IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 29, 2021, accepted June 12, 2021, date of publication June 16, 2021, date of current version June 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3089683

Prediction of Re-Occurrences of Spoofed ACK Packets Sent to Deflate a Target Wireless Sensor Network Node by DDOS

MOHAMMED ABDULAZIZ AL-NAEEM, (Member, IEEE)
Department of Computer Networks and Communications, College of Computer Science and Information Technology, King Faisal University, Al-Hasa 31982, Saudi Arabia

e-mail: naeem@kfu.edu.sa

This work was supported by the Deanship of Scientific Research at King Faisal University through Nasher Track under Grant 216028.

ABSTRACT The Wireless Sensor Network (WSN) has evolved into a new IoT scheme, and its adoption has no restrictions at present. Sadly, security has an impact on the network of wireless sensors, and Denial-of-Service (DOS) categories of attacks are security concerns. This study therefore focuses on the distributed denial of service (DDOS), especially on DDoS-PSH-ACK (ACK & PUSH ACK Flood) in WSN. An experimental analysis was developed to predict that many spoofed ACK packets were reoccurring in order to deflate the target node. In the proposed approach, several experimental scenarios for the DDOS detection function were established and implemented. The experimental analysis draws traffic flow within the several transmission sessions involving ‘‘the normal transmission within sensor nodes and cluster head’’, as well as the ‘‘transmission and retransmission scenarios within the sensor nodes and cluster head’’ at same time with different signal sizes. The main contribution of the paper is predicting DDoS attack by variability of transmission behavior with high degree accuracy. It was established that the most ideal delay between transmissions is 23 milliseconds in order to ensure that the receiving end is not overwhelmed. The result of the current study highlighted that when transmission session gets overwhelmed, that influence DDOS success.

INDEX TERMS WSN wireless sensor network, distributed DoS attack, flooding attack.

I. INTRODUCTION

The wireless sensor network is not different from the conventional computer network; however, it is exclusively the connected sensor network via radio connections without a central control system [1]. This is typical of distributed communication where a neighborhood node can be felt by every node in a system. This type of network is implemented in a different environment, mainly in overhead water monitoring systems and so many others. They are developed and could be vulnerable to certain attacks in a coordinated setting. It could usually be because of the extensive use of the Internet and the many security problems that arise in various DoS formats. DDoS is the name given to the categories of DOS attacks from various locations [2]. It is a major threat to all network security problems because it generates enormous amounts of data traffic to exhaust all target system resources and inactivate the communication link by stopping the server from processing legitimate requests for users to conduct transactions [3]. The DDOS operable computing resources are mainly the network bandwidth and processing unit of computers and memory. This is, its capacity tends to be overpowered the communication channels. Once DDOS is initiated, a large volume of unwanted traffic data will flood the target channel into a transmission connection. In some cases, the attack aims to have a network node injecting a wide range of unwanted requests with all the transmission links to the node. For example, attackers can inundate the requested data to that server by targeting an email server to overload its computer power by disabling it for any transaction. A DDOS attack with only one attacker and one victim can usually be detected easily, but a DDOS attack with a

The associate editor coordinating the review of this manuscript and approving it for publication was Guangjie Han.

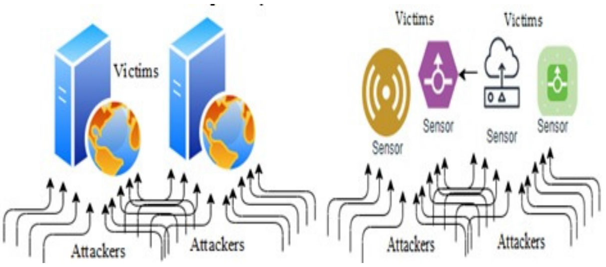

FIGURE 1. Distributed denial of service in a conventional network by the left and with the WSN by the right. Note that "Fig.1" involve two scenes. That is, DDOS scenarios on two different network environment.

large number of attackers that flood the transmission session normally leads to a great deal of damage for the hosts. Take Figure 1, for example. The DDOS attack scenarios on the left hand side are shown in conventional networked computing systems, and the WSN scenarios are shown in DDOS attacks on the right. In both cases, the attackers aim to flood the network, where they can harm whole links and make the channel inaccessible. That is why such an attack must be detected and prevented. It is very important to note that DDOS attack data traffic is not malicious. This is why DDoS attacks and regular traffic, especially in the WSN, are hard to distinguish.

DDoS attack is one of the most important threats in WSN among all security problems. The main research problem that this research is highlighting lies with DDOS attack initiation on a certain case within WSN environment. Typically, if the ignition of the DDOS went unnoticed, and if all of the evidence associated to that are also undetected. Furthermore, the uncertainty of whether the traffic flow within (1) one-way transmission sessions involving sensor nodes and cluster head, (2) the transmission and retransmission scenarios within the sensor nodes and cluster head at same time with different signal sizes can contribute to DDOS detection was still not resolved. Despite the use of many theoretical approach to predicting DDOS, in WSN areas, there are lack of provision of the variability of the transmission behavior leading to with high degree possibility of DDOS occurrences.

The existing solution to DDOS on WSN lies with the use of intrusion detection techniques [4]. Some of the techniques are based only on unauthorized access detections, while others are prevention based, and others deal both with detection and prevention of security attacks. Many institutions and trading entities have been using these approaches for many years to defend themselves from any attack on that medium.

In a typical implementation of WSN in monitoring system, like in healthcare applications where wireless sensor for a patient monitoring are in a network. It is clear that different body sensor nodes are used to capture information that are in a form of signs indicating either blood pressure or body temperature and any details required for monitoring the real-time data of the patient and coordinating with Doctors at anywhere [5]. This re-place the conventional approach for which Doctors collect patient's data directly. Even if the doctors are not there they can still get patient information from the sensor nodes of the patient via the sensors of the health service provider. This allows physicians to receive reports of an emergency in real time via the sensor nodes of a patient in the network. Physicians can reply and immediately send medical feedback. Unfortunately, in this event, DDoS attack can be devastating, that is, if attackers can attack the WSN system that required an immediate feedback for health monitoring will lead to a state of being in a life or dead situation [6]. There are many approach for defensive mechanism of WSN DDOS attacks. The crucial once lies with the use of Machine Learning techniques [7]–[12]. It was also found that supervised learning techniques is the optimal technique [13], [14]. A large body of research supports the use of machine learning techniques for DDoS attack detection. Among them, notable sources rely on the accuracy rate of DDoS detection [15]–[19].

It's obvious that to date there are many approaches provided for detecting DDOS at-tacks in the WSN. Unfortunately, these methods do not categorically establish DDOS relation to some particular transmission activities like ACK & PUSH or ACK Flood subject to PUSH-ACK in WSN. That is why this paper utilized an inherent prediction of reoccurrences of a large amount of spoofed ACK packets sent to deflate a target node.

While expanding the scope of the existing methodologies to include experimentation, this research takes special care to make sure that the approach is developed under IEEE 802.15 standard. Hence the objectives of the current study are: To design and build a network of untethered driver-less wireless sensors with a programmable GUI controller. To investigate the transmission threshold at which DDOS could occur. To analyze the transmission sessions behavior associated DDOS element. That is why ACK & PUSH ACK Flood on DDoS-PSH-ACK in WSN reoccurrences for large amount of spoofed ACK packets sent to deflate a target node will be evaluated.

II. RELATED WORK

WSN security is crucial, one of the security area that affects WSN is DDOS as de-scribed in section 1 above. It is obvious that Intrusion detections systems plays a huge part in preventing DDOS on a conventional network. But in WSN, that not been greatly discussed. In some organizations a hardware intrusion detection system is used as opposed to a software program that was mainly fairly available for intrusion detection. Likewise, it is expectable that the DDOS solution could be provided for both the software and the hardware intrusion detection system. This is not actually the case because Intrusion detection systems for Network-based are developed with different features as compared to those for Host-based. In connection with DDOS attacks, which depend only on a payload and encapsulating header, the intrusion detection system inspects the packet headers for unnecessary attributes. Previous WSN and DDOS research has demonstrated some huge amounts of important findings in artificial intelligence detection of DDOS. Crucial to this, was a reports in Al-Naeem *et al.* [8], which applies machine learning to detect DDOS, Meti *et al.* [9] reveals that ANN and SVM provide 80% detection accuracy and 100% precision values for DDOS. Similarly, Tang *et al.* [10] reveals that combining Naive Bayes, SVM, Decision tree and Deep neural network generate a huge detection accuracy and precision of DDoS attack. In the same approach, SVM alienation with wavelet kernel function have been utilized and it shows a good performance accuracy [11]. The results of the studies are based upon the fact that AI techniques generally improve performance and are reliable for WSN detection attacks [12].

Barki *et al.* [13] generalized the groups of machine learning for both supervised and unsupervised learning techniques as an optimal in which supervised learning techniques was reveals to perform better than unsupervised learning techniques. Computational efficiency matters in the detection of DDOS, that is why a lightweight detection technique for detection of DDoS attack was proposed to be associated with Management Information Base in SVM in order to have a high detection accuracy as well as the good computational efficiency [14]. Substantial body of research acknowledge the use of machine learning techniques for detection of DDoS attack. Notable sources among them relies on the accuracy rate of DDoS detection. These studies dwell on using the ANN technique and it was reveals that 99.98% accuracy of detection was obtained [15]. Furthermore, other research found 98.0% and 95.0% accuracy [16]. Other research dwells on the other performance measures on the performance of SVM where more than 95.0% where obtained in [17]. Among the approach a lot of the recent studies on WSN and DDOS. Upadhyay *et al.* [18] propose a sort of different approach for preventing WSN from DDOS attack. Their approach dwells on utilizing dynamic source routing, which is attributed to reduce energy consumption on various nodes. On the other hand, Segura *et al.* [19] reveal another light-weight but very efficient DDoS attack detection techniques associated with change point analysis. The techniques upon evaluation has demonstrated a high detection rate and linear computational complexity.

It's obvious that to date there are many approaches provided for detecting DDOS at-tacks in the WSN. Unfortunately, these methods do not categorically establish DDOS relation to some particular transmission activities like ACK & PUSH or ACK Flood subject to PUSH-ACK in WSN. That is why this paper utilized an inherent prediction of reoccurrences of a large amount of spoofed ACK packets sent to deflate a target node.

When comparing the differences in the relevant work presented in Table 1, it is clear that the majority of the work is based on Machine learning, specifically, all of the methods rely on detection performance. One of the key benchmarks used in those studies was the percentage of accuracy of DDOS detections. The differences between the two studies can be noted in those areas. To make a final assessment of the research presented in Table 1, it can establish that most of the work published that uses various algorithms and specifically, all those algorithm employ detections.

TABLE 1. Summary of empirical studies.

Author(s)	Methodology	Key Findings
Al-Naeem [8],	Conceptualized ML for detecting DDOS	Numerous machine learning techniques are capable of detecting high rate of DDOS
Meti et al. [9]	Use ANN and SVM for DDOS detection	Provide 80% detection accuracy and 100% precision values for DDOS
Tang et al. [10]	Combined Naive Bayes, SVM, Decision tree	Generate a huge detection accuracy and precision of DDoS attack
Yang and Wang [11]	SVM alienation with wavelet kernel function	Achieved a good performance accuracy
Barki et al. [13]	Compared supervised and unsupervised learning	Supervised learning techniques perform better in DDOS detection
Yu et al [14].	A lightweight detection technique of DDoS.	High detection accuracy as well as the good computational efficiency
Ahanger, [15]	Used ANN technique	99.98% accuracy of DDOS detection was obtained.
Saied et al. [16]	Used ANN to detect DDoS in real time environments	Found 95.0% accuracy of detection.
Al-Issa [17].	Used decision trees and SVM	Decision trees technique achieved better (higher) true positive rate
Upadhyay et al. 18]	Used dynamic source routing (DSR) for DDOS attack.	Energy of concerned nodes has been used for detection with routing
Segura et al. [19]	Light-weight DDoS attack detection	Evaluation shows a high detection rate and linear computational complexity

III. METHODOLOGY

The research design for the current study is presented in Figure 2. An experimental analysis involving scenarios developed for some set of WSN were performed. A graphical user interface (GUI) was developed for node accessibility. The GUI serves as a controlling resources for all the sensor nodes. The connection of the devices with the software program is by using a Bluetooth connection. While the

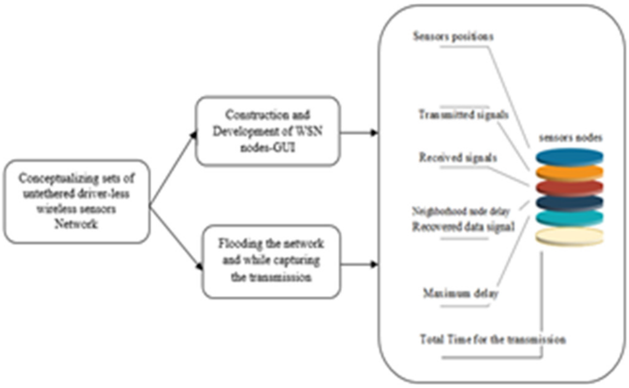
Conceptualizing sets of untethered driver-less wireless sensors Network
Construction and Development of WSN nodes-GUI
Flooding the network and while capturing the transmission
Sensors positions
Transmitted signals
Received signals
Neighborhood node delay
Recovered data signal
Maximum delay
Total Time for the transmission
sensors nodes

FIGURE 2. Conceptualization of the research approach.

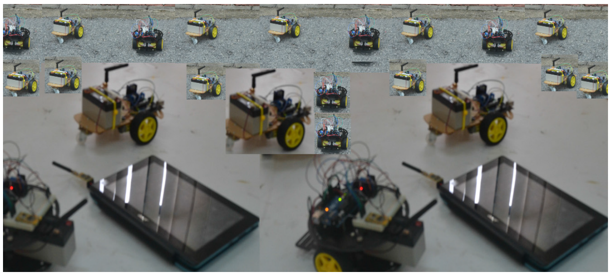

FIGURE 3. The wireless sensor nodes and cluster head in the WSN adopted for this study.

connection between the device nodes are established with 433 MHz radio frequency (RF), and HC-12 transceiver. The wireless sensor nodes in a WSN adopted for this study are presented in Figure 3. Each sensor node is a constructed-couples of sets of untethered driver-less unit in a network control by a cluster head (a tablet computer) established with wireless backbone. The tasks in the network are related to transmitting information that includes the location of all the sensors nodes within the networked environment, the battery levels of each unit, their speeds, the current operation status.

Each sensor node can be able to transmit signals to any specific sensor node or all them at once. The cluster head control is the tablet computer with a communication module and each sensor note is also fitted with a communication module. The tablet computer is the central communication unit where it manages the communication with and between all other sensor nodes.

The reason for adopting this approach is to determine when a new connection requests are sent to a sensor node at which certain time does it get overwhelmed? Typically, in a synchronize flood, an intruder doesn't complete connection request. A huge weakness of working in shared media is that any wireless antenna can completely block transmissions for the entire network by repeatedly transmitting join requests. The experimental analysis involves flooding the network from the programmable interface in the tablet computer to all other while capturing the transmission activities. This continues in series of bursting the flow of the data signal as presented in Table 2. The table is labelled with *S* "representing sensors nodes", *SP(m)* representing "sensors positions in meters", *Tx(kb)* to be representing "transmitted signals in kilobits", *Rx(kb)* to be representing "received signal in kilobits", *Ts(sec)* to represent "the Total Time for the transmission in seconds", *Md(ms)* to represent "Maximum delay in milliseconds", *Mn(ms)* to represent "Minimum delay in milliseconds", *Dn1(ms)* to represent "Neighborhood node delay in milliseconds" *Dn2 (ms)* to represent "the second order delay in milliseconds", *Dn3 (ms)* to represent "the third order delay in milliseconds", *Ls(kb)* to represent "the lost data signal in bytes", and *Rs(kb)* to represent "the Recovered data signal in kilobytes".

There was careful consideration given to make sure that all the sensors be interconnected with each other and with the cluster heads so they can exchange information. If a signal is captured from the session, all of those being sent will then be shown on the capture programme. The research then discovered that there are delays in the order of transmissions from different location, as well as in the time in which a signal arrives, a destination. The time delays were increased for each repeated sensor readout in order to coincide with the sensor positions.

The transmission behaviour of the network is such that the second order delay is at the minimum of 23 milliseconds within a set of sensor positions. This has highlighted how easily DOS or DDOS attack can be detected within the network. That is any traffic with some behavior that goes above the transmission session captured. Expectedly, if signals are transmitted over certain distance in the first round, then changing sensors nodes location might lead to either the increase in distance until transmission distance of the transmitted sensor nodes exceed ranges, where delays will be recorded as the transmission continues. achievable.

The experimental approach used for the detection of DDOS is set to select the most efficient feature sets that are as the consequence of the DDOS attacks. In this case the situation that we found at hand is a classification problem. That is to classify those features that are indicating the responses of all the attributes of DDOS.

IV. ANALYSIS AND PRESENTATION OF RESULTS

The test scenarios are based on the same parameters as Table 1. The transmission detects faults while maintaining distance of 25ms at about 970 metres. Since the advertised distance for the transmitter was 1 km, after a few tests, the necessary delay showed 25 milliseconds. However, the only thing revealed was that even if the transmitter is able to reach approximately 1 km, not all data reaches successfully when the delay varies. Thus, from that distance we went down. It is also important to note that at this point, when we achieved the optimum transmission delay of 25 milliseconds, no change was needed for successful transmission although the distance has changed.

TABLE 2. Traffic flow within the transmission session.

	SP	*Tx*	*Rx*	*Ts*	*Md*	*Mn*	*Dn₁*	*Dn₂*	*Dn₃*	*Ls*	*Rs*
Nodes	*(m)*	*(kb)*	*(kb)*	*(sec)*	*(ms)*	*(ms)*	*(ms)*	*(ms)*	*(ms)*	*(kb)*	*(kb)*
S1	1.5	320	73	23.502	276	47	280	18	266	62	5.944
S2	1.5	320	265	25.602	290	53	83	23	64	62	17.08
S3	1.5	320	405	27.576	53	52	60	28	36	62	25.2
S4	101	320	405	27.583	55	56	60	28	36	62	25.2
S5	971	320	107	12.47	1354	49	77	28	53	62	7.916
S6	661	320	405	27.587	56	55	60	28	36	62	25.2

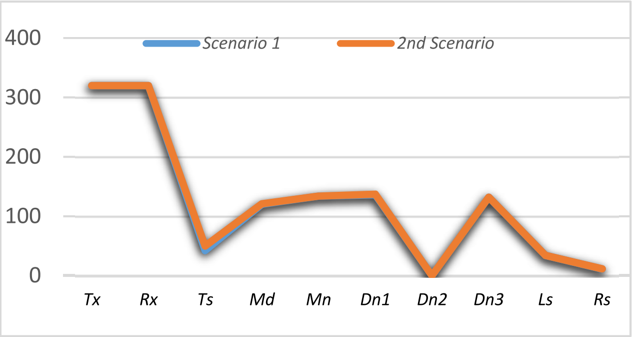

FIGURE 4. Normal transmission within sensor nodes and cluster head.

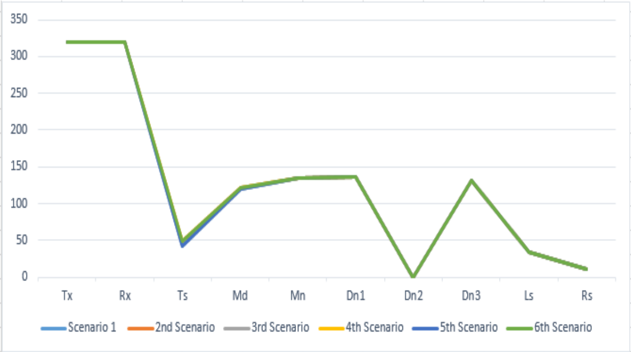

FIGURE 5. Transmission and retransmission scenarios within the sensor nodes and cluster head.

These experimental test yielded successful results at the distance obtained out of the eight experiments that were undertaken. Those key distances identified are 0.5 meter and 660 meters, hence, these are suitable distances for testing the atom tablet as a master node. The results are almost identical to the results obtained with the high performance processor.

A. FLOODING THE TRANSMISSION SESSION

The flood attack from DDOS burst generate enormous volumetric signal data in the entire sensor node in the network to overwhelm the targeted node. In the case of signal data reaching either the cluster head or other nodes, the software program has captured the transmission processing session. In the same way, there has been a slight change in the overall time of all transfers, compared to the transmission that involves many delays over a different distance and no delays. The difference in load and transmission length may be the reason for this. There is no need to set a threshold for this approach.

After these few tests, the transmission of data for all the nodes was conducted. Scenario-by-scenario experiments were carried out. That is to flood the signal data from 320 bytes and increase the size and location of sensors. The time when transmission changes sign has been determined. The first experiment comprises two scenarios with all sensor nodes and the head of the cluster. Data signal have been sent within 3 nodes, with an approximate distance of 2 m from the cluster head. This has led to 229 transmissions and a total signal data of 320 kb, each as the transmissions do not exceed the maximum data capacity that the channel can carry. The flow is therefore not observed delay in two scenarios (See Figure 4).

Considering six scenarios with the same transmission session, but only retransmits another signal upon received, in order not to overwhelmed with a continuous string before processing successfully, some difference output was captured (see Figure 5). The results indicate that the average signal data received is similar to the data sent (see Figure 5).

The flooding of the transmission was carried out with same six scenarios. The transmission session was flooded the multiple signals data across the entire connections. At this point each sensor node is sending, that means the transmission session was intentionally set out to be overwhelmed with a continuous string for processing (see Figure 6). It can be seen that in each scenario there is a spike in of signal data, however transmission continues.

B. EXCESSIVE FLOODING THE TRANSMISSION SESSION

After transmitting relatively, the size of signal data within the capacity of the sensors nodes, the experiment further floods the transmission session with excessive signal data in order to examine the effect of DDOS attack. However, the experiment in this part was carried out in series. Starting with scenario one to scenario six, by increasing size of the signal data send (see Figure 7).

During the previous test cases, the data stream had a moderate rate of smoothness; however, with this test case the flow expanded dramatically within the same time frame. That is continuous transmission flooding the session. Even though it

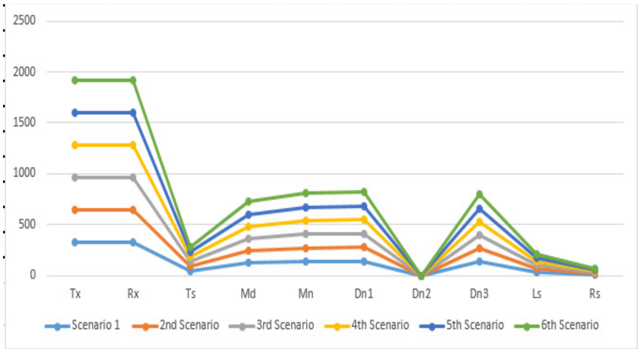

FIGURE 6. **Sensor nodes and cluster head transmitting at same time.**

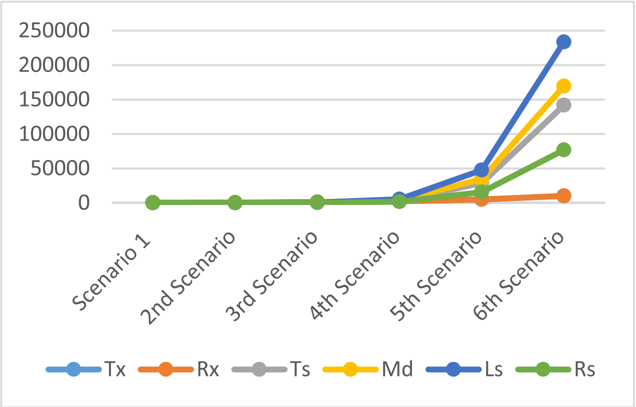

FIGURE 7. **Sensor nodes and cluster head transmitting with different signal sizes in series of the scenarios.**

was revealed that the most ideal delay between transmissions is 23 milliseconds in order to ensure that the receiving end is not overwhelmed by the previous experiments, this current experiment goes beyond that.

This transmission type is particularly works well for scenarios that need a large amount of data, but also works for scenarios where a large amounts of data are required. TCP creates many parts out of significant data to provide segments for broken or unreliable connections, and identifies them by using the required sequence numbers, thus permitting full functionality of the network resources to be allocated for just one large amounts of information. There must also be an exception to the requirement of transmission speed. In this case, the time lag must be considered when it is possible to transmit at speeds that do not use TCP protocol. That 23 milliseconds may or not be significant depending on whether a high performance is needed in this transmission is the criteria. This is why the first, second, and third order d-delays are given special consideration in this research. Thus, an overwhelmed transmission channel can be effectively evaluated by flooding the transmission session with traffic or through deliberate channel congestion.

Following the argument presented for determining when transmission session get overwhelmed. The six scenario parameters for this study were used by the previous experiment and transmission was flooded further in order for the DDOS flooded attribute to be extracted. Taking into account the flow of the created scenarios, each node in the send to each node. We then use the captured programme to check the transmission session's behavior. The total transmission and the transmission delay was found to be very high between transmissions. This is important as we can now conclude on this type of transmission. The transfer stopped immediately after the delay reached a peak (see Figure 8). It is important to note that this technique and the captured values are for transmitters in all the scenarios used to minimize transmission time under 433 MHz and to maximize transmission time.

Certain performance assessment measures have been applied to the recorded data in order to measure or determine the accuracy of transmission sessions capture data. The data has been transformed (normalization) to scale the range of values within a uniform scale in order to improve the quality of the evaluation [20]. These measures has been used with four traffic conditions options, which allow intrusion detection system to detect intrusion successfully [21]. Hence the parameters below have been found prominent for performance evaluation measures: [22]

- True Positive (TP) represent the amount of transmission sessions capture data that are properly classified on all the scenario. That is the amount of transmission on all sessions send is considerable
- True Negative (TN) is the amount of transmission sessions capture data that are correctly rejected from the entire transmission sessions capture data. That is the percentage of transmissions captured data that are of the class whose contents cannot be identified and recorded.
- False Positive (FP) represent the amount of transmission sessions capture data that are wrongly rejected from the form the entire transmission sessions capture data. That is the number of transmissions sessions capture data that are discarded and does not accurately reflect the actual quantity being transmitted.
- False Negative (FN) is the amount of transmission sessions capture data that are wrongly classified to the correct transmissions sessions capture data. That is the amount of transmission sessions data that incorrectly classify to the correct once.

In addition to the parametric definitions, a series of corresponding metric values were calculated: accuracy, precision, recall, False Accept Rate (FAR). Based on those measures, the metrics may be defined as deduced as follows:

Accuracy (PA) calculate the amount or percentage of data that is being captured according to transmission sessions. That is how much of the data from each transmission to include in the session records defined by equation (1).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \tag{1}$$

While the concept of accuracy is based on making a guess and then testing that guess, the Precision edition adds the ability to double-check the results. It's a straightforward metric

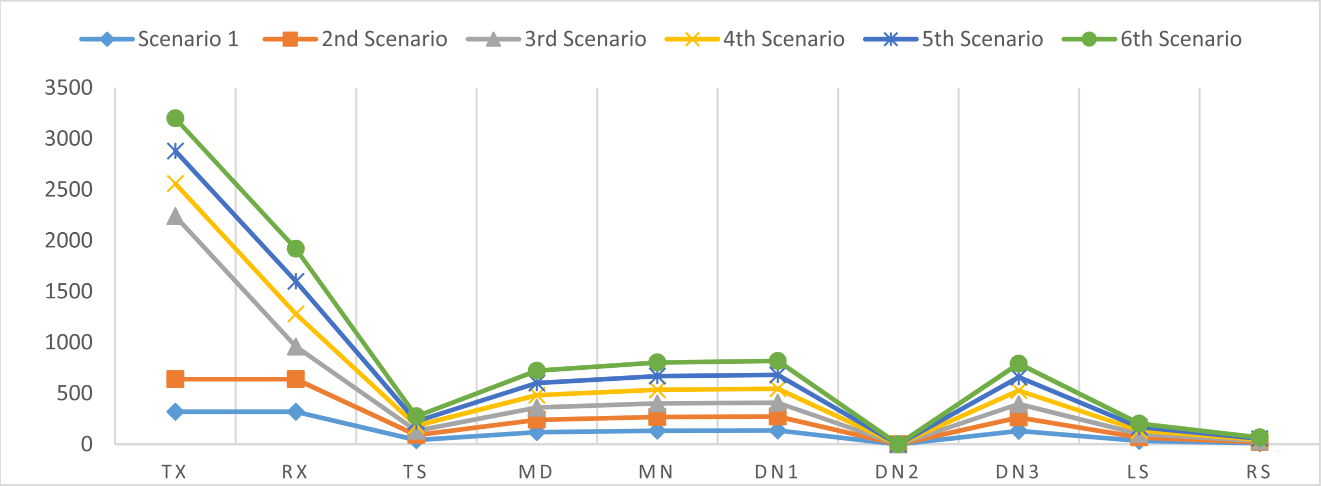

FIGURE 8. Maximum signal data send over sensor nodes and cluster head transmitting with different signal sizes.

that calculates the fraction of the time for which the correct outcome is returned. That is, it is a quality that improves the amount of information that can be acquired. Accurate cases comprise 100% of the amount of "outcome" and precision is a simple measure that calculate the portion of cases where the correct result is returned. It is calculated by using equation (2).

$$Precision = \frac{Tp}{TP + FP} \times 100\% \tag{2}$$

In the experimental analysis the real transmission sessions captured data is the mean difference between inaccurate and correct predicted data, not just the absolute amount of forecasted data, therefore, the rate of detection of real transmission sessions capture data is called Recall which is also called Detection Rate (DR). It is calculate by equation (3).

$$DR = Recall = \frac{Tp}{TP + FN} \times 100\% \tag{3}$$

FAR is the proportion of detection cases in which incorrectly transmission session captured data are incorrectly accepted? This means that a false acceptance is indicated if an inaccurately amount of data from transmission sessions is accepted as valid. It is computed by the false detection rate of the data and evaluated by equation (5).

$$\text{FAR} = \frac{FP}{FP + TN} \times 100\%. \tag{4}$$

Parameters for each of the six experimental scenarios used are validated. These include the flooding of the transmission session by "Normal Transmission" within sensor nodes and cluster head. The "Transmission and Retransmission" within the sensor nodes and cluster head, as well as the transmission of the "Sensor nodes and cluster head" at same time. The transmission of different signal sizes is linked to the observed delays. Hence the validation results of the captured data indicate that the best result comes at a transmission of the Sensor nodes and cluster head within the same time at 23ms delay. It generates the highest detection accuracy of 94.62%, for the successful transmissions rate that are correctly detected (TP = 11520, TN = 101, FN =451, FP =210). The precision is 98.21% and the recall is 96.23%, while false acceptance rate is 67.52% and false rejection rate is 68.22%.

V. DISCUSSION

This paper presents the actual tests for examining how WSN get overwhelmed, in such a way that all the threats behaviors associated to DDoS attack can be evaluated. Typically, DDOS attack can be launched at the time where a certain group adversary activity is coordinated. In most instances the area where the attacks occur is difficult to determine, but most of the attacks are due to a large number of volumetric traffic details being sent to overwhelm them. The attack is common in the apply on the Internet and it causes a lot of damage to online transaction. In some cases, the attacked might not be intentionally applied, but cases like registrations that supposed to end at a certain due date, and if majority of the people wait for last minutes, they will tend to overwhelmed the Internet with large amount of transactions traffic towards the server, which will eventually get stocked. This is also treated as a security issues, and should be taking seriously.

In terms of WSN, it is not different, because both the Internet and WSN approaches provided to ensure necessary security measure for preventing the security attacks is important. Some techniques will also emerge every time a new threat arises. However, based on detections of any of security associated with authorization it is not critical but others that strictly for preventions, while some are basically dealing with both detection and preventions of any security attacks. The techniques for this research rely on techniques for various practical applications of WSN. It is widely used in many places now, like the installation of surveillance cameras.

The details of the problems are mostly monitored in the environment where a typical implementation for WSN is carried out. This study has resulted in successful findings, through which the distance is appropriate to determine how signal data are shared over a connection. Similarly, like with a sensor for patient monitoring, this is an important network environment that must be designed so as not to become overwhelmed. The impact of such a network environment is that the traditional system approach in hospitals is re-established. Although the network is still vulnerable to attacks, with such a promise. This is why DDoS studies are required. The results of this study showed that the DDOS can be devastating in WSN. It has also indicated that the easiest thing to do is overwhelm the systems if attackers can attack WSN systems that require an immediate feedback. Blowing the system will lead to a system crash. It may not be for the network resources only.

The result of the current study also highlighted when transmission session gets overwhelmed and the factor influencing the DDOS success. The main contribution of the paper is predicting DDoS attack by variability of transmission behavior with high degree accuracy. It was established that the most ideal delay between transmissions is 23 milliseconds in order to ensure that the receiving end is not overwhelmed. It was discovered that flooding transmission is associated to the flow of the network scenarios created, every node in the send to every node. Similarly, it is also related to the behavior of the transmission session. That is the entire total transmission session and delay in between transmission is crucial in terms of the security of the WSN. Furthermore, transmission behavior that leads to delay can cause crash that is why it is important to consider.

The future work of this current research focuses on issues related to some critical aspects of DDOS, specifically in the part where bursting the sensors network was not the issue, rather, it might be infecting the sensors with a specific attribute, for example, Thomas *et al.* [23] draws attention to one type of DOS attack known as a ''denial of sleep attack,'' which is defined as a type of DOS attack where the goal is to keep the target sensors awake. While this research focuses on predicting DDOS deflation of a target WSN node, future research should go on predicting infecting network's sensors to go into a ''sleep'' condition. Another future path should be to predict DDOS attacks on WSNs using well-planned procedures, because it has been shown that using a pattern discovery approach with a trusted model allows for earlier identification of adversaries who follow specific attack patterns [24]. As a result, predicting the pattern of how DDOS would infect sensors in WSN could be extremely beneficial to the field of WSN. Finally, it's worth noting that the use of fully-connected sensory environments is gaining traction in a variety of fields and research, is progressively giving solutions to the problems that they confront. A good example is the ''intelligent transport system'' [25], therefore future research should look at the prediction of DDOS attracts in the most widely used WSN.

VI. CONCLUSION

This study is on WSN has undertaken an experimental analysis for determine the effect of DDOS in WSN. The paper has been able to determine the current issues and challenges of security of WSN, specifically related to the DDOS attack. It has also highlighted the transmission issues associated to overwhelming transmission session of WSN and the factor influencing the success of DDOS attack. This typically a major constraint realizing that DDOS can be a possible even unintended applied. That is solving security issues as applied to WSN can a major problem since it can emerge unintended. An experimental analysis was carried out and occurrence and reoccurrences of generating large amount of data is a feature of any network. The finding shows that the proposed approach is able to detect DDoS attack with high degree accuracy. The main contribution of the paper is predicting DDoS attack by variability of transmission behavior with high degree accuracy. The network requires approximately 23ms between transmissions in order to allow the end receiver to handle the information received with no distortion, which is considered to be the most ideal delay

REFERENCES

[1] Z. Yu and J. J. P. Tsai, ''A framework of machine learning based intrusion detection for wireless sensor networks,'' in *Proc. Int. Conf. Sensor Netw., Ubiquitous Trustworthy Comput.*, Jun. 2008, pp. 272–279.

[2] A. E. Cil, K. Yildiz, and A. Buldu, ''Detection of DDoS attacks with feed forward based deep neural network model,'' *Expert Syst. Appl.*, vol. 169, May 2021, Art. no. 114520.

[3] S. D. Çakmakçı, T. Kemmerich, T. Ahmed, and N. Baykal, ''Online DDoS attack detection using mahalanobis distance and kernel-based learning algorithm,'' *J. Netw. Comput. Appl.*, vol. 168, Oct. 2020, Art. no. 102756.

[4] G. M. Borkar, L. H. Patil, D. Dalgade, and A. Hutke, ''A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept,'' *Sustain. Comput., Informat. Syst.*, vol. 23, pp. 120–135, Sep. 2019.

[5] S. Nashwan, ''AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment,'' *Egyptian Informat. J.*, vol. 22, no. 1, pp. 15–26, Mar. 2021.

[6] S. S. Javadi and M. A. Razzaque, ''Security and privacy in wireless body area networks for health care applications,'' in *Proc. Wireless Netw. Secur.* Berlin, Germany: Springer, 2013, pp. 165–187.

[7] M. Zekri, S. E. Kafhali, N. Aboutabit, and Y. Saadi, ''DDoS attack detection using machine learning techniques in cloud computing environments,'' in *Proc. 3rd Int. Conf. Cloud Comput. Technol. Appl. (CloudTech)*, Oct. 2017, pp. 1–7.

[8] M. Al-Naeem, M. A. Rahman, A. A. Ibrahim, and M. M. H. Rahman, ''AI-based techniques for DDoS attack detection in WSN: A systematic literature review,'' *J. Comput. Sci.*, vol. 16, no. 6, pp. 848–855, Jun. 2020.

[9] N. Meti, D. G. Narayan, and V. P. Baligar, ''Detection of distributed denial of service attacks using machine learning algorithms in software defined networks,'' in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Udupi, India, Sep. 2017, pp: 1366-1371.

[10] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, ''Deep learning approach for network intrusion detection in software defined networking,'' in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Fez, Morocco, Oct. 2016, pp. 258–263, doi: 10.1109/WINCOM.2016.7777224.

[11] M. Yang and R. Wang, ''DDoS detection based on wavelet kernel support vector machine,'' *J. China Univ. Posts*, vol. 15, pp. 59–63, Sep. 2008.

[12] O. G. Matlou and A. M. Abu-Mahfouz, ''Utilising artificial intelligence in software defined wireless sensor network,'' in *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Beijing, China, vol. 1, Oct. 2017, pp. 6131–6136.

[13] L. Barki, A. Shidling, N. Meti, D. G. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software defined networks," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Jaipur, India, Sep. 2016, pp. 2576–2581, doi: 10.1109/ICACCI.2016.7732445.

[14] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," *Comput. Commun.*, vol. 31, no. 17, pp. 4212–4219, Nov. 2008.

[15] T. A. Ahanger, "An effective approach of detecting DDoS using artificial neural networks," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Chennai, India, Mar. 2017, pp. 707–711.

[16] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016.

[17] A. I. Al-issa, M. Al-Akhras, M. S. ALsahli, and M. Alawairdhi, "Using machine learning to detect DoS attacks in wireless sensor networks," in *Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol. (JEEIT)*, Amman, Jordan, Apr. 2019, pp. 107–112.

[18] R. Upadhyay, U. R. Bhatt, and H. Tripathi, "DDOS attack aware DSR routing protocol in WSN," *Procedia Comput. Sci.*, vol. 78, pp. 68–74, Jan. 2016.

[19] G. A. N. Segura, S. Skaperas, A. Chorti, L. Mamatas, and C. B. Margi, "Denial of service attacks detection in software-defined wireless sensor networks," 2020, *arXiv:2003.12027*. [Online]. Available: http://arxiv.org/abs/2003.12027

[20] A. I. Abubakar, H. Chiroma, and S. Abdulkareem, "Comparing performances of neural network models built through transformed and original data," in *Proc. Int. Conf. Comput., Commun., Control Technol. (I CT)*, Apr. 2015, pp. 364–369.

[21] N. Mohd, A. Singh, and H. S. Bhadauria, "A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks," *Wireless Pers. Commun.*, vol. 111, no. 3, pp. 1999–2022, Apr. 2020.

[22] H. J. Choi, H. Lee, and J.-Y. Choi, "Is a false positive really false positive?" in *Proc. 23rd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2021, pp. 145–149.

[23] D. Thomas, R. Shankaran, Q. Z. Sheng, M. A. Orgun, M. Hitchens, M. Masud, W. Ni, S. C. Mukhopadhyay, and M. J. Piran, "QoS-aware energy management and node scheduling schemes for sensor network-based surveillance applications," *IEEE Access*, vol. 9, pp. 3065–3096, 2021.

[24] R. H. Jhaveri and N. M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," *Int. J. Commun. Syst.*, vol. 30, no. 7, p. e3148, May 2017.

[25] S. Verma, S. Kaur, A. K. Sharma, A. Kathuria, and M. J. Piran, "Dual sink-based optimized sensing for intelligent transportation systems," *IEEE Sensors J.*, early access, Jul. 28, 2020, doi: 10.1109/JSEN.2020.3012478.

MOHAMMED ABDULAZIZ AL-NAEEM (Member, IEEE) received the B.Sc. degree in CIS from the College of Management Science and Planning, King Faisal University, in 2005, and the M.Sc. degree in networks and communications (specialized in information security) and the Ph.D. degree in networks and communications (specialized in wireless networks) from Monash University, Australia, in 2009 and 2015, respectively. He is currently the Chairman of the Department of Computer Networks and Communications, King Faisal University. His research interests include wireless networks, network security, machine learning, artificial intelligence, and pattern recognition.