least routing burden or the most authentic number of routing packets. Overhead 71 has been compromised by hostile actors as a result of their sending of many bogus and worthless packets. In the case of an attack, normal routing's performance is measured by the least value of routing packets, which indicates the best overall network performance. When compared to conventional and MDP routing, the actual data packets transported in the network are vanishingly small when using minimal routing packets. The routing packets in MDP are less densely packed, making for a safer channel of communication.

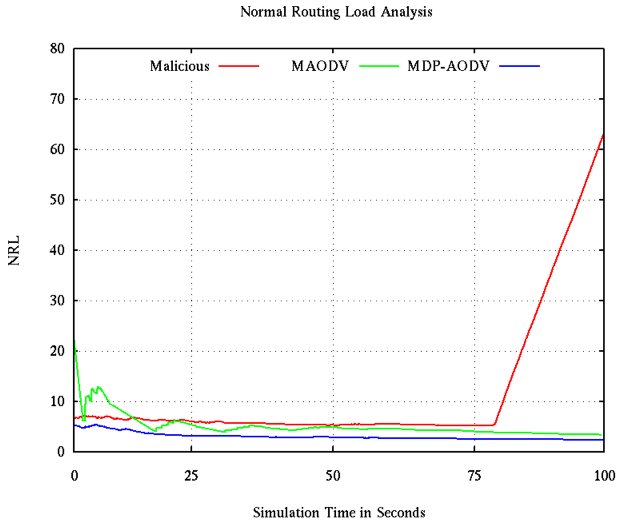

Figure.3 NRL Analysis

C. Throughput Analysis

How many bytes are received at the receiver per second is a measure of throughput. During an assault, the network's performance drops because of the overwhelming number of routing packets. Throughput analysis under assault, comparing the existing MAODV with the proposed MDP-AODV, is shown in the graph below. MDP-AODV has higher performance than the other methods when evaluated in Kbps of throughput. Heavy routing packet flooding in the network causes throughput drops during an assault. It can be measured all the way to the simulation's conclusion. Nonetheless, the MDP-AODV method improves throughput compared to the prior design.

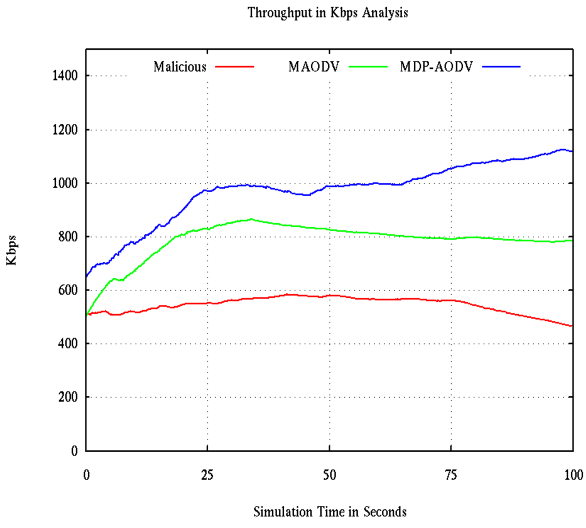

Figure. 4 Throughput Analysis

D. Packets Receiving Analysis

This graph shows the analysis of malicious attack packets received, as well as the suggested MDP-AODV and MAODV. Due to severe flooding, an attacker's presence in the network immediately influences the packets that are received. Here, the malicious attack and MDAODV get less packets, around 4600 and 5018, but the suggested MDP-AODV receives 6050 packets at the destination. Good packet reception is necessary for a network to operate more effectively. The more packets that are received, the better the routing performance. The suggested plan stops all malicious attack activities and cleans the network of the virus.

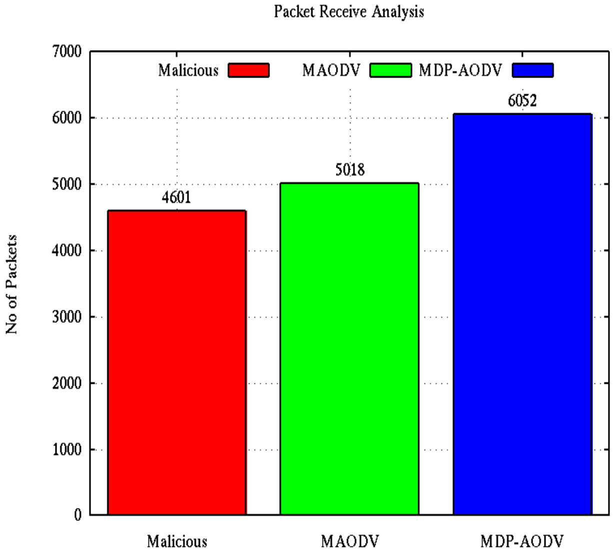

Figure.5 Packets Receiving Analysis

E. Delay Analysis

Senders send a certain number of packets to the destination, some of which are discarded by the network for unknown reasons. The percentage of packets that were received on time, signifying no data delay, however packets may reach at their destination late because of an attacker or other circumstances. Although the majority of senders send data on schedule, it takes longer for the data to reach its destination owing to network delays. Malicious nodes have the longest delays. The earlier MAODV system minimises time and offers protection from nefarious intruders. Due to packet filtering and superior route selection in WSN, the performance of the proposed MDP-AODV is proven to have reduced latency. If the delay is significant, there may be an issue with the formation of strong links. When compared to the MAODV method, the suggested technique is faster by 0.5 milliseconds.

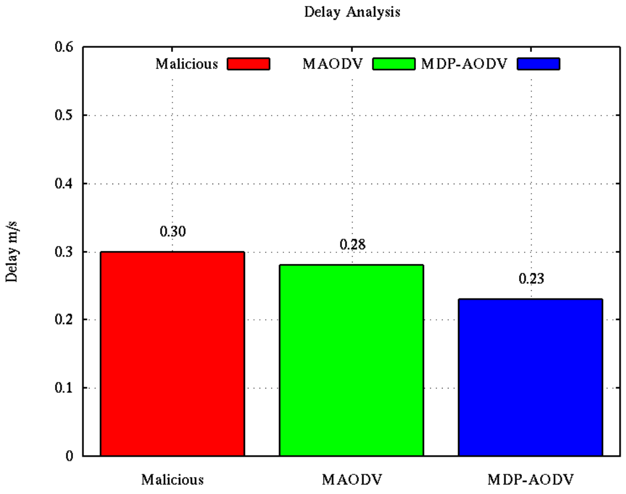

Figure.6 Delay Analysis

F. Summarized Performance Analysis

Table 2 displays the network's overall performance. This table shows the complete breakdown of performance metrics in precise numbers, including the number of packets transmitted, received, and dropped in the network under assault, before MAODV, and MDP-AODV. In the presence of an attacker, the protection plan allows for normal conduct.

Table 2: Performance Analysis

	Malicious	M-AODV	MDP-AODV
Send	5174	5473	6409
Receive	4601	5018	6052
Drop	573	455	357
PDR	71.14	91.69	94.43
NRL	63.35	3.33	2.48
Delay [ms]	0.30	0.28	0.23

V. Conclusion and Future Work

In difficult circumstances when conventional network infrastructure is impractical and in places that people cannot reach, WSN can establish networks. Despite WSN's guarantee, there are still a number of issues. Security for WSNs is critical. The installation and effectiveness of WSNs may depend on security. Data packets are discarded or injected by malicious nodes. Networks are overrun by unwanted or useless data as a result of malicious node assaults. MDP-AODV employs packet filtering to find malicious network attackers. Malicious nodes are discovered by MDP-AODV using the packets they send. Packets from the attacker contain no message. Communication networks are impeded by poor connectivity. This MDP-AODV stops malicious node attacks and disables attacker nodes. Nearly all network performance is lost during an attack, but the recommended method restores it to levels consistent with regular routing. The route overhead is lower for MAODV. The other metrics are also better, and the PDR is 4% better than the previous MAODV scheme. This study explores a fundamental and reliable idea that may be applied and tested in the future with more network nodes. With our network-layer security solution, routing and forwarding operations are protected.

In the future, we'll examine the tactics used by additional assaults, such as vampire and remapping attacks, and work to develop defenses against them. We will also work to improve the routing capabilities of the routing protocols discussed in this dissertation.

VI. References

[1] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020, doi: 10.1109/ACCESS.2019.2962829.

[2] A. Sapio and G. R. Tsouri, "Low-power body sensor network for wireless ECG based on relaying of creeping waves at 2.4GHz1," in *2010 International Conference on Body Sensor Networks, BSN 2010*, 2010, pp. 167–173. doi: 10.1109/BSN.2010.18.

[3] A. K. Sagar, S. Singh, and A. Kumar, "Energy-Aware WBAN for Health Monitoring Using Critical Data Routing (CDR)," *Wirel Pers Commun*, vol. 112, no. 1, pp. 273–302, May 2020, doi: 10.1007/s11277-020-07026-6.

[4] J. Su, A. X. Liu, Z. Sheng, and Y. Chen, "A partitioning approach to RFID identification," *IEEE/ACM Transactions on Networking*, vol. 28, no. 5, pp. 2160–2173, 2020, doi: 10.1109/TNET.2020.3004852.

[5] F. Ishmanov and Y. bin Zikria, "Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues," *J Sens*, vol. 2017, 2017, doi: 10.1155/2017/4724852.

[6] P. Dwivedi and H. Sharan, "Analysis and Detection of Evolutionary Malware: A Review," *Int J Comput Appl*, vol. 174, no. 20, pp. 42–45, 2021, doi: 10.5120/ijca2021921005.

[7] J. Mirkovic and P. Reiher, "td lkj;bb.kccdDoS Defense Mechanisms *," vol. 34, no. 2, pp. 39–54, 2004, [Online]. Available: http://delivery.acm.org/10.1145/1000000/997156/p39-mirkovic.pdf?ip=150.183.226.91&id=997156&acc=ACTIVE%0ASERVICE&key=336BF258277217C3.336BF258277217C3.4D4702B0C3E38B35.4D4702B0C3E38B35&__acm__=1519027992_7bc0bb359ba5bc79f940b61d45f461bc

[8] T. A. Ahanger and A. Aljumah, "Detection and Defense against Distributed Denial of Service Attack Using Packet Filtration in Wireless Sensor Networks," *International Journal of Computer Networks and Communications Security*, vol. 5, no. 12, pp. 277–284, 2017, [Online]. Available: http://search.proquest.com/openview/a7dd5991e8e9832ef69641e2eb482d34/1?pq-origsite=gscholar&cbl=2044553

[9] L. Durante, L. Seno, and A. Valenzano, "A formal model and technique to redistribute the packet filtering load in multiple firewall networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2637–2651, 2021, doi: 10.1109/TIFS.2021.3057552.

[10] S. G. Fatima, S. K. Fatima, and S. MohdAli, "A security protocol for wireless sensor networks," *International Journal of Advanced Research in Engineering and Technology*, vol. 10, no. 2, pp. 155–174, 2019, doi: 10.34218/IJARET.10.2.2019.017.

[11] H. Alrahhal, R. Jamous, R. Ramadan, A. M. Alayba, and K. Yadav, "Utilising Acknowledge for the Trust in Wireless Sensor Networks," *Applied Sciences (Switzerland)*, vol. 12, no. 4, 2022, doi: 10.3390/app12042045.

[12] B. Manjuprasad, A. Dharani, and S. Nayak, "Energy Efficient Secure Firewall and Packet Filtering System in Wireless Sensor Networks," no. January, 2014, doi: 10.12691/ajst-2-1-1.

[13] H. Yang, X. Zhang, and F. Cheng, *A Novel Wireless Sensor Networks Malicious Node Detection Method*, vol. 284. Springer International Publishing, 2019. doi: 10.1007/978-3-030-21373-2_59.

[14] W. She, Q. Liu, Z. Tian, J. sen 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, doi: 10.1109/ACCESS.2019.2902811.

[15] A. Ali and Z. Akbar, "Evaluation of AODV and DSR routing protocols of wireless sensor networks for monitoring applications," *Blekinge Institute of technology, …*, no. October, pp. 1–47, 2009, [Online]. Available: http://digitalamedier.bth.se/fou/cuppsats.nsf/all/cf795b6489e5bc9ec12576a500363a0e/$file/Thesis documentation.pdf

[16] P. K. Srivastava, R. P. Ojha, K. Sharma, S. Awasthi, and G. Sanyal, "Effect of Quarantine and Recovery on Infectious Nodes in Wireless Sensor Network," *International Journal of Sensors, Wireless Communications and Control*, vol. 8, no. 1, pp. 26–36, 2018, doi: 10.2174/2210327908666180413154130.

[17] S. Jiang, J. Zhao, and X. Xu, "SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments," *IEEE*

Access, vol. 8, pp. 169548–169558, 2020, doi: 10.1109/ACCESS.2020.3024219.

[18] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey," *Wirel Commun Mob Comput*, vol. 2020, 2020, doi: 10.1155/2020/2643546.

[19] P. Nancy, S. Muthurajkumar, S. Ganapathy, S. V. N. Santhosh Kumar, M. Selvi, and K. Arputharaj, "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks," *IET Communications*, vol. 14, no. 5, pp. 888–895, 2020, doi: 10.1049/iet-com.2019.0172.

[20] S. Patnaik, "Preface," *Advances in Intelligent Systems and Computing*, vol. 309 AISC, no. VOLUME 2, pp. 65–70, 2015, doi: 10.1007/978-81-322-2009-1.

[21] I. Butun and R. Sankar, "Prevention and Detection of Intrusions in Wireless Sensor Networks," vol. 3558411, no. January, p. 184, 2013, [Online]. Available: https://login.ctu.idm/oclc.org/?url=http://search.proquest.com/docview/1350633998?accountid=26967