I. J. Computer Network and Information Security, **2019, 11, 1-13**
Published Online November 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.11.01

Active Defense Strategy against Jamming Attack in Wireless Sensor Networks

Nawfal F. Abdulqader AL-Shaihk
Computer Engineering Department, Cankaya University, Ankara-Turkey
E-mail: nsau93@gmail.com

Reza Hassanpour
Computer Engineering Department, Cankaya University, Ankara-Turkey
E-mail: Hassanpour.reza@gmail.com

Received: 18 September 2019; Accepted: 28 October 2019; Published: 08 November 2019

Abstract—Wireless Sensor Networks WSNs are being utilized increasingly nowadays due to their ability to collect data from stationary, moving, reachable or unreachable fields. Progressive developments in WSN techniques add efficiency, reliability and better power management possibility, but they are still vulnerable and sensitive to security threats. The most effective threat to WSN is DOS attacks, which are detectable but in many cases unpreventable yet. An authentication-based defensive approach against DOS attack combined with jamming attack that prevents transferring data between attacked nodes in a cluster and cluster head node is proposed in this study. The proposed method encompasses developing an algorithm with ability to bypass attacked path via alternative safe one under control of cluster head to mitigate the False Node Excluding DOS due to jamming attack. The proposed method has been experimentally tested against similar methods from the literature with arbitrary study cases. Our proposed algorithm shows promising results in mitigating False Node Exclusion DOS (FNEDOS) attack where a full recovery of the attacked node is achieved in case of isolated nodes, and improvement between 36% and 52% is obtained when the attack affects a group of nodes at proximity.

Index Terms—Wireless Sensor Networks (WSN), False Endorsement DOS (FEDOS), Denial of Service (DOS), False Node Exclusion DOS (FNEDOS), Jamming Attack.

I. Introduction

Due to widely utilization of WSNs, they face several challenges that affect their efficiency and lifetime. Some of these challenges are deployment, reliability, routing and monitoring, programmability, power supplying and security [8]. Security is the most significant challenge due to its relation with securing collected data and transmitting it between nodes. Therefore, data protection against outsider and insider adversaries or attacks is the most significant issue among others. The most dangerous and unpreventable attack is Denial of Service (DOS) attack due to its ability to use different techniques to suspend or reduce the effective functionality of nodes. In this study, a method is proposed to defend WSN against certain types of DOS attacks namely jamming attack, and mitigating its effect even if it is still attacking the communication channels between the sensor nodes and the cluster heads.

DOS attack aims to disturb either the node functionalities or data transmission channels to prevent nodes from providing services or communicating with each other. One type of these DOS attacks is a jamming attack. Krauß et.al. propose a method as an authentication defense against false endorsement DOS attack based on creating a gray-list [22]. In their method, cluster head (CH) generates a report about occurrence of a certain phenomenon and broadcast it to all corresponding cluster nodes asking their endorsement on the generated report. Cluster nodes (CN's) check phenomenon time stamp and occurrence of phenomenon itself. If verification process passes, an endorsement is generated and forwarded to the CH, which authenticates the endorsing node. Endorsements from CNs are accepted unless an error occurs with endorsement message, in such a case, node grey-listed and CH waits until CN resends the same message as a proof for its last endorsement. In this case CN is trusted again and removed from the gray-list. If proof message is delayed or prevented, CH excludes CN from further endorsements while CN is still functioning correctly. The above-mentioned delays and preventions can be due to jamming attacks, which can put part of the network out of work.

Excluding functioning nodes after one iteration of failure in resending proof for the last endorsement makes WSN lose innocent nodes. In addition, it is necessary to provide alternatives to defend against this pitfall especially when jamming attacks last for a long time. I addition, the node under attack is not informed that its endorsement was not delivered.

In this paper, an algorithm is proposed to prevent excluding well-functioning innocent nodes by utilizing the communication capabilities of the neighboring nodes around the node under attack. This algorithm delivers delayed or blocked endorsement from attacked nodes via multiple paths. The proposed method has been experimentally tested against similar methods from the literature with arbitrary study cases. More specifically we have considered the method proposed by Krauß et.al. [22] to verify the performance of our algorithm.

The remaining of this paper is organized as below:

Section (II) introduces the security issues in WSN Security and attack types. Section (III), presents the related works about mitigating DOS attacks. In Section (IV) we introduce some algorithms to prevent false endorsement. Section (V) provides the details of our proposed active defense strategy. Section (VI) presents testing and analyzing results. In Section (VII) we draw our conclusion and suggest the possible future directions.

II. WSN Security and Attacks

Security presents one of the most challenging issues in WSNs besides other issues such as sensor deployment, scalability, energy efficiency, computational power and QoS (Quality of Service). WSNs, in addition to the security threats in traditional networks, are exposed to extra kinds of security challenges due to the wireless nature of their connectivity. Wireless broadcasting of collected data lets adversaries to intersect the transition frequencies illegally and remotely. Moreover, the deployment of sensors in open wide areas gives the possibility to the attackers to interact directly with the sensors to take codes, ciphering keys, passwords and so on. These vulnerabilities of WSNs have motivated researchers to develop techniques to mitigate attacks on WSNs [12, 13]. In this section we provide a brief overview of the WSN security. However, it should be noted that main concentration of this research is mitigating attacks occurring at the physical layer. Overall, WSN security measurements should meet several requirements as described below [15, 16, 17].

A. Security Requirements

The proposed solutions for mitigating security threats should have the following characteristics:

Availability

As mentioned before, WSN normally deployed in either friendly or adversary ambient and in both cases, it is needed to keep the WSN services and collected data available for authorized sink nodes. In other words, WSNs should be protected against DOS attack [12].

Integrity

WSNs transmit data wirelessly from node to another until it reaches the sink or the head of the cluster node. Hence, it is more likely that the data is modified during transmission. Integrity protects transmitted data from any malicious modification through transmission process [13].

Confidentially

Only intended nodes should understand transmitted data. In other words, it must be guaranteed that the transmitted data are hidden from adversary nodes.

Freshness

The main purpose of WSN is to collect data and transmit it to the main station. This implies that timing is a significant issue especially in sensitive applications such as military or health care. In such cases, delay in delivering data imposed by malicious adversaries can cause loss of freshness in data. Therefore, in time data delivery is considered a security goal.

Authentication

Yet another goal of security in WSN is to prevent adversaries from injecting any additional illegal massages via legal WSN transmission channels. The receiver node must make sure that received data comes from true and authenticated nodes.

Access Control

Participant nodes within a WSN must have the ability to utilize the communication facilities of the network however, access to these facilities should be denied for foreign nodes. Accordingly, massages that belong to foreign WSN's must be detectable.

Non-repudiation

WSN nodes should not neglect to transmit any received message to the next hop.

B. Attack Types on WSNs

WSN's face different types of attacks due to the variety of purposes behind attacking WSN's. WSN attacks can be classified into several categories as illustrated below.

a. Passive attacks

Some of the attacks are limited in listening to transmission channels in order to analyze transmitted data and extract useful information such as detecting which node serves as the head of a cluster. These kinds of attacks are extremely difficult to detect because there are no activities or modifications applied to originally transmitted data. These kinds of attacks usually occur before active attacks, which are the second category of attacks.

b. Active Attacks

In this category, the aim of the attackers is to remove transmitted data, modify them, inject fake information, replay old information, mimic legal nodes, and/or cause a denial of service in a certain WSN. In this category, the most significant active attacks can be listed as, tampering where attackers access the nodes physically in order to get critical information such as encryption keys or algorithms, black hole attack in which an adversary node broadcast fake routing information to make other nodes route data traffic through the attacking node. In selective forwarding the attacker which behaves like a member node simply blocks or drops certain packets instead of forwarding them. Jamming attacks where the attacker disturbs the radio transmission channels by using the same frequencies for broadcasting useless information. In blackmail attack, an adversary node declares another set of nodes as malicious nodes. An exhaustion attack happens when an adversary node passes unnecessary information to other nodes. The main idea is to exhaust the energy of the legal nodes by receiving useless information and processing them. In wormhole attack, adversary nodes placed at the boundaries of WSN area can receive or transmit information by means of tunnels. In identity replication attack, adversary node clones another legal node and acts as part of WSN to collect important information. Unlike Sybil attack, legal node and malicious node share the same ID.

III. Related Work

One of the most important attacks in WSN is a DOS attack. The significance of this attack comes from its resilience to detection. Therefore, a lot of efforts have been devoted to achieving a high detection efficiency. We categorize these methods based on their detection and prevention capabilities as described below.

Clustering and Energy Balancing Methods

The main idea of the algorithms in this category is the creation and distribution of a new type of node named Control Nodes (Cnodes) which are included within the clusters. Cnodes take the responsibility of monitoring the data traffic to detect malicious nodes. Cnode election algorithms using random-based election, energy balancing-based election and distance from nodes have been reported in the literature. The algorithms take into consideration the time periodicity of election and re-election against the timing of CH election. In [25], authors while focusing on high detection ratings of DOS attacks, provide a good energy-preserving solution. They considered the hierarchical topology clustering algorithms such as Low-energy Adaptive Clustering Hierarchy (LEACH). The detection of compromised nodes depends on electing suitable Cnodes which are responsible for monitoring data traffic in WSN. There are three methods for the election:

- Distributed Self-election,
- Cluster head-centralized election
- Base station-centralized election.

The authors proposed a Cnode to be re-elected periodically to ensure that each non-CH node has the chance to be elected. In this way, the algorithm provides a good power balancing and high detection rate under the condition that Cnode re-election period must be shorter than re-election period of CH. In [30] and [41], authors execute LEACH for multiple iterations to split the first level of clusters into sub-clusters. The node energy level is included in the cluster head election formula in level-1 which elects the node with the highest power. Higher levels sub-clusters with number of nodes more than 2 are constructed with sub CH (considered as Cnode for corresponding cluster). The LEACH iterations keep generating sub-clusters out of sub-clusters as long as the minimum node per cluster condition is satisfied. Cnodes generated in this way, are assigned to the cluster with the nearest CH from them. In this way, the algorithm achieves a higher efficiency of traffic monitoring and better DOS attack detection. However, on the other hand increasing the number of Cnodes causes higher power dissipation, an issue which has not been discussed or mentioned. Besides, LEACH algorithm gives the nodes the right to self-electing whether they are Cnode or not. This issue causes non-uniform distribution of Cnodes within a single cluster. In [42], LEACH is also used to achieve recursive clustering of WSN exactly as reported also in [30] and [41] with almost similar results. The authors, however, improved the recursive-clustering technique by using a novel clustering algorithm named Fast and Flexible Unsupervised Clustering Algorithm (FFUCA) and compare its results with LEACH algorithm. FFUCA provides an optimal solution for deploying nodes where average squared distance between Cnode and sensor nodes is calculated for 3 clusters are 136.61 for LEACH and 24.05 for FFUCA. They also provide better DOS detection. The improvements are shown in terms of false-negative f_n and false-positive f_p for both algorithms where LEACH has $f_n = 16\%$ and $f_p = 3\%$, but FFUCA manages to reach $f_n = 12\%$ and $f_p = 8\%$. In [32], for achieving highest possibility to detect DOS attacks with best energy balancing, a dynamic method is proposed to elect control nodes CN's by considering the remaining energy in each of them. LEACH algorithm is used to construct the WSN topology. CN's are responsible for monitoring the traffic between nodes and their behavior as well as preventing DOS attacks. The CN's are elected periodically based on the highest remaining energy criteria and hence, each node may be elected as a CN. This consideration may increase the lifetime of WSN however, it may make elected CN's undistinguishable from adversaries. In [33], the compromised Cnode tries to prevent being detected by showing high residual energy. *Verification Nodes V-node*s are responsible for monitoring residual energy of Cnodes and compare it against a mathematical model of expected power consumption. In order to reduce the power consumption due to monitoring process by both Cnodes and Vnodes, a Vnode is designated to a Cnode for a given time interval and after collecting enough power level recordings, the collected data is compared with a mathematical model of normal power consumption. Any abnormal expectation leads to detection of compromised Cnode and is reported to the base station.

Frameworks and Schemes Category

In this category, some schemes and methods for detecting and defending against DOS attacks were provided by arranging well-known DOS detecting and mitigating algorithms into such structures to provide high efficiency. In [19], the proposed framework is composed of attack detection and attack defense countermeasure stages. In the detection stage, some of the widely used algorithms for DOS detection are integrated together as sub-modules to detect DOS attacks in different network layers of WSN. In defense stage, various defensive methods utilized to perform the better countermeasure against detected dos attack as shown in Fig. 1.

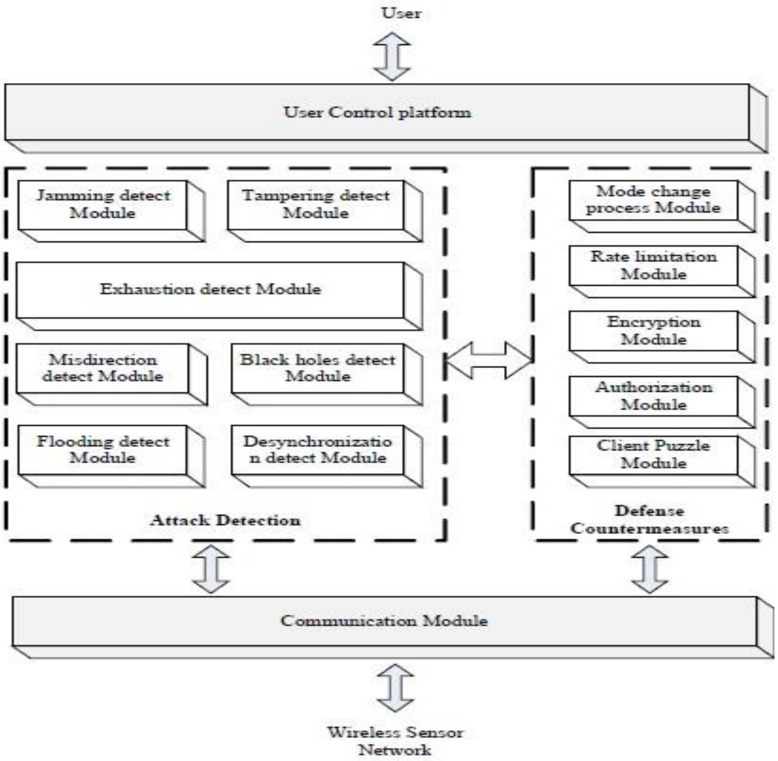


Fig.1. Architecture of detecting and defending bridge system.

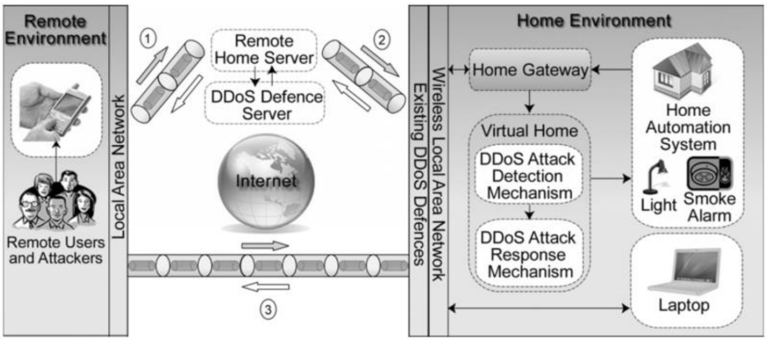


Fig.2. The proposed defense scheme against DDoS

The communication module in figure 1 acts as a real-time WSN bridge for the attack-defense system in sending and receiving packets. User control platform is designed to let users interact with the proposed system. Attack detection component consists of sub-modules working independently. Each sub-module detects specific kind of attacks where if an attack is detected the corresponding flag is set and is sent as a message to communication module. Attack defense countermeasure component receives the warning messages and activates the corresponding defense sub-module against certain DOS attacks. The advantage of this framework is the ability to add more types of DOS attack countermeasure sub-modules with high degree of flexibility. In [21] and [44], authors concentrate on DOS attacks upon WSN's in *Home Automation Systems (HAS)*. Their defense scheme targeted the low-level DOS attacks by proposing an approach consisting of three parts: Virtual Home (VH), Remote Home Server (RHS) and DDOS Defense System (DDS). The main idea of this approach is to create a virtual home stage to detect the DDoS attacks and prevent it from reaching real WSN as shown in Fig 2.

In virtual home-DDOS attack detection mechanism, end-to-end encryption is used to ensure the user's privacy unless an attacker captures the encryption key. If any adversary behavior is detected, a corresponding flag is set and a message is sent to RHS to analyze the Home Gateway message. If attack is recognized, DDOS defense server will take countermeasures against it. However, if the attack is not recognized the communication between RHS and home gateway is blocked. In such a case, Response Mechanism overcomes the incoming low-level attack.

Measurements and Analysis Category

The most common application of WSNs is collecting data from their deployment fields whether it is reachable or not, and at a friendly area or at a hostile one. Here, the most significant issue is to achieve the highest efficiency within the duty time. Therefore, WSN designers need to have information about the normal behavior of WSN as well as their behavior under attacks especially when DOS attack as its where its detection is more involved. Hence, these measurements and analyses are very important.

In [23], the authors focus on analyzing Sensor-Medium Access Control (S-MAC) protocol, which provides good energy properties, scalability and collision avoidance. The S-MAC protocol consists of four essential components: periodic listen and sleep, collision avoidance, overhearing avoidance, and message passing.

In case of no authentication, two different situations may arise: first situation is when the adversary node B' is located between two nodes A and B (i.e. r1< r) as shown in Fig 3.

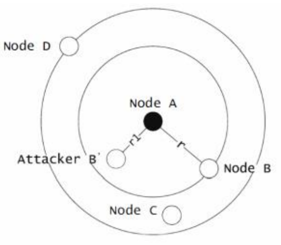


Fig.3. DoS attack by neighboring node in S-MAC

B' replies the *clear to send (CTS)* packet to A instead of B. The second situation arises with a collision attack where B' keep sending fake Sync and *request to send (RTS)* packets to both A and B and cause collisions. The power consumption is analyzed and compared with similar situations where an authentication algorithm is applied. The overall results show less power consumption if authentication is used. In [28], Authors aimed to detect flooding DOS attacks that exhausted the energy of sensor nodes. Authors tend to achieve desired detection by deploying entropy estimator nodes. The entropy estimation is a classification algorithm that is normally used in data mining and machine learning applications for distinguishing between normal and abnormal behaviors. The detection process is based on simplified Entropy Estimation for key information that is attached to traveling messages. This information in WSN is the key used for authentication and encryption of messages instead of collected information because collected information such as temperature or light intensity could regularly change with time. In [37], authors try to find the most effective metrics for examining the behavior of WSN nodes and decide whether nodes are under attack or not. These metrics may be a base for developing an intrusion detection system IDS. The authors focus on jamming attack and black hole attack to test the impact of their metrics on WSN. To be sure that the selected metrics are generally applicable, they vary some parameters such as Topology (mesh/collect), Traffic (high/low), Transmission power (high/low) and Type of Attack (jamming/black-hole/no attack). Metrics can be divided into three categories: elementary metrics, collection tree specific metrics, and mesh network-specific metrics. They found that packet delivery rate is the most conclusive metric detecting attacking behavior. By analyzing the listening time and the number of neighboring nodes, both of them can detect the attack on all nodes. In [45], very useful information about the survivability of WSN is provided for the designers of WSN. The survey covers sink nodes, major CHs and miner CHs as in Fig 4.

The authors give a definition of survivability as " *The ability to provide basic services after attacks or system error*". Survivability evaluation consists of two approaches. The first approach is the *analysis of services offered by network* which is the communication rate between CHs. The second approach is the *probability of being in a state obtained by Markov Chain* which computes the probability of CHs failure rate especially in case of miner cluster head.

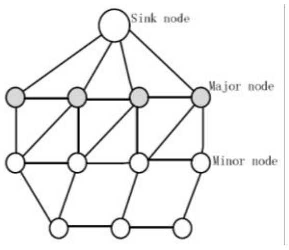


Fig.4. Tree structure of cluster-based WSN

Authors base their evaluation upon two criteria, namely the density of nodes and the initial power of nodes. As a result of this evaluation, they find that the survivability increase if node density and initial power increase.

Authentication Approach Category

Data collected from a certain field especially form hostile ones, should be protected from attackers who try to capture significant information, disturb data transmission, change transmitted data, etc. Therefore, authentication aims to make authenticated data available to authorized users only. As power consumption is the most crucial factor in WSN's, more power will be consumed in nodes applying authentication. Moreover, it is applicable to a limited number of attacks such as jamming attacks. In addition, multi-hop communication also appears as a challenge, which raises the vulnerability of communication paths due to the attacks by compromised nodes.

In [18], the authors proposed a DoS resilient enhanced two-factor authentication scheme for WSNs. The so-called two-factor authentication consists of two parameters that nodes in WSN utilize for identifying the sender and to verify sender node at the receiving node. These two factors are any two elements well known for both sides such as password and/or digital signature. The two-factor authentication scheme relies on two enhancing methods. First, lightweight pre-authentication using Merkle hash tree. Second, personalized secret parameters for sensor nodes. Authors concluded that their modified Two-factor scheme has the ability to resist the *Gateway impersonation attack with node captured* and *Forgery attack with node captured* with high efficiency of more than 90% and to adapt dynamically to DoS attacking scenarios.

In [34] and [38], address the challenge that communications may suffer *resource-draining* attacks where the attacker floods the WSN with useless or fake messages leading to higher power consumption and buffer overflow. As a countermeasure, a *Hop-by-Hop Broadcast Source Authentication Protocol (H^2BSAP)* method was proposed which provides authentication along the path to the sink node. In this way, threats are limited to one-hop neighbors only. H^2BSAP reduces the time needed for data verification where nodes need to buffer received data for a short while. The protocol also imposes extra overheads in computation, storage, and transmission, which are considered as open issues. The protocol also suffers from scalability problem.

In [43], authors claim that most of the anonymous authentication protocols designed for WSN-based real-time applications are suffering from missing synchronization between participants within the WSN, which leaves them vulnerable to DOS attack. The authors proposed a model consisting of three parts: the set of users U, a gateway GW, and a set of sensor nodes SN that acts in a real-time monitoring manner. Successful authentication is done when user U sends an authentication request to GW using a temporary identification TID, GW responding with generating a new TID for user U. The new TID lets U access sensor nodes SN through public channel and a secret key shared between them. This solution can be easily integrated into the current protocols and reduce communication and computational efforts during re-synchronization.

In [22], it is assumed that attackers can compromise sensor nodes and inject false or fake data to trigger false alarms. Also, they can inject a large number of messages in order to exhaust the nodes' energy through multi-hop communication. This type of attack is called *Path-based Denial of Service (PDoS)* attack (i.e. attack by compromised nodes along communication path). As a solution for these attacks, multiple nodes can cooperate to produce an authenticated report. *False-Endorsement-Based Denial of Service (FEDoS)* is an attack when an attacker compromises one of cooperated nodes and generates a false endorsement message (MAC) which cannot be verified in report generating node. Accordingly, report-generating node (CH) compresses endorsements and sends it to sink node. This issue is solved by making endorsing node send a proof message for correct endorsement after a certain time. This solution is sensitive to Jamming attack, which affects the communication channel between cooperating nodes and cluster heads. Hence, authors propose a gray-list approach where the report-generating node CH, will not exclude the node under jamming attack at once but put it in gray-list until proof is received with the next endorsement. The drawback of this approach is higher energy consumption in comparison with previous solution. Moreover, if grey list is full, attacked node may be excluded from further report endorsement.

False Endorsement-Based Algorithms

Nodes belonging to a certain cluster, send their endorsements to cluster head (CH). To mitigate FEDoS attack, cluster nodes should send the same endorsement again after a time interval as a proof for the previously sent endorsements. If proof endorsements do not reach cluster head within the time interval, delayed node CN is excluded from further endorsement. Christoph Krauß, Markus Schneider and Claudia Eckert in [22], propose that if a node sends the first endorsement but the proof endorsement does not reach CH, add delayed node to a Grey-List until node's proof message of the old endorsement reaches CH together with a new report endorsement.

Authors in [22], assume that jamming attack can be detected via certain algorithms but it cannot be prevented. Therefore, they considered the effect of jamming upon communication between endorsing node CN and cluster head CH. The considered type of jamming attack is the one that prevents or delays CN messages from reaching the cluster head but does not destroy the message itself.

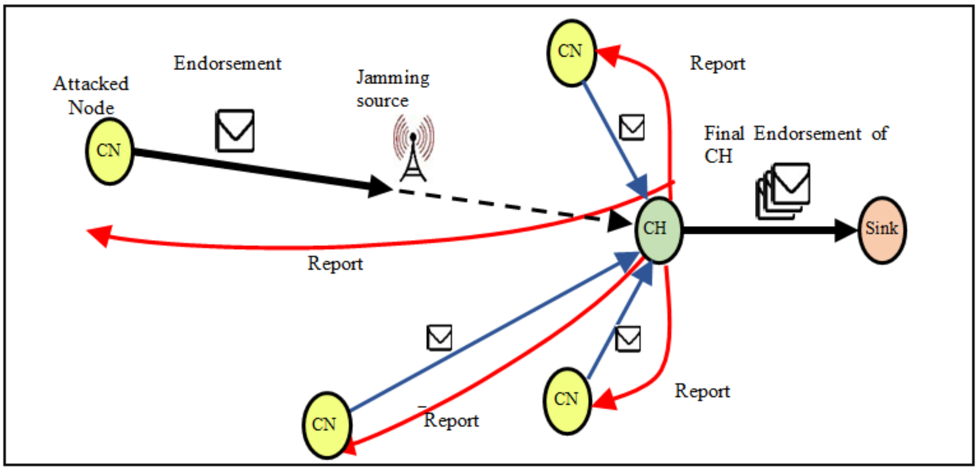


Fig.5. Jamming attack model

Fig. 5 represents False Endorsement based algorithm while considering the jamming attack. The messages of the node under attack are prevented or delayed to reach CH for longer than the threshold time, while other nodes' messages are delivered correctly. As a defense mechanism, Grey-List enhancement is considered. CH removes attacked node from trusted list and inserts it into the Grey-List. Therefore, attacked node has a chance to send delayed endorsement for the last report together with the next endorsement report. Receiving an endorsement report, CH checks if the endorsing node lies in the Gray-List or not and if its previous endorsement was verified correctly. If so, CH removes node from the Gray-List and returns it back to the trusted list. Otherwise, if the node is still under jamming attack or the Gray-List is full, the node under attack is excluded from further endorsement reports.

Analysis of FEDoS Mitigating Method

The method successfully prevents FEDoS attack by re-computing the hash values and comparing it with the received ones. A major drawback of this method is in considering Jamming attack. If the last endorsement hash value does not reach CH at all or delayed longer than the threshold, the node will suffer from False-Exclusion while it is still functioning correctly. This means that if jamming attack continues preventing messages from reaching CH, more innocent nodes will be excluded incorrectly.

IV. Proposed Active Defense Strategy

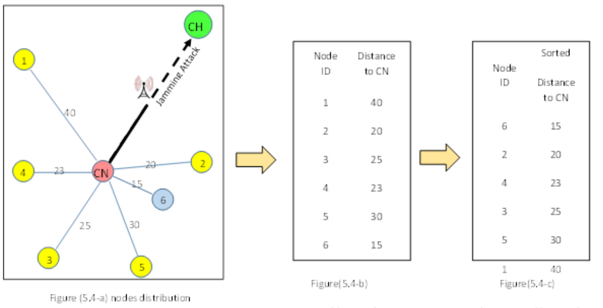
The pitfall of false-excluding in FEDoS method is a direct consequence of delayed delivery of proof endorsements due to continued jamming attacks. This requires an enhancement to prevent excluding well-functioning nodes from further report endorsements. The proposed enhancement provides a solution for multipath endorsement message delivery and does not enforce direct communication between attacked node and the cluster head for transferring messages.

Assumptions of the Proposed Strategy

To achieve the desired results, several assumptions are taken into consideration while designing proposed model as described below:

- The cluster head has not been compromised.
- Cluster head has higher energy, storage, and computational capabilities.
- The deployed sensor nodes are stationary.
- Nodes are deployed randomly.
- Cluster head has information about which nodes are functioning correctly, doubtful nodes and nodes under Jamming attack.
- The node under jamming attack is still alive and functioning correctly.
- Cluster head controls communication between nodes.

Proposed Strategy



Node ID	Distance to CN
1	40
2	20
3	25
4	23
5	30
6	15

Node ID	Sorted Distance to CN
6	15
2	20
4	23
3	25
5	30
1	40

6-a 6-b 6-c

Fig.6. The cluster head behavior

Fig. 6, depicts the cluster head behavior when CN ID is located in Gray-list and it might be excluded as jamming attack is still acting. First, as depicted in Fig. 6, CH collects the location information of the deployed nodes. Then CH computes the distances between the attacked node to every other node. Finally, CH sorts the distance table in ascending manner to pick the nearest neighbor to the attacked node CN. Obviously, distance is an effective parameter in reducing consumed energy. Cluster head also collects information about the doubtful nodes in the cluster, which are compromised nodes or act as an adversary trying to inject false endorsement messages. For instance, node number (6) in Fig. 6 represents a doubtful node. Therefore, when CH selects the nearest safe neighbor node to a node under attack (CN), doubtful nodes will be bypassed even if they lie at a nearer distance to CN.

After selecting the nearest safe neighbor to CN, CH sends it a message with ID of an attacked node (CN) and a request for endorsement. This message requests the selected nearest neighbor node (node 2 in Fig. 6) to ask the attacked node CN to forward its endorsement to CH through the selected nearest neighbor.

In this process, timing is a very important factor to ensure the transmission of the messages is accomplished within the expected time threshold. Therefore, the selected neighbor stores the transmission time of the request to CN.

When CN receives the request message, it responds by forwarding its endorsement, hash value, node ID, and the retransmission time to the selected nearest neighbor. As soon as the selected neighbor node receives the endorsement, it forwards it to CH with the following information:

- Selected neighbor node ID, which is important information especially if CH manipulated multiple jamming attack cases.
- Attacked node ID to inform CH that this endorsement belongs to a specific attacked node and to ensure that the nearest node requests the correct CN.
- The CN endorsement message and its Hash value.
- The transmission time of the request message to CN and the arrival time of the reply.

When CH the message, an authentication process starts immediately. Initially, CH checks the time difference between requesting and reply time. If it is more than the threshold then CH realizes that the link between the nearest node and CN is also affected by jamming attack. If time difference is within the acceptable range, CH re-computes the hash value for the received endorsement and compares it with the hash value in the message. In comparison to the hash values match, the CN is removed from the gray list and permitted to send further endorsements. However, if comparison fails, it implies that CN suffers from other attacks (s) in addition to jamming attacks.

Fig. 7 shows the case that the nearest neighbor node (2) fails to communicate with CN, or the authentication of CN endorsement forwarded by the nearest neighbor is not approved. In this case, CH selects another neighbor node from sorted distance table and repeats the process. As it is shown in Fig. 7, the dashed line represents the failed authentication path but the solid line between CH and node (4) represents the second attempt by CH to receive the endorsement of the attacked node. The cluster head CH keeps trying different neighbor nodes until the first correct endorsement authentication occurs. The attacked node will be trusted again for further endorsement and removed from grey-list if such authentication is reached.

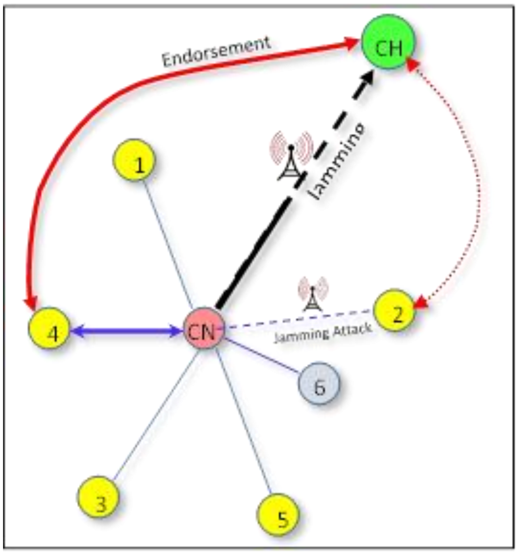


Fig.7. The case of first neighbor node failure

V. Testing and Experimental Results

In order to verify the ability of the proposed method to mitigate false exclusion nodes in DoS attack, several test scenarios have been applied. There are some assumptions considered as initial conditions to apply these scenarios. The testing approach is considered to include six different parameters in order to put the proposed algorithm under a wide range of testing possibilities. These factors are:

- The number of deployed nodes (size of network) and their positions. These values are selected randomly.
- Node status: if a node is under active jamming attack, it is labeled as 'YES', otherwise the label is 'NO'.
- The number of nodes under attack which is a percentage of the total deployed nodes.
- Defense level parameter, where '1' indicates a grey-listed node, which is not currently under jamming attack. A level value of '2' refers to grey listed nodes under active jamming attack.
- Doubtful nodes around the node under attack. These nodes may suffer from other kinds of attacks making them unsafe to deliver endorsement. These nodes are selected randomly and as a percentage of total nodes.
- Nodes that inject false data. These nodes are a subset of the nodes under attack, which represent double attacked nodes.

These parameters are varied individually or in combination to ensure the efficiency of the false node exclusion DoS mitigation algorithm. We have considered two main scenarios for verifying our proposed method. The first scenario assumes the nodes under jamming attack are randomly distributed in the deployment area of the sensor nodes. The second scenario adds the extra restriction that the jamming attack is concentrated in a specific area. In both scenarios the location of the sensor nodes and nodes under attack are selected randomly. Tables 1 and Table 2 provide the parameters used during the experiments. The experiments at each scenario repeated 100 times and the average values considered as the numeric performance results. This scenario further restricts access to the nodes under attack. Test scenarios are described in the following sub-sections.

Scenario (1)

In addition to the previously described test parameters, another parameter is added to prove the ability of the proposed algorithm to detect double attacked nodes as well as doubtful nodes (Table 1). A double attack indicates that a certain node is under jamming attack while the authentication process has detected that it was attacked with some other type of DoS attack such as being compromised and injecting false endorsement. This assumption gives an extra advantage to enhance the algorithm in addition to its proved and tested abilities.

Table 1. Parameters of the first testing scenario

number_of_nodes	*100 nodes*
jamming_state	*'Yes'*
attacked node_percentage	*10 %*
defense_level	*2*
doubtful_node percentage	*10 %*
false_injecting_node_percentage	*40% (of attacked nodes)*

Fig. 8 through Fig. 13 depicts the application of the first scenario to evaluate the proposed algorithm.

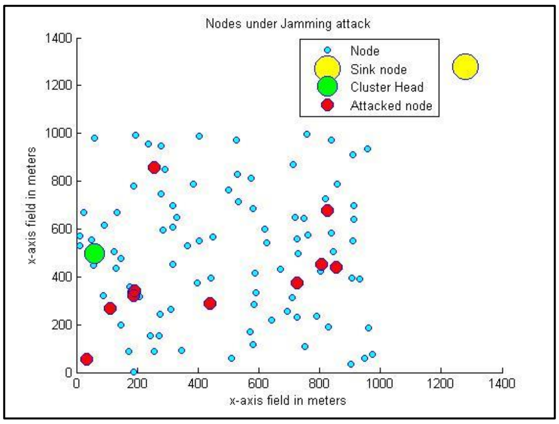


Fig.8. The distribution of attacked node and the location of CH

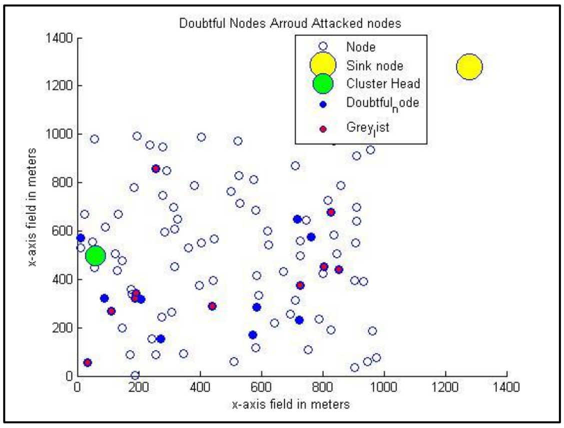


Fig.9. The distribution of doubtful nodes and gray-listed nodes

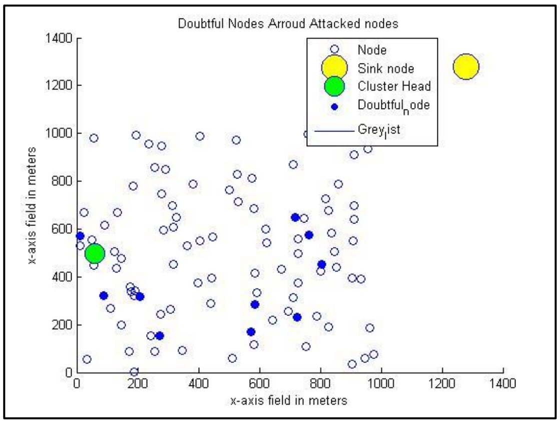


Fig.10. The gray-listed nodes after applying the proposed method

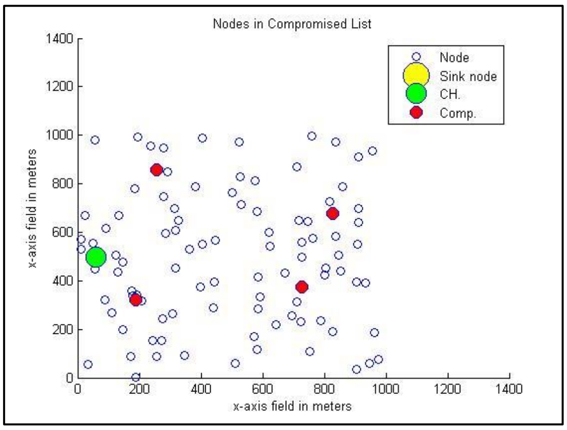


Fig.11. The distribution of compromised nodes

Fig. 8 through Fig. 13 shows the behavior of the proposed algorithm against all possible previously mentioned six input parameters. Fig. 8 shows the cluster structure and the distribution of the nodes under jamming attack that the algorithm tries to authenticate. Fig. 9 combines the attacked nodes and the doubtful nodes around them before authentication. After applying the proposed method, the nodes under attack are reached through the nodes in the trusted list (if such a path exists) and hence, the gray list is updated by removing the nodes under attack as depicted in Fig. 10. As a result of applying the authentication procedure, the compromised nodes are identified as depicted in Fig. 11. In this study, we have considered injecting false hash values as the second type of DoS attack. The compromised nodes are removed from grey list and added to compromised list for further consideration (Fig. 12). The final stage of the test scenario leaves the grey list empty where all healthy nodes are added to the trusted list and accepted for further report endorsements (Fig. 13).

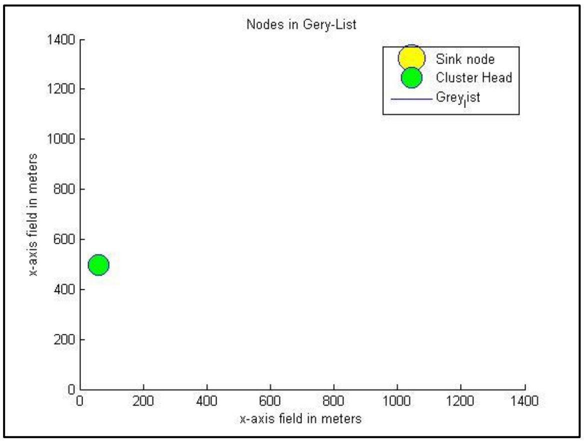


Fig.12. The gray list after applying the proposed method

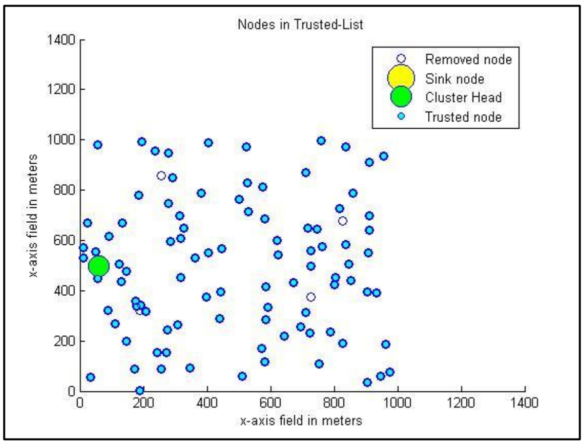


Fig.13. The trusted list after applying the proposed method

Scenario (2)

The second test scenario aims to verify the ability of the proposed algorithm to authenticate the attacked nodes when the jamming attack concentrates in a local area of the network and affects the nodes in a certain radial distance from the jamming attack center. The parameters are shown in Table 2.

Table 2. Parameters of the second testing scenario

number_of_nodes	*500 nodes*
jamming_state	*'Yes'*
attacked node_percentage	*10 %*
defense_level	*2*
doubtful_node percentage	*10 %*
false_injecting_node_percentage	*10% (of attacked nodes)*
attack_state	*'region'*

Results of the second testing scenario

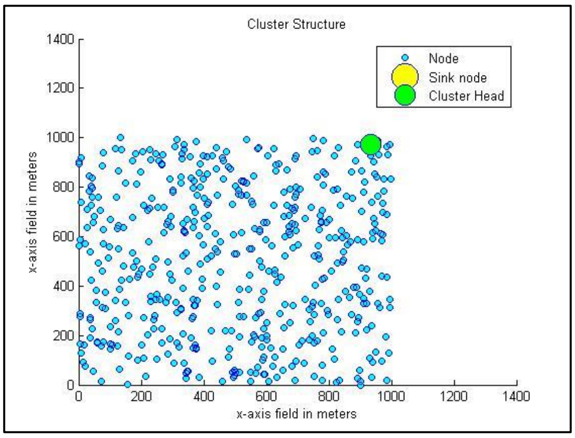


Fig.14. Distribution of the nodes

Fig. 14 through Fig 16 show the behavior of the enhanced algorithm against jamming attack when the nodes under attack are concentrated in a limited region. We assume that the cluster head is located outside of jamming attack region. The distribution of the nodes has been depicted in Fig. 14. The nodes under attack are among the trusted nodes, however, we have assumed a jamming attack center with a given radius limits the affecting area of the attack. This assumption causes the nodes under attack to be inside a limited area as depicted in Fig. 15. Applying the proposed method to authenticate the nodes in the gray list and move them to the trusted nodes list provides the results that are depicted in Fig. 16.

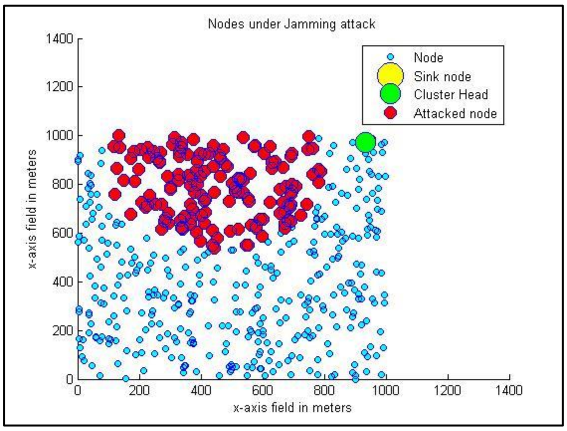


Fig.15. Nodes under attack

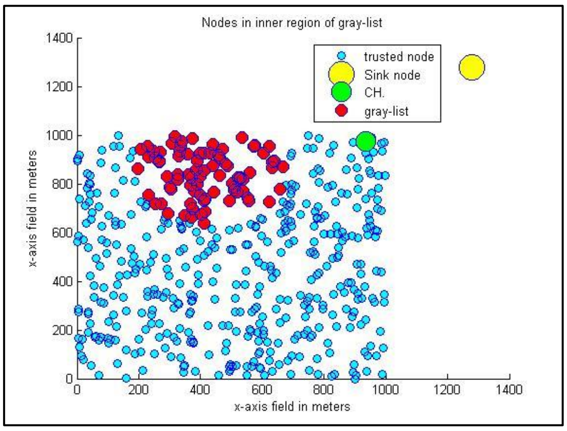


Fig.16. Updated gray list after applying the proposed method

As it is clear from Fig 16, the algorithm authenticated only nodes lying on the boundary of the jamming attack region. Many of the nodes further inside the jamming attack region are not reachable through any path consisting of trusted nodes only. It should be noted that the rate of the nodes remaining in the gray list unauthenticated depends on the density of the nodes in the jamming attack area, the number/percentage of the nodes being affected by the jamming attack, and the radius of the jamming attack area. In our experiments the improvement was between 36% and 52%. This improvement indicates the percentage of the nodes under attack that is removed from the gray list and was obtained by repeating the experiment 100 times. However, even in the worst case the proposed algorithm is capable of reducing the number of unauthenticated nodes in the gray list and improving the performance of the network in general.

Analysis of the Proposed Defenses Strategy

The goal of the proposed strategy is preventing false exclusion of nodes from participation in sending endorsements when they are alive and functioning correctly.

Moreover, the proposed method can detect double attacks on a node. While jamming attacks prevent messages from reaching CH, attacked node may be compromised by another attack. Moreover, the proposed algorithm gives CH a chance to receive the endorsements of the attacked node via different paths. CN can find a way to deliver its endorsement if at least one of its neighboring nodes can communicate with CH.

In addition, as a significant property of the proposed algorithm, delivering endorsement of the attacked node is carried out under the full control of CH, because having no acknowledgment sent back from CH, CN does not know if it is under jamming attack. From a security perspective, the proposed method does not require CN to broadcast its endorsement to neighboring nodes, which may result in capturing sensitive information such as node ID and hash value of endorsement and use them for false data injection by a compromised node. Meanwhile, broadcasting imposes higher power consumption cost on node energy. The simulated experiments shows that when the attacked nodes are isolated, or at random positions of the network, the method can almost fully (100%) recover the gray list nodes. In case of having jamming attack affecting a group of nodes at a specific location, the improvement ranges between 36% and 52%. The main disadvantage of the proposed method is its increased communication activates.

VI. Conclusion

With emerging of numerous WSN applications, their security has attracted the attention of many researchers recently. DoS attack is one of the attacks which poses a serious challenge in WSNs as it is hard to detect and prevent. In this study, we have considered the issue of excluding the nodes under DoS attack from further communications by the cluster head which degrades the performance of the network. We have proposed a method for mitigating the False Node Exclusion DoS (FNEDOS) in case that the nodes are under jamming attack, which prevents them from transferring messages to the cluster head. The proposed enhancement method provides a solution for original False Endorsement DoS (FEDOS) method limitation, which causes excluding innocent nodes from participating in endorsing cluster head broadcasted reports. The enhancement includes an algorithm to detect and utilize alternative safe paths for delivering the endorsements of the nodes under attack node. In addition, the proposed method does not allow broadcasting and hence, disclosure of sensitive data while considering the side effect of higher power dissipation due to broadcast messages. The experimental results reveal that when the number of nodes under attack is low, or they are not concentrated in a limited region, the proposed method is capable of mitigating false exclusion of innocent nodes from endorsements. Although the performance of the proposed method degrades when the nodes under attack densely cover a small area, still some improvement is achieved in comparison with similar methods proposed in the literature.

As the future extension directions, there are several possible approaches to enhance FNEDOS algorithm. The first possibility is to enhance the algorithm through an energy-aware methods [1], which can reduce power consumption due to extra communication processes, and balance energy consumption to prolong the lifetime of the cluster. Secondly, the algorithm can be improved by utilizing intelligent search algorithms for optimum path selection between attacked nodes and cluster head especially when multi-hop paths are considered. The third possibility is extending the algorithm to non-stationary sensor nodes. In addition, a combination of intelligent algorithms and multi-channel communication may be taken into consideration to address the open issue of regional attacks problem.

References

[1] Alsultan, Mohammed, Kasim Oztoprak, and Reza Hassanpour. "Power aware routing protocols in wireless sensor network." *IEICE Transactions on Communications* 99.7 (2016): 1481-1491.

[2] Aazam, Mohammad, et al. "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved." *Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on*. IEEE, 2014.

[3] You, Pengfei, Yuxing Peng, and Hang Gao. "Providing information services for wireless sensor networks through cloud computing." *Services Computing Conference (APSCC), 2012 IEEE Asia-Pacific*. IEEE, 2012.

[4] Flammini, A., and E. Sisinni. "Wireless sensor networking in the internet of things and cloud computing era." *Procedia Engineering* 87 (2014): 672-679.

[5] Liu, Qing, and Anfeng Liu. "On the hybrid using of unicast-broadcast in wireless sensor networks." *Computers & Electrical Engineering* 71 (2018): 714-732.

[6] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." *Computer networks* 38.4 (2002): 393-422.

[7] Prasanna, S., and Srinivasa Rao. "An overview of wireless sensor networks applications and security." *International Journal of Soft Computing and Engineering (IJSCE), ISSN* (2012): 2231-2307.

[8] Sharma, Sukhwinder, Rakesh Kumar Bansal, and Savina Bansal. "Issues and challenges in wireless sensor networks." *Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on*. IEEE, 2013.

[9] Hari, Parli B., and Shailendra Narayan Singh. "Security issues in Wireless Sensor Networks: Current research and challenges." *Advances in Computing, Communication, & Automation (ICACCA)(Spring), International Conference on*. IEEE, 2016.

[10] Hergenröder, Anton, and Jens Horneber. "Facing challenges in evaluation of WSN energy efficiency with distributed energy measurements." *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. IEEE, 2011.

[11] Yue, Ying-Gao, and Ping He. "A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and future directions." *Information Fusion* 44 (2018): 188-204.

[12] Messai, Mohamed-Lamine. "Classification of attacks in wireless sensor networks." *arXiv preprint arXiv:1406.4516* (2014).

[13] Hari, Parli B., and Shailendra Narayan Singh. "Security issues in Wireless Sensor Networks: Current research and

challenges." *Advances in Computing, Communication, & Automation (ICACCA)(Spring), International Conference on*. IEEE, 2016.

[14] Ahlawat, Priyanka, and Mayank Dave. "An attack model based highly secure key management scheme for wireless sensor networks." *Procedia Computer Science* 125 (2018): 201-207.

[15] Ioannou, Christiana, and Vasos Vassiliou. "The Impact of Network Layer Attacks in Wireless Sensor Networks." *Secure Internet of Things (SIoT), 2016 International Workshop on*. IEEE, 2016.

[16] Hwang, Ren Junn, and Yan Zhi Huang. "Secure Data Collection Scheme for Wireless Sensor Networks." *Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on. IEEE, 2017.*

[17] Shahzad, Furrakh, Maruf Pasha, and Arslan Ahmad. "A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures." *arXiv preprint arXiv:1702.07136* (2017).

[18] Wang, Fei, et al. "A DoS-resilient enhanced two-factor user authentication scheme in wireless sensor networks." *Computing, Networking and Communications (ICNC), 2014 International Conference on*. IEEE, 2014.

[19] Ouyang, Xi, et al. "A novel framework of defense system against dos attacks in wireless sensor networks." *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*. IEEE, 2011.

[20] Arazi, Ortal, Hairong Qi, and Derek Rose. "A public key cryptographic method for denial of service mitigation in wireless sensor networks." *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*. IEEE, 2007.

[21] Gill, Khusvinder, and Shuang-Hua Yang. "A scheme for preventing denial of service attacks on wireless sensor networks." *Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE*. IEEE, 2009.

[22] Krauß, Christoph, Markus Schneider, and Claudia Eckert. "An enhanced scheme to defend against false-endorsement-based DoS attacks in WSNs." *Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,*. IEEE, 2008.

[23] Kim, Kihong, and Jinkeun Hong. "Analysis of power consumption of S-MAC protocol according to DoS attack." *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*. IEEE, 2010.

[24] Saghar, Kashif, et al. "Applying formal modelling to detect DoS attacks in wireless medium." *Communication Systems Networks and Digital Signal Processing (CSNDSP), 2010 7th International Symposium on*. IEEE, 2010.

[25] Ballarini, Paolo, Lynda Mokdad, and Quentin Monnet. "Modeling tools for detecting DoS attacks in WSNs." *Security and Communication Networks* 6.4 (2013): 420-436.

[26] Muraleedharan, Rajani, and Lisa Ann Osadciw. "Cross layer denial of service attacks in wireless sensor network using swarm intelligence." *Information Sciences and Systems, 2006 40th Annual Conference on*. IEEE, 2006.

[27] Gu, Qijun, and Peng Liu. "Denial of service attacks." *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications* 3 (2007): 454-468.

[28] Kim, Mihui, Inshil Doh, and Kijoon Chae. "Denial-of-service (dos) detection through practical entropy estimation on hierarchical sensor networks." *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*. Vol. 3. IEEE, 2006.

[29] Raymond, David R., and Scott F. Midkiff. "Denial-of-service in wireless sensor networks: Attacks and defenses." *IEEE Pervasive Computing* 7.1 (2008).

[30] Mansouri, Djamel, et al. "Detecting DoS attacks in WSN based on clustering technique." *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*. IEEE, 2013.

[31] Zhang, Heng, et al. "DoS attack energy management against remote state estimation." *IEEE Transactions on Control of Network Systems* (2016).

[32] Guechari, Malek, Lynda Mokdad, and Sovanna Tan. "Dynamic solution for detecting denial of service attacks in wireless sensor networks." *Communications (ICC), 2012 IEEE International Conference on*. IEEE, 2012.

[33] Monnet, Quentin, Lynda Mokdad, and Jalel Ben-Othman. "Energy-balancing method to detect denial of service attacks in wireless sensor networks." *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014.

[34] Bekara, Chakib, Maryline Laurent-Maknavicius, and Kheira Bekara. "H 2 BSAP: A hop-by-hop Broadcast Source Authentication Protocol for WSN to mitigate DoS attacks." *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*. IEEE, 2008.

[35] de Biasi, Gabriel, and Luiz FM Vieira. "Taxonomy of Security Attacks in Opportunistic Networks." *Opportunistic Networks: Mobility Models, Protocols, Security, and Privacy* (2018): 67.

[36] Mohammadi, Shahriar, and Hossein Jadidoleslamy. "A comparison of link layer attacks on wireless sensor networks." *arXiv preprint arXiv:1103.5589* (2011).

[37] Riecker, Michael, Daniel Thies, and Matthias Hollick. "Measuring the impact of denial-of-service attacks on wireless sensor networks." *Local Computer Networks (LCN), 2014 IEEE 39th Conference on*. IEEE, 2014.

[38] Bekara, Chakib, Maryline Laurent-Maknavicius, and Kheira Bekara. "Mitigating Resource-Draining DoS Attacks on Broadcast Source Authentication on Wireless Sensors Networks." *Security Technology, 2008. SECTECH'08. International Conference on*. IEEE, 2008.

[39] Almomani, Iman, and Bassam Al-Kasasbeh. "Performance analysis of LEACH protocol under Denial of Service attacks." *Information and Communication Systems (ICICS), 2015 6th International Conference on*. IEEE, 2015.

[40] Mokdad, Lynda, and Jalel Ben-Othman. "Performance evaluation of security routing strategies to avoid DoS attacks in WSN." *Global Communications Conference (GLOBECOM), 2012 IEEE*. IEEE, 2012.

[41] Mansouri, Djamel, et al. "Preventing denial of service attacks in wireless sensor networks." *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015.

[42] Fouchal, Said, et al. "Recursive‐clustering‐based approach for denial of service (DoS) attacks in wireless sensors networks." *International Journal of Communication Systems* 28.2 (2015): 309-324.

[43] Gope, Prosanta, Jemin Lee, and Tony QS Quek. "Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks." *IEEE Sensors Journal* 17.2 (2016): 498-503.

[44] Gill, Kashif, S-H. Yang, and Wei Wang. "Scheme for preventing low-level denial-of-service attacks on wireless sensor network-based home automation systems." *IET Wireless Sensor Systems* 2.4 (2012): 361-368.

[45] Jiang, Zhongqiu, Shu Yan, and Liangmin Wang. "Survivability evaluation of cluster-based wireless sensor network under DoS attacks." *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*. IEEE, 2009.

Author' Profiles

Nawfal F. Abdulqader AL-Shaihk received his BSc degree from the Computer Engineering Department of Baghdad University in 2000. Later on in 2015 he continued his study in the Computer Engineering Department of Cankaya University and received his MSc degree in 2018. His main research interests are computer networks, and computer security.

Reza Hassanpour is an associated professor affiliated with the Computer Engineering Department of Cankaya University, Ankara, Turkey. He received his BS, MS, and PhD degrees in computer engineering from Shiraz University in 1995, Tehran Polytechnic University in 1998 and Middle East Technical University in 2003, respectively. He has conducted and supervised many research works in computer networks, intelligent systems, and machine learning.

How to cite this paper: Nawfal F. Abdulqader AL-Shaihk, Reza Hassanpour, "Active Defense Strategy against Jamming Attack in Wireless Sensor Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.11, pp.1-13, 2019. DOI: 10.5815/ijcnis.2019.11.01