Efficient Anomaly Detection Technique for Future IoT Applications

Ahmad Naseem Alvi[1], Muhammad Awais Javed[2], Bakhtiar Ali[3], Mohammed Alkhathami[4]*
Department of Electrical and Computer Engineering, COMSATS University Islamabad, 45550, Islamabad, Pakistan[1,2,3]
Information Systems Department-College of Computer and Information Sciences,
Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia[4]

***Abstract*—Internet of Things (IoT) provides smart wireless connectivity and is the basis of many future applications. IoT nodes are equipped with sensors that obtain application-related data and transmit to the servers using IEEE 802.15.4-based wireless communications, thus forming a low-rate wireless personal area network. Security is a major challenge in IoT networks as malicious users can capture the network and waste the available bandwidth reserved for legitimate users, thus significantly reducing the Quality of Service (QoS) in terms of transmitted data and transmission delay. In this work, an Anomaly Detection Mechanism for IEEE 802.15.4 standard ($ADM_{15.4}$) to improve the QoS of the IoT Nodes is proposed. $ADM_{15.4}$ also proposes a mechanism to block the malicious nodes without affecting the overall performance of the medium. The performance of $ADM_{15.4}$ is compared with the standard when there is no such anomaly detection is present. The results are obtained for different values of SO and for different sets of GTS requesting nodes and are compared with the standard in the presence and absence of malicious nodes. The simulation results show that the $ADM_{15.4}$ improves data transmission up to 19.5% from IEEE 802.15.4 standard without attacks and up to 52% when there is malicious attacks. Furthermore, $ADM_{15.4}$ transmits data 33% reduced time and accommodate 56% more GTS requesting legitimate nodes as compared to the standard in the presence of the malicious attacks.**

***Keywords*—Anomaly detection; IoT networks; security**

I. Introduction

Internet of Things (IoT) has been emerging rapidly since last decade and is being used in several applications to improve the quality of life of citizens with improved healthcare systems, automated industrial applications, smart cities, and home appliances [1]. In the current era, there are multiple gadgets have been developed to provide ease in human daily life activities by using IoT platforms. Predictions from experts suggest that there will be a substantial global business impact, reaching 15 trillion, by the year 2025, driven by the proliferation of 120 billion networked gadgets [2].

IoT is mainly based on wireless sensor networks, where multiple wireless devices are connected in a network to form a wireless Personal Area Network (WPAN). Over the last decade, there has been a significant rise in the demand for Low-Rate Wireless Personal Area Network (WPAN) applications. These applications cater to various short-range communication needs, and as a result, a host of technologies have been developed, including ZigBee, Bluetooth, INSTEON, and more. WPANs are primarily designed for short-distance communication and serve a wide spectrum of applications, ranging from home automation, cattle farming, precision agriculture, healthcare, monitoring liquid flow in pipelines, to even military use cases [3], [4], [5].

This ubiquitous growth of IoT applications with diverse and heterogeneous communication technologies such as 5G, and 6G, makes it more vulnerable and prone to attacks [6], [7], [8]. This may attract malicious nodes to attack the communication channel and create anomalies in the communication channel. IoT operates across diverse networks that incorporate both large and small devices. Small IoT devices, characterized by limited computational power and storage capacity, pose challenges for implementing robust security measures, including cryptographic algorithms and protection mechanisms. Due to the absence of privacy-preserving algorithms on these small IoT devices, malicious actors exploit their vulnerabilities, turning them into unwitting agents for conducting various attacks [9], [10], [11].

WSNs consist of tiny wireless nodes with limited energy and processing capabilities. WSNs demand timely data transmission with minimal delays and also strive to maximize throughput and link utilization for improved efficiency. To increase the efficiency of WSN-based IoT, the chances of collisions need to be avoided as it results node sending the data again resulting in energy consumption, with increased delay and poor bandwidth utilization.

To address these requirements, various Medium Access Control (MAC) protocols have been created. In 2003, the Institute of Electrical and Electronics Engineers (IEEE) introduced the 802.15.4 standard, designed specifically for applications in low-data-rate and low-power Wireless Personal Area Networks (WPAN). This standard boasts an exceptionally low duty cycle, even less than 0.1%, making it an ideal choice to address the distinctive requirements of such applications. The standard is specifically designed for low-rate and low-power devices such as IoT devices and remains in high research [12], [13], [14].

IEEE 802.15.4 standard operates in beacon-enabled and non-beacon-enabled modes. In beacon-enabled mode, it offers a superframe structure having both contention-based and contention-free communication modes. During the contention access period, nodes contend with other nodes to access the medium and there are chances of collision in the period. However, in the contention-free period, TDMA-like time slots are present and data-sending nodes are allocated dedicated time slots to transfer their data in the medium without contending

*Corresponding authors.

with other nodes and by avoiding chances of collisions.

Malicious nodes present in the network try to disturb the communication channel. Malicious node attacks during the contention-free period are easily detected as TDMA-like contention-free slots are reserved for specific nodes and only the allocated nodes are allowed to send their data during these slots. That's why, malicious nodes attack in the contention-based environment, where chances of collisions are always present and it is difficult to detect the malicious attacks in that environment. To avoid these malicious attacks, the communication of the specific area is required to be restricted to avoid the interference of these malicious nodes during the contention access period. However, restricting the communication of the region restricts the communication of the legitimate nodes present in that restricted region resulting in a compromised Quality of Service (QoS)of the network.

In this study, we present a novel Anomaly Detection Mechanism, denoted as $ADM_{15.4}$, tailored for the IEEE 802.15.4 standard. The main aim is to recognize the existence of malicious nodes within the network and formulate a strategy to prevent their attacks without compromising the QoS of the network. The salient features of the proposed $ADM_{15.4}$ scheme are mentioned below.

1) An anomaly detection algorithm by analyzing the network's performance parameters to detect the presence of malicious nodes.
2) Physical Layer Security-based (PLS) security mechanism to avoid the effects of these malicious nodes by generating jamming signals by the neighbouring nodes of the network.
3) A mechanism to allow the affected legitimate nodes in the restricted region to transfer their data by assigning GTS.
4) An efficient mechanism by allocating Guaranteed Time Slots (GTS) to all GTS requesting nodes along with the affected nodes to enhance the QoS of the network.

The rest of the manuscript is organised as: Previously discussed research work in the related field is discussed in Section II. A brief discussion about the working of IEEE 802.15.4 standard and possible attacks on it are discussed in Section III. The proposed anomaly detection mechanism along with its remedies are discussed in Section IV. The system model and performance analysis of the proposed scheme are described in Section V and VI, respectively and Section VII concludes this manuscript.

II. Related Work

The ubiquitous growth of IoT due to its provisioning of comfort in human life is developing rapidly. Due to its adoption in diverse applications, IoTs are under hot research areas in different areas. Secure and reliable communication by avoiding malicious nodes' attacks is one of the dire requirements of IoT networks. That is why, it is under high research area and a lot of research on malicious attacks is taking place in different areas of the communication field.

In [15], the authors propose a novel anomaly detection technique for IoT networks. In this work, the authors use an imbalance data technique, that is when normal data is more than the malicious data and vice versa by applying reinforcement learning on the data set of Network Security Laboratory-Knowledge Discovery and Data Mining Tools Competition (NSL-KDD). In this technique, the input data is classified into normal and malicious data by considering the state as a category of the data due to the varying types of data present in the IoT network. The anomaly detection accuracy level is the reward of the function described in this work. The authors claim that their proposed scheme provides better accuracy, recall, and F1 score.

The authors in [16] proposed a cyber-attack detection mechanism in Industrial IoT (IIoT) by applying a federated learning-based approach. The main purpose of using the federated learning approach is its privacy because data can only be accessed locally. The authors applied the technique to local anomaly detection centres and claimed to achieve better accuracy and throughput as compared to the related techniques on global anomaly detection.

Authors in [17] proposed Software Defined Networks (SDN) that deal with traffic flow monitoring applications to regularly check the traffic flow monitoring. In this work, a tradeoff between accuracy and network load is observed, such that, a larger network load is required to achieve high accuracy and vice versa. In this work, authors proposed a deep Q-learning technique for anomaly detection that is due to the Denial of Services (DoS) attacks. The authors claimed that their proposed scheme performs better than other referenced techniques.

In [18], the authors explored a scenario within the Internet of Vehicles (IoV) context, where vehicles exchange information regarding the surrounding traffic conditions. Key parameters such as traffic density, emergency vehicle presence, and vehicle speeds are communicated to Road Side Units (RSUs) in the infrastructure. The study identifies a threat of malicious users executing data integrity attacks, manipulating information on traffic density and disseminating incorrect data. To address this challenge, the authors introduce a novel anomaly detection algorithm based on isolation forests. Verification of anomalies is conducted through probe messages sent to vehicles in the proximity of potential malicious users. Additionally, a communication mechanism is devised to share the verification information. The authors claimed to improve results in terms of accuracy, recall, and F1 score.

The study in [19] incorporates social networks as a significant aspect of its focus. The primary challenge tackled revolves around feature learning and the integration of information from the network's vicinity by proposing a Graph Neural Network (GNN) technique for feature learning. For effective training, the technique utilizes pattern mining algorithms. In addition, the authors also introduced a novel loss function. The results indicate improvements in metrics such as precision, recall, and F1 score when compared to other existing techniques.

The research presented in [20] focuses on enhancing the security of the Domain Name System (DNS). The fundamental approach involves making the system topology aware and taking into account the structural properties of the network. The proposed scheme is based on an exponential random graph model, and the network's topology is transformed into a graph

format. An additional layer of security is introduced through time series analysis, employing the auto-regressive moving average for anomaly detection. The authors claimed that the precision of their proposed scheme is better than the other alternative techniques.

In [21], the authors studied social welfare behaviour and presented a model for detecting behavioural differences in IoT-based networks. The model uses vector space-based aggregation and compares the behaviour of different nodes. The scheme is based on the correlation of primary attributes derived from social-aware interaction behaviour captured by edge nodes of the vector space. Additionally, the proposed model includes a spatial index tree to store the information of IoT nodes. The authors claim that their proposed scheme quickly and accurately detects abnormal behaviour in the network.

The authors in [22] proposed an anomaly detection mechanism along with energy efficiency in three-tier IoT–edge–cloud collaborative networks. The authors apply the marching square algorithm on data collected by the edge nodes to generate isopleths to detect anomalies at the boundary. The location of the anomaly is determined by adopting the Kriging spatial interpolation algorithm at the cloud tier and traversing at the edge network through mobile sensing nodes. Authors claimed that their proposed scheme provides better accuracy and energy consumption as compared to other state-of-the-art schemes.

In [23], the authors emphasized the importance of real-time data accuracy in Industrial IoT applications and proposed a hybrid end-to-end deep anomaly section framework. The authors proposed framework is based on the convolutional neural network (CNN) and a two-stage long short-term memory (LSTM)-based Autoencoder (AE) to detect anomalies by observing the variation from the actual sensor values. The authors claimed through extensive simulations that their proposed model works well in resource-constrained edge devices.

Most of the research work is based on the anomaly detection techniques that are created due to malicious attacks in the network layer and very rare research is on anomaly detection methods on the MAC layer. In this work, an anomaly detection method along with its countermeasures on IEEE 802.15.4 standard is being proposed (Table I).

III. Attacks on IEEE 802.15.4 Standard

In this section, the operating modes of the IEEE 802.15.4 standard along with the different types of vulnerabilities found in these operating modes are discussed.

A. Operating Modes of IEEE 802.15.4 Standard

The IEEE 802.15.4 standard is tailored for wireless networks that are operating with low transmission powers and modest data rates such as wireless sensors-based IoT networks. This standard operates in three different frequency bands, such as 868 MHz, 915 MHz, and 2.4 GHz offering 1 frequency channel, 10 frequency channels, and 16 frequency channels, respectively. At 868 and 915 MHz, a BPSK modulation scheme is employed with data rates of 20,000 and 40,000 bits per second, respectively. However, the 2.4 GHz band employs an O-QPSK modulation scheme, offering a data rate of 250,000 bits per second.

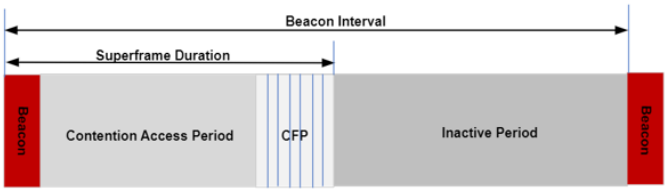


Fig. 1. A Superframe structure of IEEE 802.15.4 standard.

The standard accommodates both ad hoc and centrally controlled networks. In the ad hoc mode, nodes communicate with each other using an unslotted Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based multiple access algorithm. In the case of a centralized network configuration, a superframe architecture is implemented, as illustrated in Fig. 1. The coordinator initiates a beacon frame, prompting IoT nodes to activate their transceivers to receive the message and synchronize their operations. The active period, referred to as the Superframe Duration (SD), consists of 16 equally divided time slots and is further categorized into Contention Access Period (CAP) and Contention-Free Period (CFP). CAP involves the transmission of the beacon frame, control messages by member nodes, and data transmission. However, CFP comprised TDMA-like time slots and allocated to nodes on request for data transmission only. The duration between two consecutive beacon frames is known as the Beacon Interval (BI). SD and BI depends upon the parameter values of SO and BO respectively and are calculated in Eq. 1 and 2 [14].

$$SD = 960 \times 2^{SO} \tag{1}$$

$$BI = 960 \times 2^{BO} \tag{2}$$

here,

$$0 \leq SO \leq BO \leq 14$$

The PAN coordinator regularly generates beacon frames. Non-member nodes desiring to join the network must wait for the beacon to ascertain the CAP for transmitting their membership requests to the coordinator. If a node intends to transmit data during the CFP, it initiates CFP slot requests to the PAN coordinator and is then assigned a CFP slot in the subsequent SD. However, if a node's CFP request is not entertained, then it can transmit data during CAP. All IoT nodes follow the CSMA/CA algorithm to access the medium before transmitting their frames.

The CSMA/CA primarily comprises three parameters, such as the Number of Backoffs (NB), Backoff Exponent (BE) and Contention Window (CW). NB is about the number of tries to access the medium for transmitting a frame. Its initial value is 0 and ranges up to the value as defined in parameter $MaxCSMABackoffs$. The default value of $MaxCSMABackoffs$ is 4, which allows a node to make four attempts to access the medium availability before transmitting the frame. If it cannot access the medium then it declares the failed transmission with medium access busy

TABLE I. COMPARATIVE SUMMARY OF REFERENCED RESEARCH

Ref. No.	*Addressed Area*	*Proposed Scheme*	*Results*
[15]	Anomaly detection technique for IoT networks	Reinforcement learning on imbalanced data set with normal and malicious data classification	Better accuracy, recall, and F1 score
[16]	Cyber-attack detection mechanism in Industrial IoT	Federated learning-based approach to local anomaly detection centers	Better accuracy and throughput as compared to the related techniques
[17]	Traffic flow monitoring applications	Deep Q-learning technique for anomaly detection for DoS attack	Performs better during DOS attacks than other referenced techniques
[18]	Traffic density along with emergency traffic conditions	Anomaly detection algorithm based on isolation forests by sending probe messages	Improvement in terms of accuracy, recall, and F1 score
[19]	Incorporates social networks in feature learning	GNN technique for feature learning	Improve precision, recall, and F1 score
[20]	Security concerns of the Domain Name System	Exponential random graph model and time series analysis	Improved precision in security of the Domain Name System
[21]	Focused on social welfare behaviour in IoT-based networks	Vector space-based aggregation with spatial index tree	Quick and accurate detection of abnormal behaviour in the network
[22]	Energy efficient Anomaly detection mechanism in three-tier IoT–edge–cloud networks	Marching square algorithm on data collected by the edge nodes to generate isopleths	Better accuracy and energy consumption as compared to other schemes
[23]	Emphasized on real-time data accuracy in Industrial IoT applications	Deep anomaly section framework based on CNN and a two-stage LSTM	Improves efficiency of the resource-constrained edge devices

notification. BE determines the number of backoff periods, a node has to wait before accessing the channel and is calculated as $2^{BE}-1$. The initial default value of BE is 3 and the number of random backoff periods, a node has to wait initially is in the range of $0-7$. If it cannot find the medium idle, then the algorithm increments the BE value and the waiting range before accessing the medium increases to $0-15$. Parameter CW allows a node to check the medium availability twice before transmitting the frame.

If the transmitted frame cannot reach its destination due to collision with another frame in the medium then it is re-transmitted. If several re-transmissions reach the parameter limit defined in $macMaxFrameRetries$ parameter, then the transmission is considered unsuccessful.

B. Attacks on IEEE 802.15.4 Standard

Malicious nodes interfere with the medium to disturb the communication of legitimate nodes. This work focuses on the malicious attacks during CAP of IEEE 802.15.4 standard. The following three types of malicious node attacks are quite common in the MAC protocols to disturb the communication standards of the protocol:

1) Exhaustion Attack
2) Collision Attack
3) Unfairness Attack

1) Exhaustion attack: During the CAP, nodes utilize CSMA/CA before transmitting a frame into the medium. They assess the medium's availability by conducting a Clear Channel Assessment (CCA). Malicious nodes keep the medium occupied by transmitting a long stream of messages. This results legitimate node finding the medium busy even after multiple tries as mentioned in $MaxCSMABackoffs$ parameters and the required message initiated by the upper layer is exhausted.

Hen a node transmits its packet and cannot receive its acknowledgment, then it has to resend the packet again and again till its maximum limit and then finally declares that the packet can not be transmitted.

2) Collision attack: Collision occurs when two or more nodes transmit their packets in the medium at the same time and cause the collision. Nodes wait for the acknowledgment for a certain time as mentioned in the parameter $macAckWaitDuration$ of the standard. If transmitting nodes do not receive the acknowledgment within the specific time, then it re-transmits the frame and if the number of retries reaches the limit mentioned in $macMaxFrameRetries$, then the transmission is declared unsuccessful. Malicious nodes disturb the communication after intentionally transmitting a short message while detecting the medium busy causing collisions of the frames transmitted by legitimate nodes.

3) Unfairness attack: The standard offers fairness by allowing all nodes equal chances to assess the medium after the decrement of the backoff period. A node after completing its backoff period can access the medium in transmitting its frame. Similarly, the standard allocates GTS to nodes, on a First Come First Serve (FCFS) basis. In case, the PAN coordinator receives GTS requests more than its available limit of 7, then it assigns GTS to those nodes, whose requests arrive first. Malicious nodes do not wait for their assigned backoff periods and initiate their requests at once which reduces the fair chances of other nodes to access the medium. Similarly, it occupies the GTS by initiating early GTS requests to the PAN coordinator and GTS requests of legitimate nodes of the networks are not entertained.

These malicious node attacks create an anomaly in the IoT network applications and QoS is compromised. In this work, an Anomaly Detection Mechanism for IEEE 802.15.4 standard ($ADM_{15.4}$) in an IoT network is proposed. $ADM_{15.4}$ detects malicious attacks in the network and then proposes a comprehensive mechanism to improve the QoS of the network by avoiding malicious attacks.

IV. PROPOSED SCHEME

In this work, malicious nodes' presence is identified by proposing an anomaly detection mechanism during CAP of IEEE 802.15.4 standard. The proposed $ADM_{15.4}$ detects anomalies in the network by introducing an anomaly detection

method and then proposes a solution to neutralize its effect to improve the QoS of the IoT network. The main features of our proposed scheme and described below and its flow is mentioned in Fig. 2.

- Anomaly detection mechanism to detect the anomaly in the medium through a soft function.
- Once an anomaly is detected in a medium, the communication of the region is restricted to prevent a malicious attack by transmitting a jamming signal.
- Data transmission of the affected legitimate nodes available in the restricted region along with an efficient GTS allocating method to improve the QoS.

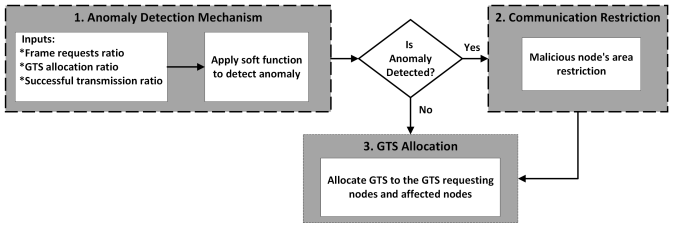


Fig. 2. A Flow of different sections of the proposed scheme.

A. Anomaly Detection Mechanism

Physical and MAC layers of most of the IoT-based networks follow IEEE 802.15.4 standard. MAC layer attacks of malicious nodes compromise the efficiency of the network. In the IEEE 802.15.4 standard, most of the attacks are during its CAP and disturb its performance. The proposed method, based on [24], is used to detect anomalies in the network using various parameters at the end of each SD. The method involves several steps, as shown in Fig. 3.

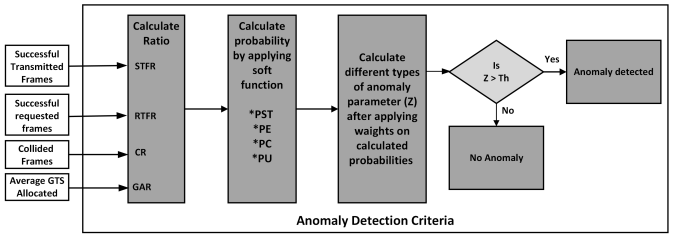


Fig. 3. Flow of the proposed anomaly detection mechanism.

1) Transmission and collision ratio: PAN coordinator at the end of each SD computes the following ratios of the different parameters that are observed during the SD.

a) Successful Transmitted Frames (STF) ratio: STF is calculated during each SD of the standard by calculating the number of successfully transmitted packets against the total number of requests.

b) Requested Frame (RF) ratio: RF is calculated as the number of frames successfully transmitted in the medium to the total number of the frames, nodes intend to transmit during an SD.

c) Collision Ratio (CR): CR is computed by dividing the total number of collisions detected by the total number of frames transmitted in the medium during SD. This metric provides insight into the efficiency of the network by quantifying the proportion of frames that experienced collisions during the specified period.

d) GTS Allocation Ratio (GAR): GAR is the maximum value among all the GTS requested nodes that is calculated as the average number of GTS allocated to a node against a total number of GTS requests received.

2) Implementation of soft function: After calculating all the ratios during the SD, a soft function (ψ) is formulated to determine the probabilities of various events based on input values. Specifically, it calculates the probability of successful transmission (PST), the probability of exhaustion attacks (PE), the probability of collision attacks (PC), and the probability of unfairness attacks (PU) using the input values of STF, RF, CR, and GAR, respectively. The mathematical expression is as follows:

$$\psi(X) = \frac{1}{1 + e^{-E \times (V-F)}} \tag{3}$$

Here, $\psi(X)$ is in the range between 0 and 1 and its outcome is the PST, PE, PC, and PU, while replacing V with inputs of STF, RF, CR, and GAR respectively in the soft function. The value of V can be determined through the desired value (Y_D) and real values (Y_R) as mentioned in Eq. 4.

$$J(V) = (Y_D - Y_R)^2 \tag{4}$$

However, E represents slope and F represents the centre of the curve. The shape of the curve is contingent upon these two values, and their dynamics evolve, recalculated after each SD as:

$$E_{K+1} = E_K + (\phi \times \frac{\partial J}{\partial E}) \tag{5}$$

Here ϕ ranges between 0 and 1 and $\frac{\partial J}{\partial E}$ are calculated as:

$$\frac{\partial J}{\partial E} = 2(Y_D - Y_R) \times \frac{E_K}{[1 + e^{-E_K \times (V-F_K)}]^2} \tag{6}$$

Similarly F_{K+1} is calculated as:

$$F_{K+1} = F_K + (\phi \times \frac{\partial J}{\partial F}) \tag{7}$$

Here $\frac{\partial J}{\partial F}$ is calculated as:

$$\frac{\partial J}{\partial F} = 2(Y_D - Y_R) \times \frac{-E_K \times e^{-E_K \times (V-F_K)}}{[1 + e^{-E_K \times (V-F_K)}]^2} \tag{8}$$

Algorithm 1: Anomaly Detection Algorithm

Input: Successful Transmission Ratio STR, Requested Frame Ratio RF, Collision Ratio CR, GTS Allocation Ratio GAR,

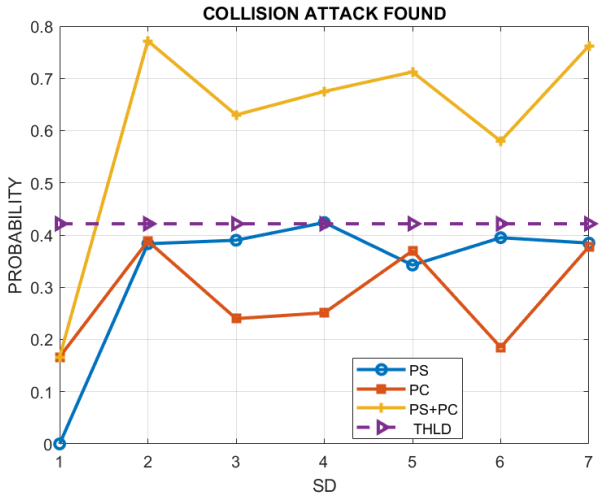
Compute $PST = 1/1 + exp(-E \times (STR - F))$
Compute $PE = 1/1 + exp(-E \times (RF - F))$
Compute $PC = 1/1 + exp(-E \times (CR - F))$
Compute $PU = 1/1 + exp(-E \times (GAR - F))$
Compute $Z_1 = (PST \times \psi) + (PE \times \theta)$
Compute $Z_2 = (PST \times \psi) + (PC \times \theta)$
Compute $Z_3 = (PST \times \psi) + (PU \times \theta)$
if $Z_1 > Th$
Exhaustion Attack
else
No Exhaustion Attack
if $Z_2 > Th$
Collision Attack
else
No Collision Attack
if $Z_3 > Th$
Unfairness Attack
else
No Unfairness Attack

3) Anomaly detection with results: After determining the PST, PE, PC, and PU, the PAN coordinator assigns weights that are within the range of 0 and 1 to each of the calculated probabilities. Each of the exhaustion, collision, and unfairness probability in combination with the weighted successful transmission probability compute the anomaly value. The calculated anomaly value is compared with the threshold value calculated in [25] to find the anomaly. The proposed anomaly detection algorithm is shown in Algorithm 1.

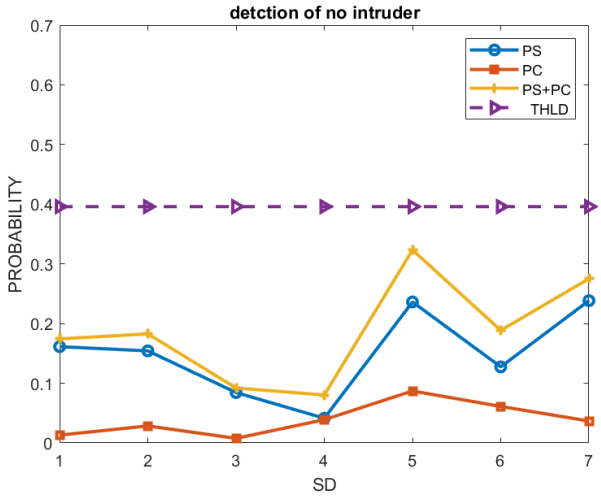
Results in Fig. 4 show the anomaly detection by the proposed algorithm to find the collision. Sub-figure 4b shows when there are no collision attacks found in the network as they are below the threshold level. However, sub-figure 4a shows the collision detection as the collision found in the network is more than the threshold limit as calculated in [25].

Results in Fig. 5 represent the presence of exhaustion attacks in the network and it is comprised of two sub-plots. Subplot 5b exhibits when there are no exhaustion attacks found as the exhaustion value represented by Z1 in the algorithm is less than the threshold value. However, exhaustion attacks are found as shown in subplot 5a, when the exhaustion value is greater than the threshold value.

Results in Fig. 6 represent the unfairness attacks. Unfairness attacks are calculated from the GTS allocation in the standard as described in Section III-B and are determined from exhaustion value Z3 from the algorithm. The figure comprises two subplots. Subplot 6a shows when the exhaustion value is greater than the threshold value due to the exhaustion attacks, however subplot 6b represents when the exhaustion value is less than the threshold limit resulting in no unfairness attacks found in the medium.



(a) Collision attacks.



(b) Without collision attack.

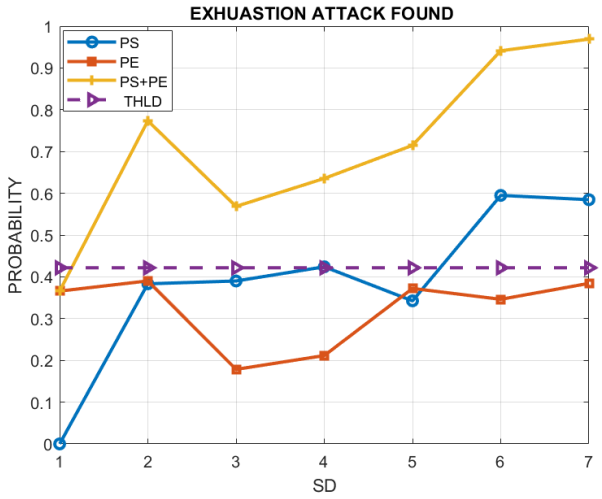
Fig. 4. With and without collision attack.

B. Prevention of Malicious Attacks

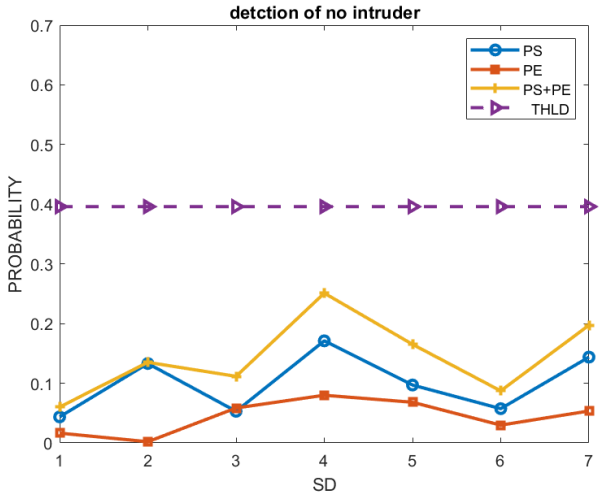
After successfully detecting the presence of a malicious node, its attacks are required to be neutralized by blocking its communication. In a terrestrial IoT network architecture, the PAN coordinator is supposed to know the location of each IoT node placed in the network with the help of its short address provided by the PAN coordinator of IEEE 802.15.4 standard. To stop the communication of the malicious nodes in the network, the PAN coordinator in its beacon frame requests one of the neighbouring malicious nodes, which has the highest residual energy level, to transmit jamming signals during CAP. Generating a jamming signal restricts the communication of all the nodes present in that area resulting in compromised QoS in that area as mentioned in Fig. 7.

C. Communication of the Affected Nodes

The communication of the legitimate nodes present in the restricted areas is provided by allocating GTS in the upcoming

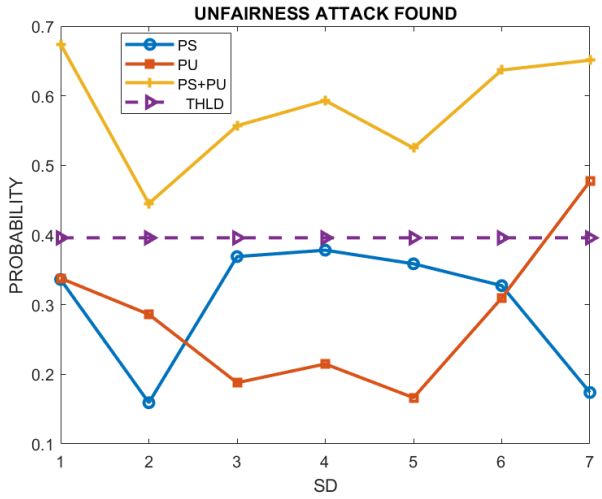


(a) Exhaustion attacks.

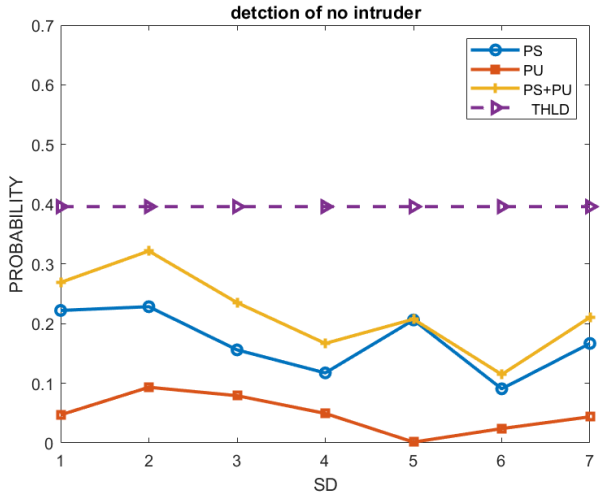


(b) Without exhaustion attack.

Fig. 5. With and without exhaustion attack.



(a) Unfairness attacks.



(b) Without unfairness attack.

Fig. 6. With and without unfairness attack.

SD. Due to restricted CAP, these affected nodes are unable to transmit their GTS requests to the PAN coordinator, In such a scenario, the GTS are assigned to these affected nodes by analyzing the nodes' previous transmission pattern. Suppose PAN coordinator receives j number of requests during past k sessions, then its expected GTS requests (GTS_i) is calculated as:

$$GTS_i = (K_{\text{last}} - K_{\text{cur}}) + \left\lceil \frac{K}{J} \right\rceil \tag{9}$$

Here, K_{last} is represented as the last SD when node i initiated the request and K_{cur} is the upcoming SD.

Each SD of IEEE 802.15.4 standard consists of 7 TDMA-like CFP slots. PAN coordinator after determining the expected GTS allocation to the affected nodes, assigns the remaining slots against the GTS requests received from the unaffected legitimate nodes. Suppose the PAN coordinator has m CFP slots available and the number of GTS required to be allocated to affected nodes is n, then the PAN coordinator can only accommodate $m - n$ GTS requested slots in the next SD. If the number of GTS requested by the unaffected legitimate nodes is less than $m - n$ slots, then it can entertain all the GTS requests. However, in case, the number of requested GTS exceeds the available slots, a scrutiny of GTS takes place based on their priority levels. This is accomplished by employing the 0/1 knapsack algorithm.

To determine the priority of a node, the default GTS requesting command frame format has been modified by utilizing its two reserved bits. Each node requesting GTS informs its PAN coordinator about the number of GTS required, along with its priority level. This information is conveyed in the last two reserved bits of the GTS characteristic field, which is part of the GTS request command frame format specified in the IEEE 802.15.4 standard, as illustrated in the accompanying Fig. 8. Priority levels of each IoT node are categorized into

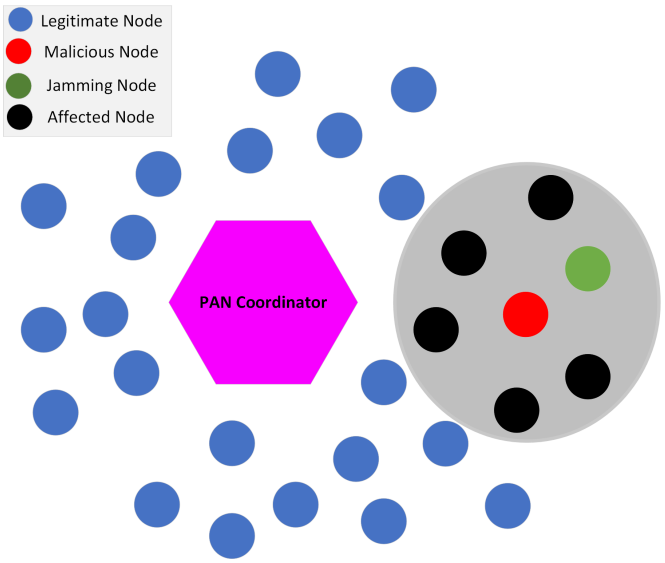


Fig. 7. IoT Network with malicious and affected nodes.

four different levels ranging from 00 to 11 representing the lowest to the highest priority levels, respectively.

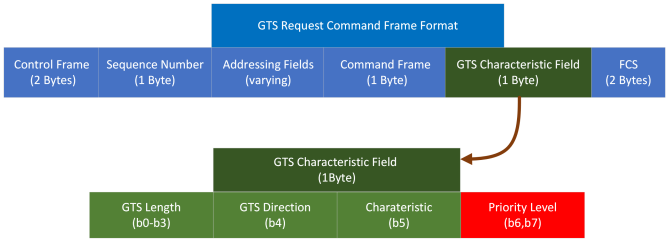


Fig. 8. Modified GTS request command frame format of IEEE 802.15.4 standard.

The PAN coordinator scrutinizes the GTS requests by applying the 0/1 knapsack algorithm. The available CFP slots in the upcoming SD are considered as sack capacity. Each GTS requesting node is mapped with an item and its requested slots are mapped as the weight of the item. The value of the item (V_i) is mapped with the value of the GTS requesting node i and depends upon its priority (P_i) and the time (T_i) that it has to wait after initiating its GTS request as:

$$Val_i = P_i \times T_i \tag{10}$$

Priority of the requested GTS as calculated from the proposed GTS requesting command frame format as shown in Fig. 7. However, the waiting time is calculated as:

$$T_i = N_i + \frac{(960 \times 2^{BO}) - X_i}{960 \times 2^{BO}} \tag{11}$$

Here, N_i represents the consecutive number of requests, the PAN coordinator receives from node i. If there is no GTS request in the previous beacon interval (BI), then its value is 0, however, if the same node is requesting GTS for the last two BI and its request is not entertained, then the value of N is 2. X_i is the duration in symbols and it is calculated as the time between the start of the beacon frame and the time when the PAN coordinator receives the GTS request.

The proposed $ADM_{15.4}$ assists the PAN coordinator in allocating the available GTS to the GTS requesting nodes as:

1) Assign GTS to all GTS requesting nodes if requesting slots are less than the available GTS in the upcoming SD.
2) Scrutinize the GTS requesting node in allocating the GTS if the number of requesting slots is more than the available GTS.

A complete algorithm for GTS allocating nodes in upcoming SD for PAN coordinator is shown in Algorithm 2.

V. System Model

Wireless sensor-based IoT nodes are being used in diverse wireless applications. Most of the wireless sensor networks use IEEE 802.15.4 standard in their MAC and Physical layers. Malicious wireless nodes being a part of the network, try to disturb the communication of the legitimate nodes and create an anomaly. In this work, the superframe structure of IEEE 802.15.4 standard operating at a 2.4GHz frequency channel is used for communication between all wireless connected nodes creating a Wireless Personal Area Network (WPAN). WPAN comprises a PAN coordinator and its member nodes. A system model of this work comprises of WPAN coordinator with legitimate member nodes and few malicious nodes as shown in Fig. 9. A WPAN coordinator acting as Cluster Head (CH) is selected based on the higher residual energy level among all nodes. All other nodes in the WPAN act as member nodes. All member nodes are in direct connection with the CH and do not use any relaying node to reach CH. Malicious nodes are part of the network and disturb the medium access of all legitimate nodes by transmitting information during CAP of the standard. This causes legitimate nodes to find the medium busy as well as increases the chances of collision in the medium with increased unfairness of the legitimate nodes.

Nodes can transmit their data during CAP as well as during CFP. A data frame transmitted during a CAP is successfully delivered, if it receives its acknowledgment within a stipulated time as mentioned in different parameters in IEEE 802.15.4 standard. Total time (ζ) required in transmitting a requesting frame during CAP is calculated as sum of backoff count (BC), data transmitting duration (TD, Propagation delay (PD), turn around (TA) time, Acknowledgment frame time (AF), and Inter-frame space (IFS) as mentioned in Eq. 12 and is shown in Fig. 10.

$$\zeta = BC + TD + (2 \times PD) + TA + AF + IFS \tag{12}$$

If X number of legitimate nodes are successful in transmitting its frames during CAP of a SD, then accumulated time (σ_{CAP}) calculated in successful transmission of data requested frames during CAP in q number of SD is calculated as:

Algorithm 2: GTS Allocation Mechanism

$w \leftarrow$ Current slot number
$W \leftarrow$ Max. number of available GTS
$a \leftarrow$ Node ID
$v \leftarrow$ Maximum Number of GTS requesting nodes
$k \leftarrow$ Maximum Number of GTS requested
$A[a, w] \leftarrow$ Cell value of a^{th} node and w^{th} slot
$w_a \leftarrow$ Slots requested by a^{th} node
if $K < W$ **then**
  Allocate GTS to all requesting nodes
end
else
  Scrutinize nodes by applying 0/1 knapsack
  Populating the 0/1 knapsack table:
  for $w = 0$ *to* W **do**
    $A[0, w] = 0$
  end
  for $a = 1$ *to* v **do**
    $A[a, 0] = 0$
  end
  for $a = 1$ *to* v **do**
    for $w = 0$ *to* W **do**
      if $w_a \leq w$ **then**
        if $w_a + A[a-1, w-w_a] > A[a-1, w]$ **then**
          $A[a, w] = w_a + A[a-1, w-w_a]$
        end
        else
          $A[a, w] = A[a-1, w]$
        end
        else
          $A[a, w] = A[a-1, w]$
        end
      end
    end
    Nodes selection Criteria:
    while $a > 1$ *and* $w > 1$ **do**
      if $A[a, w] > A[a-1, w]$ **then**
        a^{th} node is selected
        $a = a - 1$
        $w = w - w_a$
      end
      else
        $a = a - 1$
      end
    end
  end
end

$$\sigma_{CAP} = \sum_{a=1}^{q} \sum_{b=1}^{X} SD_a \times \zeta_b \tag{13}$$

The time required in transmitting data during CFP is calculated as the time when a node, initiates its request during CAP since it transfers its data in CFP slots. Number of GTS required (CFP_i) to send m amount of data by a node i in transferring its data is calculated as:

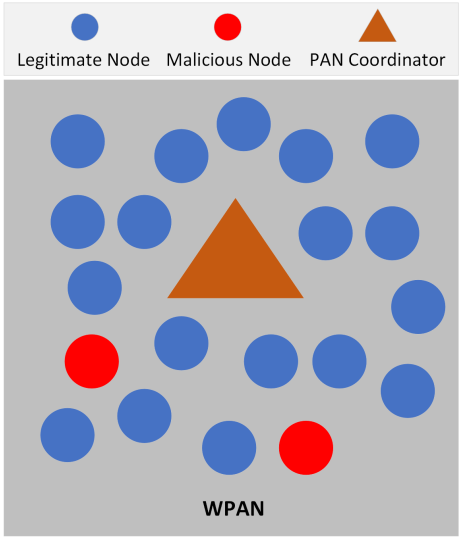


Fig. 9. System model of proposed scheme.

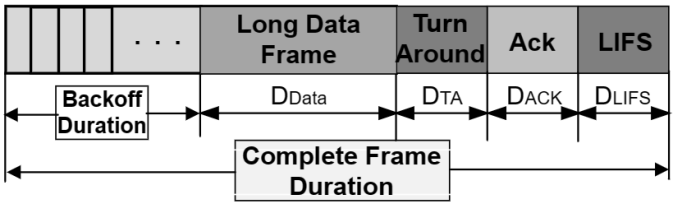


Fig. 10. A Complete frame length including acknowledgment.

$$CFP_i = \left\lceil \frac{m}{30 \times 2^{SO}} \right\rceil$$

Suppose node i sends a request of k number of GTS to the WPAN coordinator during CAP. If the WPAN coordinator successfully allocates its required GTS just before the j slots of the CFP period in the next SD, then the complete delay (CD_i) in transferring its data in its allocated GTS is calculated as:

$$CD_i = BI + SD - j + (\frac{m}{30 \times 2^{SO}}) \tag{14}$$

If p nodes are allocated GTS in each SD, then accumulated delay (σ_{GTS}) of all the WPAN in transferring data during CFP for q number of SD is calculated as:

$$\sigma_{GTS} = \sum_{a=1}^{q} \sum_{b=1}^{p} SD_a \times CD_b \tag{15}$$

VI. Results and Analysis

In this section, the performance of the proposed scheme is thoroughly examined across various dimensions. The analysis delves into different aspects, evaluating the efficacy of the proposed scheme within the system model outlined in the preceding Section V. A simulation environment is established by deploying a fixed number of legitimate nodes within a

WPAN. This network configuration includes one WPAN coordinator alongside legitimate nodes, and notably, one additional node designated as a malicious node. All nodes follow the IEEE 802.15.4 standard and communicate with each other on the same frequency channel of the 2.4 GHz frequency band. Malicious nodes are present in specific areas and their position is supposed to be identified by the PAN coordinator. A "10 X 10" meters area around the malicious node is blocked by transmitting Jamming signals during CAP by one of the legitimate nodes in that area. A random number of nodes during each SD generate their GTS requests to transmit their data during CFP. The results are analyzed for a fixed duty cycle of 50% along with varying duty cycles for different values of SO and different numbers of nodes. A list of simulation parameters is presented in the Table II.

TABLE II. SIMULATION PARAMETERS

Parameters	Values
Total Number of Member Nodes	19, 8, 12
Network Size	100 × 100
Data Rate	250Kbps
Number of Legitimate Nodes	19
Number of Malicious Node	1
Cluster Head	1
Superframe Order	0,2
Superframe Duration (msec)	15.4,61.4
Beacon Interval (msec)	30.7, 122.9
Slot Duration (msec)	1.92, 7.68
Duty Cycle	50%
Offered Load (Bytes)	50 to 125

The simulation results are observed in different prospects with and without attacks and the performance of our proposed $ADM_{15.4}$ scheme is evaluated. The performance is compared with the standard by data transmission, average transmission time, and number of GTS allocated nodes accommodated by the PAN coordinator.

A. Transmitted Data

The data transmitted is calculated for only those legitimate nodes that are allowed to transfer their data during CFP. The proposed scheme applies 0/1 knapsack algorithm in allocating GTS to the legitimate nodes. However, the IEEE 802.15.4 standard applies FCFS in allocating GTS to the requesting nodes.

Results shown in Fig. 11 represent the effect on data transmission with and without attacks. The results show that the data transmission for the same number of data-requesting nodes increases at the same rate when there is no malicious attack. On the other hand, the data transmission is affected due to malicious attacks in the second SD. However, in the proposed scheme, the data transmission is affected in the second SD, however after the blocking of the region at the start of the 3^{rd} SD, the rest of the nodes keep on transmitting their data. It can be observed from the results that between 1 and 2 SD values, there is no malicious attack and all nodes are transmitting data with same rate. However, in the 2^{nd} SD, malicious nodes attack the medium and attacks are detected by the proposed scheme at the end of the 2^{nd} SD and a prevention mechanism is applied in the 3^{rd} SD by transmitting jamming signals in the surrounding of the malicious node. This affects the communication of nodes in the specific area, however,

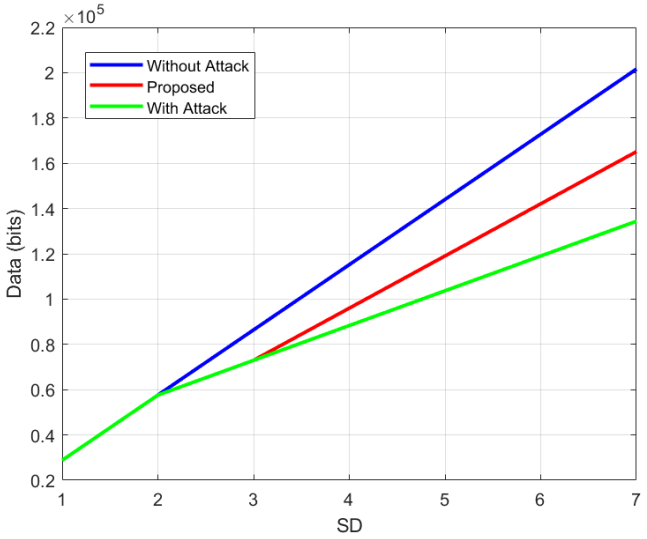


Fig. 11. Data transmission of nodes with and without attacks.

nodes present in the rest of the area remain unaffected and keep on transmitting their data.

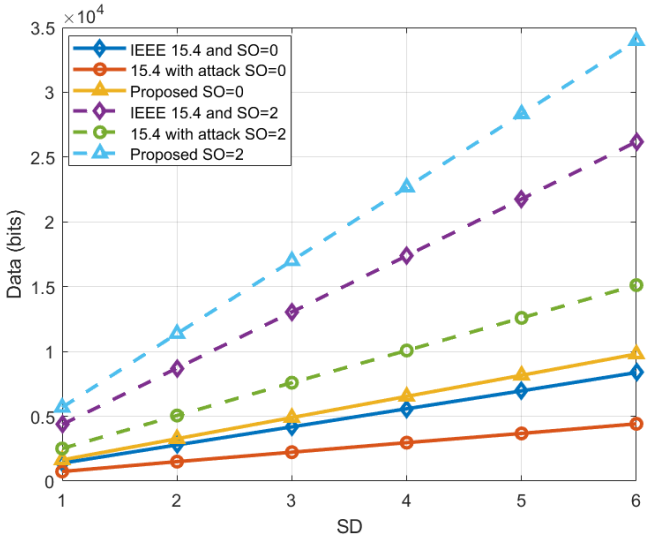


Fig. 12. Data transmission of GTS requesting nodes.

When attacks were found then $ADM_{15.4}$ allocates GTS to the nodes affected in that area as described in Section IV-B. Results shown in Fig. 12 represent the total amount of data transmitted by all nodes during CFP duration in the network when SO=0 and SO=2. The performance of the proposed scheme is evaluated by comparing its results with both the IEEE 802.15.4 standard under attack scenarios and the IEEE 802.15.4 standard in the absence of attacks. The results show that, for both values of SO, the data transmission in the proposed scheme is 30% more than the standard without attacks and and 122% more than the standard with attack. This is due to the efficient allocation of GTS among GTS requesting nodes by applying the 0/1 knapsack algorithm because it allows the PAN coordinator to optimally allocate GTS among

the requesting nodes.

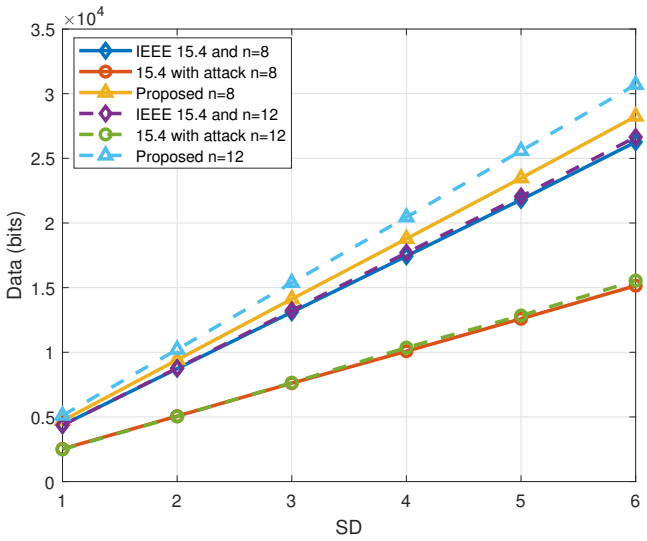


Fig. 13. Data transmission of GTS requesting nodes for different number of nodes.

The performance of the proposed scheme is validated by calculating the transmitted data during CFP when there was a random number of GTS requests from 8 and 12 legitimate nodes with an SO value of 2 as shown in Fig. 13. The results showed that the proposed scheme allowed for more data transmission for both 8 and 12 requesting nodes compared to the standard, with and without attacks. This demonstrates an optimal allocation of GTS among requesting nodes to enable more data transmission in an SD. Moreover, the results highlighted that the data transmission of the standard was severely affected during attacks because the PAN coordinator was unable to differentiate between legitimate and malicious node requests. This led to the PAN coordinator assigning GTS to the malicious nodes at the start of the CAP by applying FCFS.

B. Transmission Delay

The delay in transmitting data is calculated for those nodes that have initiated the GTS requests. The time to transmit data for all those nodes, which are successfully allocated GTS are calculated by following the Eq. 14. However, the transmission time of all those nodes which are not allocated GTS are supposed to be assigned GTS in the next SD automatically by passing through another BI.

Results in Fig. 14 show the accumulated time calculated for all GTS requesting nodes in transmitting their data. It is evident from the results, that due to malicious attacks, the overall data transmission time of GTS requesting nodes increases due to less number of legitimate nodes being assigned GTS in a superframe duration and the rest are allowed to send their data in the next superframe duration with an increase in BI time interval. However, data transmission time in proposed $ADM_{15.4}$ is the least among all and even less than the IEEE 802.15.4 standard because it accommodates a maximum number of GTS requesting nodes in transmitting their data during CFP in the current SD and less number of GTS

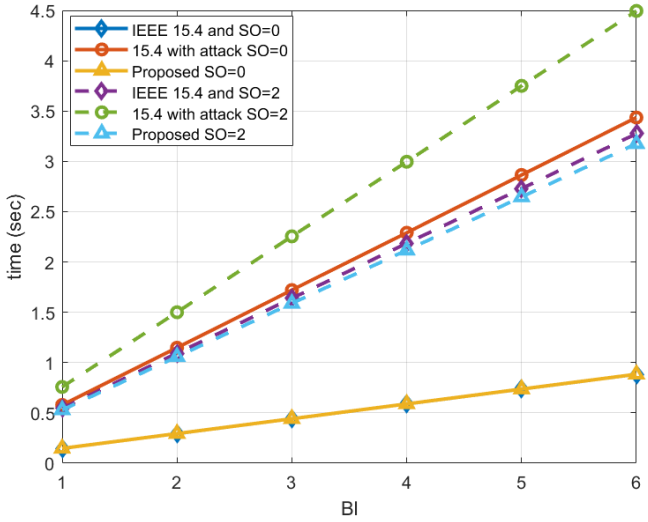


Fig. 14. Delay in transmitting data during contention free period.

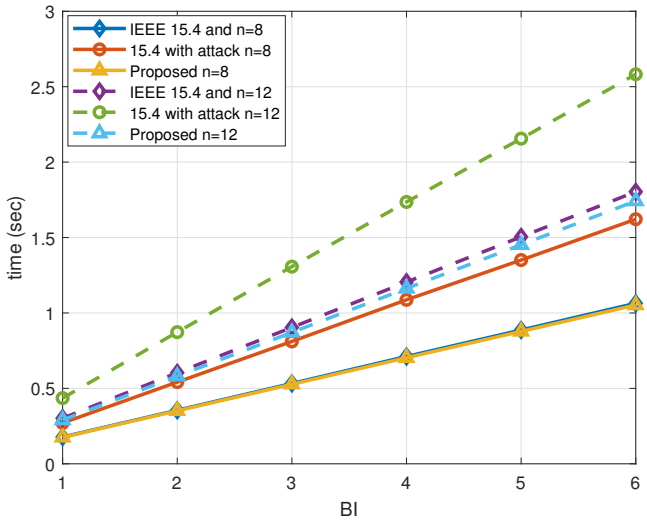


Fig. 15. Delay in transmitting data during contention free period for different number of nodes.

requesting nodes transmit their data in the next SD resulting in a reduced network delay.

Results shown in Fig. 15 represent the network delay of all GTS requesting nodes when the number of GTS requesting nodes are 8 and 12 with a 50% duty cycle. The results clearly show that the accumulated delay of all GTS requesting nodes in transmitting their data in $ADM_{15.4}$ is 0.5% to 3% less than the standard when there is no attack for both 8 and 12 GTS requesting nodes respectively. However, it is 58% and 49% less less in the presence of malicious attacks for number of nodes are 8 and 12, respectively because it allocates GTS to the malicious nodes and most of the legitimate nodes are unattended and are not allocated GTS.

Results in Fig. 16 show a comprehensive picture by calculating the difference in delay between the proposed scheme

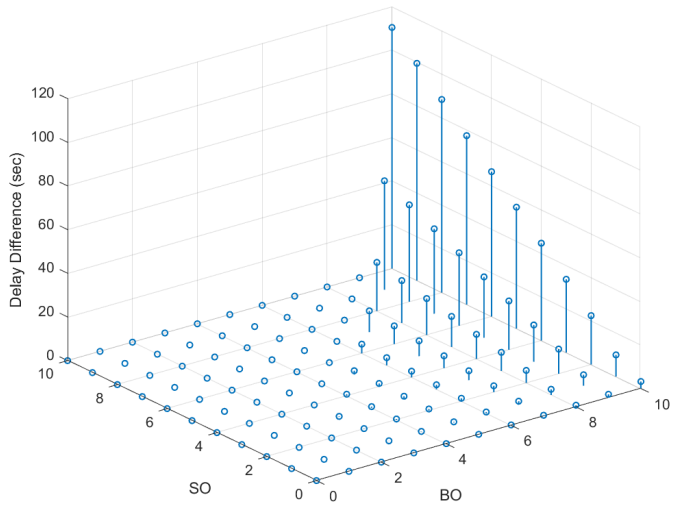


Fig. 16. Accumulated delay difference for all possible values of SO when BO=10.

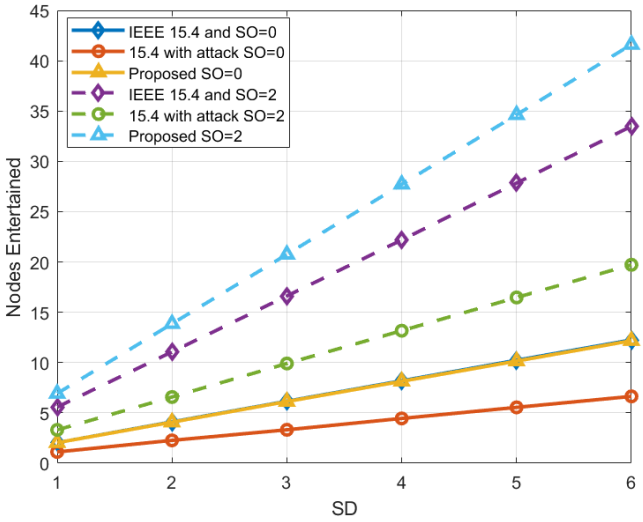


Fig. 17. Number of GTS requesting nodes entertained.

and IEEE 802.15.4 standard with attacks. The results are obtained by accumulating the total difference in delay faced by 19 legitimate nodes against all the possible values of SO when BO ranges from 0 to 10. The results show that with the increase in BO, the delay difference increases because higher BO allows an increased number of SO options and the accumulated sum of all the differences against all the possible values also increases. Furthermore, increased BO increases the BI, and unsuccessful GTS requesting nodes have to wait for another BI resulting in more delay.

C. GTS Allocating Nodes

GTS allocating nodes are calculated as the total number of GTS requests of legitimate nodes entertained by the PAN coordinator during an SD. The results are obtained for two different values of SO when the number of GTS requesting nodes is 20, and when the number SO is fixed and the number of GTS requesting nodes is 8 and 12 as shown in Fig. 17 and 18, respectively.

Fig. 17 shows the total number of GTS requesting nodes, that have been successfully allocated GTS in a SD by WPAN. It is evident from the results that $ADM_{15.4}$ entertains the maximum number of GTS requesting nodes in a SD and number of GTS entertained for $SO = 2$ are 24% and 110% more than IEEE 802.15.4 standard without attacks and with attacks, respectively. However, when $SO = 0$, then the proposed scheme allocates the same number of GTS requesting nodes as nodes entertained by IEEE 802.15.4 standard without attacks. This is due to the reason that the optimal number of GTS requesting nodes is also entertained by the PAN coordinator in IEEE 802.15.4 standard. However, due to unfairness attacks, some CFP slots are allocated to malicious nodes, resulting in less number of CFP slots left that are allocated to legitimate nodes.

Results in Fig. 18 show that the number of nodes entertained throughout the different superframe durations in the

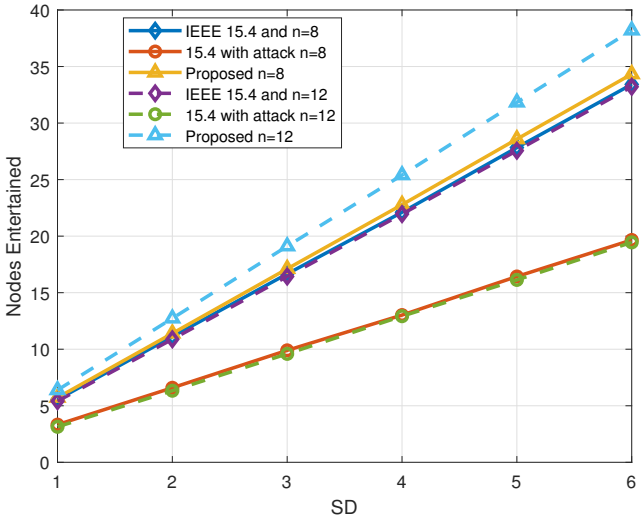


Fig. 18. Number of GTS requesting nodes entertained for different number of nodes.

proposed scheme is the highest for both numbers of GTS requesting nodes. It is evident from the results that the accumulated number of GTS requests entertained by the PAN coordinator is maximum when GTS requesting nodes are 12 in the proposed scheme. This is due to the optimal allocation of GTS to the GTS requesting nodes by applying the 0/1 knapsack algorithm as compared to FCFS used in the IEEE 802.15.4 standard. The results further show that the least number of GTS requests of the legitimate nodes are entertained in the presence of the malicious attacks because the standard does not differentiate the malicious attacks and some of the GTS are allocated to malicious nodes resulting in less number of GTS left for allocation to legitimate nodes.

VII. Conclusion

This work addresses the compromised QoS due to anomaly created by malicious nodes in the communication medium of IEEE 802.15.4 standard. In this work, an Anomaly Detection Mechanism for IEEE 802.15.4 standard $ADM_{15.4}$ is proposed. The proposed scheme detects the different types of anomaly caused by malicious node attacks during the contention access period of the superframe structure of the standard. Furthermore, $ADM_{15.4}$ proposes a PLC-based mechanism to stop the interference caused by a malicious node by transmitting jamming signals to its nearby node. This causes an interruption in a specific region and nodes in that region are unable to communicate during the contention access period. To overcome their communication interruption, these nodes are allocated GTS to transmit their information to WPAN applying a 0/1 knapsack algorithm in such a way that maximum GTS requesting nodes are entertained. The simulation results show that the proposed scheme improves the data transmission of legitimate nodes by 122% and 30% as compared to the standard with and without attacks respectively. The transmission delay of legitimate GTS requesting nodes is also reduced by 58% and 3% as compared the standard with and without attacks and accommodates up to 24% and 110% more GTS requesting nodes to transmit their data during CFP period in the current superframe duration. The improved data transmission and reduced transmission delay makes the proposed scheme suitable for future IoT applications. In the future, we will explore methods to detect anomalies due to data integrity attacks and faulty IoT sensors.

Acknowledgment

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (Grant number IMSIU-RP23082).

References

[1] K. Fizza, P. P. Jayaraman, A. Banerjee, N. Auluck, and R. Ranjan, "Iot-qwatch: A novel framework to support the development of quality-aware autonomic iot applications," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 17 666–17 679, 2023.

[2] A. A. Abdulameer and R. K. Oubida, "The impact of iot on real-world future decisions," in *AIP Conference Proceedings*, vol. 2591, no. 1. AIP Publishing, 2023.

[3] A. Gupta, T. Gulati, and A. K. Bindal, "Wsn based iot applications: A review," in *2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22)*, 2022, pp. 1–6.

[4] B. Yao, R. Tang, and S. Ma, "Consideration in wsn applying for the health monitoring of transport aircraft," in *2023 9th International Symposium on System Security, Safety, and Reliability (ISSSR)*, 2023, pp. 44–48.

[5] X. Li, B. Hou, R. Zhang, and Y. Liu, "A review of rgb image-based internet of things in smart agriculture," *IEEE Sensors Journal*, vol. 23, no. 20, pp. 24 107–24 122, 2023.

[6] B. H. S. Alamri, M. M. Monowar, and S. Alshehri, "Privacy-preserving trust-aware group-based framework in mobile crowdsensing," *IEEE Access*, vol. 10, pp. 134 770–134 784, 2022.

[7] S. You, K. Radivojevic, J. Nabrzyski, and P. Brenner, "Trust in the context of blockchain applications," in *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, 2022, pp. 111–118.

[8] D. Popovic, H. K. Gedawy, and K. A. Harras, "Fedteams: Towards trust-based and resource-aware federated learning," in *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2022, pp. 121–128.

[9] D.-Y. Kim, N. Alodadi, Z. Chen, K. P. Joshi, A. Crainiceanu, and D. Needham, "Mats: A multi-aspect and adaptive trust-based situation-aware access control framework for federated data-as-a-service systems," in *2022 IEEE International Conference on Services Computing (SCC)*, 2022, pp. 54–64.

[10] J. Guo, A. Liu, K. Ota, M. Dong, X. Deng, and N. N. Xiong, "Itcn: An intelligent trust collaboration network system in iot," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 203–218, 2022.

[11] X. Shen, W. Lv, J. Qiu, A. Kaur, F. Xiao, and F. Xia, "Trust-aware detection of malicious users in dating social networks," *IEEE Transactions on Computational Social Systems*, pp. 1–12, 2022.

[12] A. N. Alvi, S. Khan, M. A. Javed, K. Konstantin, A. O. Almagrabi, A. K. Bashir, and R. Nawaz, "Ogmad: Optimal gts-allocation mechanism for adaptive data requirements in ieee 802.15.4 based internet of things," *IEEE Access*, vol. 7, pp. 170 629–170 639, 2019.

[13] S. Khan, A. N. Alvi, M. A. Javed, Y. D. Al-Otaibi, and A. K. Bashir, "An efficient medium access control protocol for rf energy harvesting based iot devices," *Computer Communications*, vol. 171, pp. 28–38, 2021.

[14] S. Khan, A. N. Alvi, M. A. Javed, and S. H. Bouk, "An enhanced superframe structure of ieee 802.15.4 standard for adaptive data requirement," *Computer Communications*, vol. 169, pp. 59–70, 2021.

[15] X. Ma and W. Shi, "Aesmote: Adversarial reinforcement learning with smote for anomaly detection," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 943–956, 2021.

[16] X. Wang, S. Garg, H. Lin, J. Hu, G. Kaddoum, M. Piran, and M. Shamim Hossain, "Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7110–7119, May 2022.

[17] T. V. Phan, T. G. Nguyen, N.-N. Dao, T. T. Huong, N. H. Thanh, and T. Bauschert, "Deepguard: Efficient anomaly detection in sdn with fine-grained traffic flow monitoring," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1349–1362, 2020.

[18] M. A. Javed, M. Z. Khan, U. Zafar, M. F. Siddiqui, R. Badar, B. M. Lee, and F. Ahmad, "Odpv: An efficient protocol to mitigate data integrity attacks in intelligent transport systems," *IEEE Access*, vol. 8, pp. 114 733–114 740, 2020.

[19] T. Zhao, T. Jiang, N. Shah, and M. Jiang, "A synergistic approach for graph anomaly detection with pattern mining and feature learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 6, pp. 2393–2405, 2022.

[20] M. Tsikerdekis, S. Waldron, and A. Emanuelson, "Network anomaly detection using exponential random graph models and autoregressive moving average," *IEEE Access*, vol. 9, pp. 134 530–134 542, 2021.

[21] J. Tang, T. Qin, D. Kong, Z. Zhou, X. Li, Y. Wu, and J. Gu, "Anomaly detection in social-aware iot networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 3162–3176, 2023.

[22] Y. Li, Z. Zhou, X. Xue, D. Zhao, and P. C. K. Hung, "Accurate anomaly detection with energy efficiency in iot–edge–cloud collaborative networks," *IEEE Internet of Things Journal*, vol. 10, no. 19, pp. 16 959–16 974, 2023.

[23] H. Nizam, S. Zafar, Z. Lv, F. Wang, and X. Hu, "Real-time deep anomaly detection framework for multivariate time-series data in industrial iot," *IEEE Sensors Journal*, vol. 22, no. 23, pp. 22 836–22 849, 2022.

[24] N. M. F. Qureshi, A. Noorwali, A. N. Alvi, M. Z. Khan, M. A. Javed, W. Boulila, and P. A. Pattanaik, "A novel qos-oriented intrusion detection mechanism for iot applications," *Wireless Communications and Mobile Computing*, vol. 2021, p. 9962697, 2021. [Online]. Available: https://doi.org/10.1155/2021/9962697

[25] A. N. Alvi, S. H. Bouk, S. H. Ahmed, and M. A. Yaqub, "Influence of backoff period in slotted csma/ca of ieee 802.15.4," in *Wired/Wireless Internet Communications*, L. Mamatas, I. Matta, P. Papadimitriou, and Y. Koucheryavy, Eds. Cham: Springer International Publishing, 2016, pp. 40–51.