www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 3, PP. 577-586
Manuscript received September 22, 2021; revised August, 2022. DOI: 10.24425/ijet.2022.141277

Configurable Secured Adaptive Routing Protocol for Mobile Wireless Sensor Networks

Ahmed Alnaser, Hessa Al-Junaid, and Reham Almesaeed

***Abstract*—This paper aims at designing, building, and simulating a secured routing protocol to defend against packet dropping attacks in mobile WSNs (MWSNs). This research addresses the gap in the literature by proposing Configurable Secured Adaptive Routing Protocol (CSARP). CSARP has four levels of protection to allow suitability for different types of network applications. The protocol allows the network admin to configure the required protection level and the ratio of cluster heads to all nodes. The protocol has an adaptive feature, which allows for better protection and preventing the spread of the threats in the network. The conducted CSARP simulations with different conditions showed the ability of CSARP to identify all malicious nodes and remove them from the network. CSARP provided more than 99.97% packets delivery rate with 0% data packet loss in the existence of 3 malicious nodes in comparison with 3.17% data packet loss without using CSARP. When compared with LEACH, CSARP showed an improvement in extending the lifetime of the network by up to 39.5%. The proposed protocol has proven to be better than the available security solutions in terms of configurability, adaptability, optimization for MWSNs, energy consumption optimization, and the suitability for different MWSNs applications and conditions.**

***Keywords*—Routing Protocol; Mobile Wireless Sensor Networks, WSN; security**

I. Introduction

ONE of the major advancements in the WSN field is the introduction of the Mobile Wireless Sensor Network (MWSN). In the MWSN, the sensor nodes are mobile which makes the sensor network applications more versatile compared to the static nodes. The mobile nodes' movement can be either dependent or independent of each other. Some applications in the fields of healthcare, military, transportation, and industry require the mobility of sensor nodes to support the mobility of the sensed objects [1]. There are three possible types of mobility: random mobility, predictable or fixed mobility, and controlled or adaptable mobility [2]. The mobility introduces new challenges to the sensors network such as the network coverage and reliability of communication as well as introducing new security challenges.

There are many security concerns when investigating MWSN, especially with the added challenges because of the mobility and the nodes' limited resources [3]. MWSN can be targeted by many types of security attacks. Some of these attacks target the routing functionality of the network such as the Sinkhole and Blackhole attacks, which compromise the network and data availability. These types of attacks are considered packet dropping attacks because they attract communicated packets by advertising attractive routing paths and then prevent packets from reaching intended destinations. The efficient energy consumption of WSNs and MWSNs such as in [4] [5] [6], network connection and delay such as in [7], and fault tolerance such as in [8] are the most researched field for routing protocols in WSNs and MWSN whereas security is not considered in most of the available network routing protocols mostly because security operations can consume valuable resources of the mobile nodes in MWSNs. Many protection methods depend on the protection provided in higher Open Systems Interconnection (OSI) layers. Securing the network routing process will result in earlier detection and prevention, which will prevent attackers from consuming valuable network resources and affecting the data availability and integrity in the network. The aim of this paper is to propose a novel secured routing protocol to contribute to securing the routing functionality in MWSNs. The proposed protocol is aligned with the nodes' scarcity of resources such as power, computational, memory, and storage limitation. The protocol is in compliance with the confidentiality, integrity, availability, and authentication requirements of MWSNs.

II. Related Works

Packet dropping attacks such as Blackhole, Greyhole, and Sinkhole attacks are extremely devastating attacks to the MWSNs. The main defense mechanism in protecting against these attacks is securing the routing operations. In this section, state-of-the-art secure routing protocols are surveyed and reviewed by summarizing the related work. For each contribution, key points and limitations of the proposed solution will be listed.

Yin and Madria proposed the Hierarchical Secure Routing Protocol Against Blackhole Attacks (HSRBH) [9] which uses MAC for verification between group leader, sink, and neighbours. While the protocol is optimized for WSNs, it is optimized for stationary nodes. Packets drop when nodes changes group leaders frequently. Improve security and performance of AODV protocol against Blackhole [10] uses two steps of analysing collected data and eliminating process based on rules for detecting and eliminating suspected Blackhole devices. AODV is optimized for MANETs and not efficient in MWSNs. It consumes high energy and results in false-positive eliminations. The Configured mobile agents to

Authors are with University of Bahrain, College of Information Technology, Kingdom of Bahrain (e-mail: haljunaid@uob.edu.bh, ralmesaeed@uob.edu.bh).

detect and prevent Sinkhole attacks [11], [12], [13] contributions use mobile agent software to collect information about the entire network. The detection is based on comparing sequence number and threshold value. They are designed to prevent sinkhole attacks only, they consume high energy, and are optimized for MANETs only. REWARD based on received, watch, and redirect operations [14] detects single and multiple Blackhole nodes with nodes monitoring their neighbours to ensure packets are forwarded. The protocol is consuming high energy because packets are sent more than once. REWARD assumes the network is reliable and collision-free and require nodes to have a transmission range that exceeds the next-hop node. It is relying only on reliability measures and cannot detect forged packets. Intrusion Detection System AODV Routing Protocol (IDSAODV) [15] uses route updates by ignoring first RREP message received. It consumes high energy, lack end-to-end management, and has delay in packets delivery. Detection of Blackhole attacks in MANETs [16] utilizes record table to store all route reply messages and compare sequence numbers of the destination in RREQ and RREP with threshold value. It is only optimized for MANETs and only uses reliability measures for protection therefore cannot protect from forged sequence numbers. In the Prevent Blackhole attacks on the medical WSNs [17], the routing direction of the RREQ and RREP is reversed and the RREQ contains a security check (hashed node number with timestamp). The protocol has limited application where data only requested by base station and only optimized for MANETs. Malicious nodes can forge captured RREQ to attract all communication and attacker can capture base station packet and extract security check value. Dynamic Source Routing protocol with an embedded Dynamic Trust Management System (DTMS) [18] is optimized for WSNs. Each node will calculate the trust value for its neighbours periodically and will assigns trust value for each node (0 to 1). The protocol does not account for mobile nodes with frequent neighbour changes, broadcasted trust value can be forged, and it has high overhead on the routing process for long paths (accumulative address). Deploying (UAVs) to detect Blackhole attacks [19] is a proposed solution which utilize the already deployed UAVs in some WSN applications. It uses Sequential Probability Ratio test method to block the compromised nodes. The solution depends on many factors such as the possibility of deploying UAVs, number of nodes, velocity of the nodes, hardware requirement, and proximity of UAVs when deploying in hostile environments. Enhancement on the zone routing protocol (ZRP) [31] is based on bluff probe packet with nonexistence address and consider the node that replies as malicious. It can detect multiple Blackhole nodes that are working together in MANETs. Solution is only optimized for MANETs and Attacker with global knowledge of the network can evade detection by replying only to valid addresses. Detection method for Blackhole nodes in WSNs based on trust management [32] records each delivered packet by keeping a streak score for each node. The solution consumes high energy and can result in false positives in unreliable network connection. Mitigating black hole attacks in WSNs using node-resident expert systems [33] is based on analysing nodes' behaviour and anomalies in neighbour nodes. Analysing mechanism works all the time and examines all behaviour and traffic which result is huge energy consumption. Catching packet droppers and modifiers in WSNs [34] Detect packet dropping attacks by using extra bit information added to all packets. It Uses encryption and authentication mechanisms to protect the packets. Huge energy is consumed to encrypt and decrypt every packet. BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks and Energy Management with Multiple Sinks (EMMS) [35], [36] contributions use multiple base stations deployed in the network to collect data. They are designed to work in WSNs. Nodes should be stationary and only work in application with multiple mobile base stations.

There are many studies, methods, and contributions to combat packet dropping attacks, but to the best of our knowledge, none of them considered security of the mobile nodes in the MWSN. The only paper worked in this context was by [37]. Chung and Cho proposed a multi-path routing determination algorithm based on fuzzy logic to detect selective forwarding attacks in MWSNs. They used AODV as a routing protocol and the mobility was not considered as a factor in their solution.

Many other studies focused on the MANETs [20] , [21], [22], [23], [24], [25], [26], [27], [28], [29] and [30] were there are major differences between MWSN and MANET such as the existence of base stations, size of the network, number of nodes, computational capabilities, power restrictions, and other factors. Many of the investigated methods used to secure MANETs from packet dropping attacks are more suitable for MANETs and may create additional energy overhead in MWSNs such as sending a huge number of packets that prevent sensor nodes from entering sleep mode to preserve energy. Other studies use methods with high computational and energy consumption such as encrypting all packets multiple times such as the work proposed by [34].

The researches accomplished to protect WSN are even fewer than those done for MANETs. All these studies do not account for mobility as a factor. Also, most of the researches focused on partial security issues such as focusing only on Blackhole attacks while ignoring other packets dropping attacks such as Sinkhole attacks or selective forwarding attacks such as Grayhole attacks. Other reviewed solutions were protecting against packet dropping attacks by using reliability controls, which may be easily forged by malicious attackers such as relying on replies from neighbours or always dropping the first RREP to avoid Blackhole RREP. In addition, there are no any comprehensive studies that discuss the routing protocols, security issues, and security attacks and provide a solution for any of these attacks for MWSNs.

After addressing many problems in the available state-of-the-art studies, we believe there is a great need for a solution to protect MWSNs from packet dropping attacks. The proposed protocol should be aligned with the nodes' scarcity of resources such as power, computational, memory, and storage limitation.

III. Research Method

In order to design the secured routing protocol, a set of steps were followed. Because the most challenging factor in integrating security into MWSNs is energy consumption, the design of the protocol was influenced by the most energy-

efficient type of routing protocols which are the hierarchically clustered routing protocols. These protocols allow the integration of security features without compromising the network resources. After choosing the protocol type, the code was designed, and the security functions were integrated into the code. While all investigated secured routing protocols have a predetermined security configuration, the proposed protocol was designed and built on the concept of allowing the network admin to adjust the required parameter of the security features to perfectly suit the network's intended purpose. The protocol is called CSARP and provides configurability, adaptive protection, security against packet dropping attacks, and mobility optimization. To achieve the configurability, the network admin is allowed to choose from four different protection levels to allow for support for more MWSNs applications. Also, the network admin will be allowed to configure the cluster heads ratio to allow the protocol to be suitable for different network scenarios. Adaptive protection was achieved by providing repeated detection process in case of malicious node detection. The mobility optimization was achieved by allowing nodes to change the cluster heads member based on location and by including the mobility factors in the feasibility investigation of the nodes to be cluster heads. The code was implemented using MATLAB software.

The simulation and benchmarking of CSARP was done with and without the presence of malicious attacks. The simulation was run using a defined set of parameters and conditions to allow accurate benchmarking. To achieve accurate simulation of the MWSNs, nodes were assigned random locations in each run to simulate nodes movement. To achieve accuracy despite the movement of the nodes, averages of multiple simulations were considered.

IV. PROPOSED CSARP ROUTING PROTOCOL

Hierarchically clustered routing protocols are the most popular type of protocols for WSNs and MWSNs. They offer low energy consumption by allowing nodes to use minimal transmission power as they connect to the cluster heads in the range rather than transmitting to the base station. Some of these protocols effectively address the mobility factor of the MWSNs such as the LEACH-mobile-enhanced and MBC protocols. Because of the hierarchical nature of these protocols, security operations can be introduced or integrated into deferent levels. The design of the proposed secured routing protocol is influenced by LEACH-mobile-enhanced and MBC protocols.

A. Security Design

The design of the CSARP protocol is aligned with the security requirements of MWSNs. The following is the list of the relevant security requirement and how CSARP comply with them:

1) Confidentiality: In CSARP, each node will have two pairs of keys which are used for the communication between the sink and nodes.
2) Integrity: The main detection in CSARP is targeted against the packet dropping attacks, which affect data integrity. For detection packet, the protocol uses keyed hash function to ensure integrity of detection process.
3) Availability: To achieve availability, CSARP will maintain the security of the network and will prevent packet dropping attacks and will contain malicious nodes.
4) Authentication: For Authentication, CSARP is using two pairs of keys for each node verification process.

B. Adaptability

All investigated security protocols lack the flexibility to be used in different operational scenarios. Also, they either have too many security operations with high energy consumption or have insufficient security measures in favour of preserving energy. This research's proposed protocol will have adaptive features that allow the protocol to perform differently to the different levels of security incidents. The proposed protocol will have four levels of security prevention settings which are designed to recover from packet dropping attacks. The adaptive feature will be disabled in the first two levels to preserve the energy. In second and third levels, the adaptive feature will work to ensure that when a malicious node exists in the network, the protocol will repeat the detection stage until all malicious nodes are detected. This should ensure malicious infection is contained. The adaptive feature will not be activated unless there is a threat in the network.

B. Configurability

There are different applications in MWSNs with different tolerances to security attacks and energy consumption. Some applications will require the most energy possible and may sacrifices not getting data from some nodes in the favour of prolonging the lifetime of the network. Other applications require the most availability of accurate data such as the critical health sector applications. This study proposed the ability of the network owner or admin to input or change the value of security tolerance or the relationship between energy consumption and security operations. The protocol allows four security configuration settings which are none, basic, balanced, and advanced.

All available routing protocols force a fixed percentage of the cluster heads ratio from the total nodes. The number of needed cluster heads depends on some factors such as the number of nodes, distance to the sink, the velocity of nodes density of nodes, and available energy level. Because of that, the cluster heads ratio is also a configurable setting in this proposed protocol. The network admin will be allowed to configure the percentage of the cluster head from the total nodes or use the default defined percentage.

C. Cluster Heads Selection

In the investigated routing protocols, cluster heads are chosen based on the residual energy and with a similar probability for all nodes to be chosen. Also, each node will not be chosen again when there are other nodes that have not been chosen. This means even if the node is not the best candidate for being a cluster head, it will be chosen if all other nodes have been elected before. In the proposed protocol, nodes can be elected again and the election is based on multiple factors. The mobility of nodes has an impact on the security of the network. While

nodes are moving, distances to the sink, routing paths, and neighbour nodes change. Also, there are mobility factors that should be considered such as the velocity of the nodes which affect the frequency of changing location.

In the proposed protocol, the selection of the cluster heads will be based on calculating the feasibility value for each node. Later, the nodes with the highest feasibility value will be elected as cluster heads. The feasibility value is calculated using three factors which are the residual energy ratio, velocity ratio, and the number of times as cluster head. Residual energy ratio is a calculation of the residual energy over the initial energy. Residual energy ratio is more accurate than the residual energy because it accounts for the initial energy value which represents the node's initial energy requirement. So, if there are two nodes with the same residual energy but one of them had less initial energy, the election process will choose this node because of the assumption that this node consumed less energy and therefore assumed to last longer. Velocity ratio is calculated using the difference between the current location and previous location which indicates the frequency of changing locations. The number of times as cluster will be also considered to allow the nodes that have already served as cluster heads to have more resistance to be elected again but at the same time allow the process of selecting cluster heads to be able to select the node again if it is the best candidate after considering all factors.

D. Mobility Optimization

To support mobility, mobile nodes can leave their cluster head and join another cluster head with less distance. Also, when the sink is closer to any node than other cluster heads, the node will send data directly to the sink. Another optimization to MWSN is the use of the nodes' mobility factors as part of cluster head selection, which results in selecting nodes with less mobility to minimize the nodes' frequency to change their cluster heads.

E. CSARP Protocol Functions

The proposed protocol consists of the following functions:

NetworkAdminInput: This function will take the input from the network administrator and will return one of the four protection levels. The function will accept input values of 0 to 3 representing the available protection levels.

AdaptiveProtection: This function will return the status of the adaptive protection feature.

ClusterHeadRatio: This function will allow the network admin to enter the ratio of the cluster heads compared to the total number of the sensors in the network. The ratio is set to a default value of 1-to-10 which means 10% of the sensors will act as cluster heads. The number of cluster heads will be calculated according to (1), where CH represent cluster head and n is the total number of sensors,

$$\text{Number of CHs} = \text{CH ratio} * n \quad (1)$$

ClusterHeadSelection: This function is responsible for selecting cluster heads. The base station will calculate the feasibility for each sensor to become a cluster head. The top sensors with the highest feasibility will be selected according to the selection ratio which is set to a default value of 1-to-10 of the total number of nodes. Equation (2) to (5) are used for selecting cluster heads. Table I shows the cluster heads selection equation symbols.

TABLE I
CLUSTER HEADS SELECTION EQUATION SYMBOLS

Symbol	Description
Si	Sensor number
F	Feasibility to be a cluster head
RER	Residual energy ratio
VR	Velocity ratio
CHC	Cluster head counter
RE	Residual energy
IE	Initial energy
CX	Current X location
CY	Current Y location
PX	Previous X location
PY	Previous Y location
R	Per Round
AsCH	Sensor selected as cluster head

$$F_{Si} = RER_{Si} - VR_{Si} - CHC_{Si} \quad (2)$$

Where,

$$RER_{Si} = \frac{RE_{Si}}{IE_{Si}} * 100 \quad (3)$$

$$VR_{Si} = \frac{\left((CX_{Si},CY_{Si}) - (PX_{Si},PY_{Si})\right)}{R} \quad (4)$$

And,

$$CHC_{Si} = Counter\ (AsCH_{Si}) \quad (5)$$

AttackDetection: This function is the core detection function of the proposed protocol. The function will be responsible for detecting packet dropping attacks by sending hashed random message to each node as a HELLO message and receives the hashed reply from each node to decide if there are compromised nodes. Each node is initiated with two keys which will be known to the base station. The hashed message is created by hashing a random value using the first key and waiting for the node to reply to the same random value hashed with the second key. So, the first key is used for encryption by the base station and for decryption by the node and the second key is used for encryption by the node and for decryption by the base station. If the node did not reply to the HELLO message, the node will be considered either blocked or malicious and will be added to the suspicion list. The detection function will investigate the node status by sending the HELLO message through a different route to confirm if the node is malicious. Once the node is confirmed to be malicious, it is added to a blacklist and removed from the network.

AttackPreventionLevel1: The first prevention level is the basic security level with the energy-oriented approach.

AttackPreventionLevel2: The second prevention level is a balanced security approach, and it is the default security setting.

AttackPreventionLevel3: The third prevention level has advanced security operations with a Security-oriented approach.

Fig. 1 shows the full CSARP processes flowchart starting with the input from network admin then initialization of the parameters. The main rounds loop will start and will continue while there are alive nodes. Setup phase will start followed by the detection process. Later steady-state phase will start for collecting data. Before the end of each round, another detection process will be initiated if advance protection level is selected. When the code is executed, the network admin should supply the required protection level value and the cluster heads required selection probability.

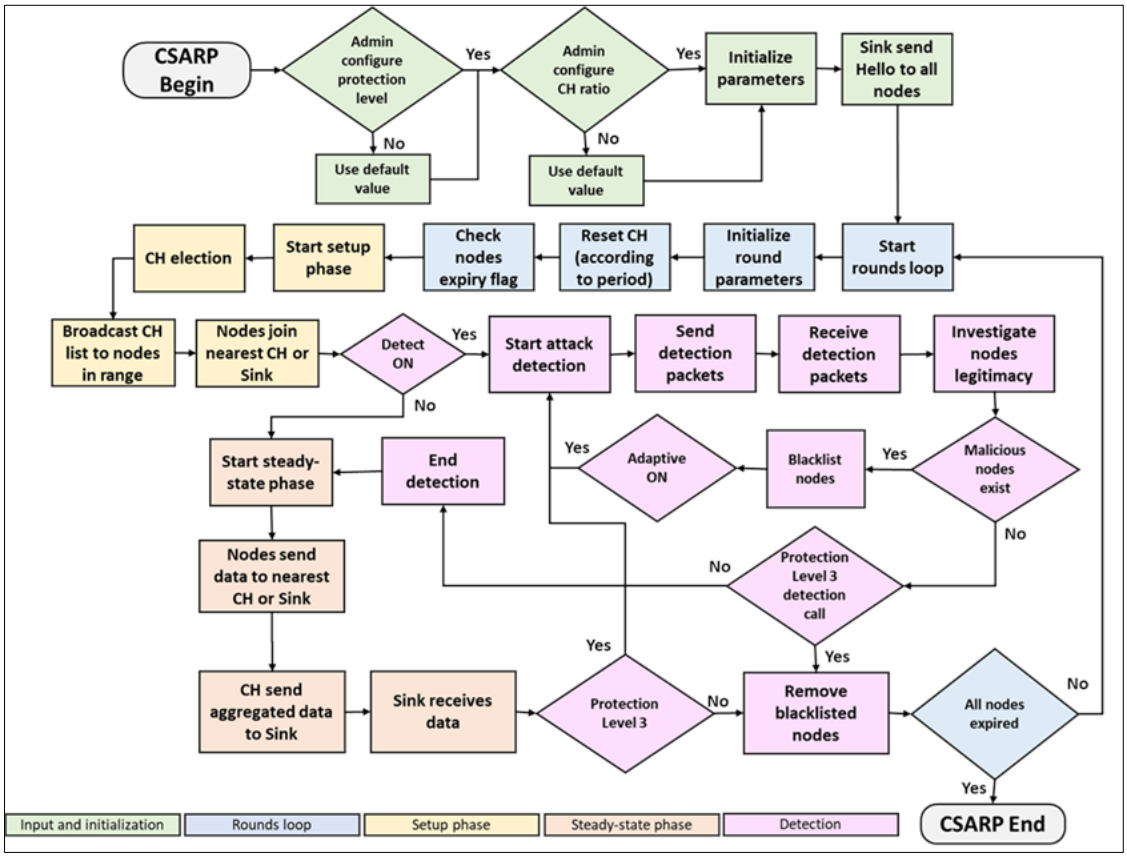

Fig. 1 CSARP routing algorithm

V. PERFORMANCE ANALYSIS

A. Simulation Setup

The proposed CSARP was simulated to investigate the effectiveness of protection functionality and the reliability of data communication. Each protection level was simulated in the presence of an attack and without any malicious behaviour. In order to achieve higher accuracy, an average of multiple simulations for the same parameters will be calculated. The simulation is executed using a set of conditions such as network area, number of nodes, probability of nodes to be a cluster head, and initial energy. The conditions were chosen to make the result accurate, comparable, and repeatable. The calculation of the energy consumption is based on LEACH algorithms and was calculated using the implementation of [38] with reference to [39]. Equations (6) to (9) represent the energy consumption, where E is the energy, Si is the sensor number, p is the packet size, d is the distance, Etx is the energy consumed for sending packets, Emp is the amplification coefficient of energy transfer, Efs is energy loss in space, Erx is the energy consumed for receiving a packet, Eda is data aggregation energy, and do is the distance to the base where Emp or Efs depends on do,

For sending a packet,

$$do = \sqrt{\frac{Efs}{Emp}} \tag{6}$$

If $(d > do)$,

$$E_{Si} = E_{Si} - ((Etx * p) + (Emp * p * d^4)) \tag{7}$$

If $(d < do)$,

$$E_{Si} = E_{Si} - ((Etx * p) + (Efs * p * d^2)) \tag{8}$$

For receiving a packet,

$$E_{Si} = E_{Si} - ((Erx + Eda) * p) \tag{9}$$

The conditions listed in Table II were taken into consideration during the simulation:

TABLE II
SIMULATION CONDITIONS

Condition	Description
Number of nodes	100
Area of network	100 m * 100 m
Initial energy for each node	0.05 J
Probability of node selection as cluster heads	10%
Protection level	0, 1, 2, 3 (all levels are tested)
Sink location	((X/2),(Y/2)) centre of area
Data Packet size	4000
Hello Packet size	100
Packets sent in steady-state phase	10
Nodes Radio Range	0.5*100*$\sqrt{2}$ = 70.7107 m
Location of nodes	Randomized in each simulation
Number of malicious nodes	0, 1, 3 nodes (all scenarios are tested)
Detection of Malicious nodes	If a malicious node is confirmed malicious, it will be removed (expire)

Number of simulations per set of conditions	Each set of conditions will be simulated 5 times and the average will be calculated
Comparison factors	Number of rounds, number of detections, communicated packets, packet loss, Protection Level
Etx	50*0.000000001 J/bit
Erx	50*0.000000001 J/bit
Eda	5*0.000000001 J/bt
Emp	0.0013*0.000000000001 $J/bit/m^4$
Efs	10*0.000000000001 $J/bit/m^2$
do	87.7058 m

Fig. 2 is showing a simulation with protection level 3 and 10% cluster heads ratio to all nodes. The protection process identified 3 malicious nodes and removed them from the network by considering the nodes expired. Expired malicious nodes are represented by red circles. The cluster heads are represented by circles with red X. Fig. 2 shows the nodes that are a member of a cluster head connected with blue line to each cluster head. The nodes that are not a member of any cluster head will send the data directly to the sink, which is represented by blue square. Fig. 3 is showing all expired nodes as red dots. The identified malicious nodes were removed from the network. The lifetime of the network is represented by the total number of rounds. All packets represent all communicated packets, which are Hello packets, detection packets, and data packets. The loss represents the number of lost packets due to the malicious attack. In this simulation, none of the lost packets contain data as the only lost packets are hello and detection packets. The second part of Fig. 3 is showing the expired nodes per each round. At the end of the second round, the suspected nodes were confirmed malicious and removed from the network. Until the 133rd round, the only expired nodes are the malicious nodes. At 142nd round, almost 50% of all nodes were expired. All nodes expired at 150th round and the simulation was ended.

B. Simulation Results Analysis

The Simulation was executed with three scenarios for each level by using one malicious node, three malicious nodes, and without the presence of malicious nodes. Each combination executed five times to produce a more accurate average. Table III contains the results for each scenario in each protection level. The three simulated scenarios are for the network with the presence of none, one, and three malicious nodes. In each scenario, the average of five simulations is calculated. The results in the previous section are collected from 60 simulations with different conditions.

Sink location is fixed while the locations of nodes were randomized in each simulation to have a simulation of a real-life application of MWSNs in each simulation process. Because locations were randomized, the number of data packets, packet loss, and lifetime of the network will vary accordingly. Averages of the collected results were taken to ensure the accuracy of the results. Each comparison factor is discussed below:

Number of detections: Without any protection such as in protection level 0, the protocol fails to identify any packet dropping attacks on the network and the malicious nodes will be considered legitimate and will cause packet loss. In Protection levels 1, 2, and 3, the protocol successfully detects all malicious nodes from the first round and before data packet communication. The protocol then adds them to the suspected list to confirm the detection in order to remove them totally from the network. In the simulation, the malicious nodes appear as expired nodes.

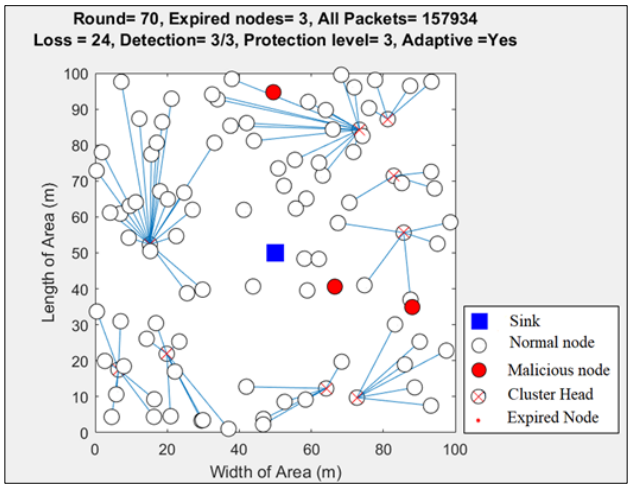

Fig. 2 Executing CSARP Simulation

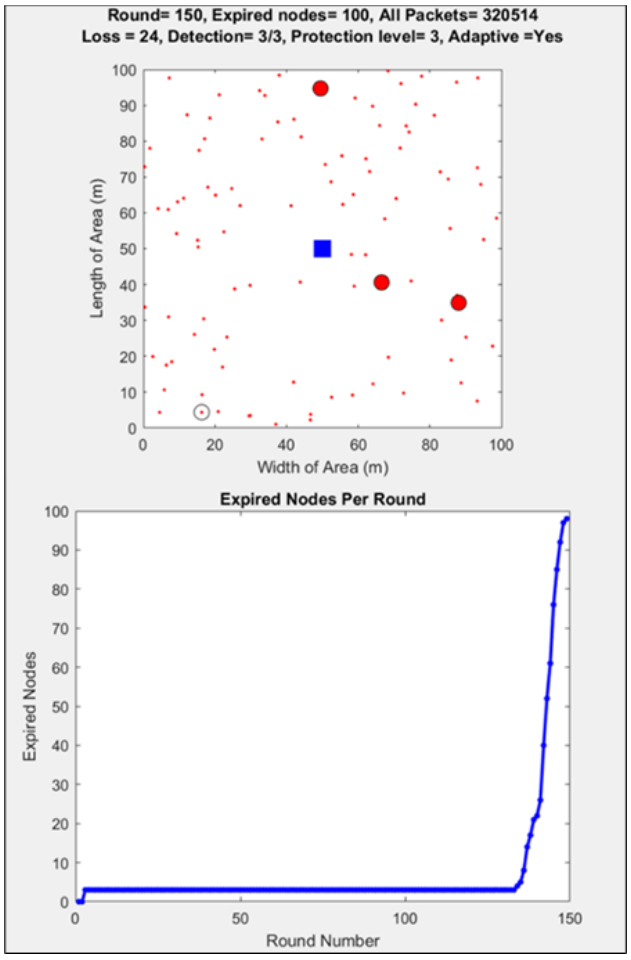

Fig. 3 CSARP Simulation Results

TABLE III
SIMULATION RESULTS FOR DIFFERENT PROTECTION LEVELS

Protection Level	**Level 0 (No protection)**			**Level 1 (Basic Protection, Adaptive Off)**			**Level 2 (Balanced Protection, Adaptive On)**			**Level 3 (Advance Protection, Adaptive On)**		
Malicious nodes No.	None	1 node	3 nodes	None	1 node	3 nodes	None	1 node	3 nodes	None	1 node	3 nodes
Total Rounds	156	158	157	154	155	155	151	153	154	150	149	148
	156	158	158	154	154	154	152	152	154	152	148	153
	158	158	156	153	154	151	159	156	150	147	149	148
	158	157	160	153	154	155	156	152	154	147	148	148
	160	157	160	154	151	153	152	157	156	148	150	149
Average	**158**	**158**	**158**	**154**	**154**	**154**	**154**	**154**	**154**	**149**	**149**	**149**
Detection	0	0	0	0	1	3	0	1	3	0	1	3
	0	0	0	0	1	3	0	1	3	0	1	3
	0	0	0	0	1	3	0	1	3	0	1	3
	0	0	0	0	1	3	0	1	3	0	1	3
	0	0	0	0	1	3	0	1	3	0	1	3
Average	0	0	0	0	1	3	0	1	3	0	1	1
All Packets	254954	248906	240103	296698	296694	284505	301762	284940	278456	345892	336925	336531
	258710	241779	231744	297838	285294	282981	302182	296475	277444	340563	339282	325644
	249412	247819	244606	301163	295564	289282	289578	289242	292239	355006	339918	329962
	250177	246210	233096	302753	295068	287886	294544	302386	275537	352346	347560	327237
	244390	243666	231670	298979	300463	276545	298102	282026	285437	342103	339725	334059
Average	**251529**	**245676**	**236244**	**299486**	**294617**	**284240**	**297234**	**291014**	**281823**	**347182**	**340682**	**330687**
Packet Loss	0	2610	8160	0	14	86	0	18	56	0	18	62
	0	2122	7408	0	26	96	0	28	94	0	18	76
	0	2452	7460	0	18	60	0	14	78	0	32	50
	0	2952	6744	0	20	68	0	22	70	0	10	58
	0	2652	7724	0	18	42	0	14	70	0	14	90
Average	**0**	**2558**	**7499**	**0**	**19**	**70**	**0**	**19**	**74**	**0**	**18**	**67**

Number of rounds (lifetime of the network): the average of the number of rounds for the protection level 0 regardless of the presence of any malicious nodes is 158 rounds while protection level 1 average is 154 rounds. This indicates that there is a 2.5% decrease in the lifetime of the network. Protection level 2 has adaptive protection as an additional feature over protection level 1. The lifetime of the network in level 1 and level 2 is not affected by the existence of the adaptive feature. Protection level 3 will consume an additional 3.2% compared to level 1 and level 2 with a total difference of 5.7% in lifetime between protection level 0 and level 3.

Communicated Packets: There are three types of packets in the simulation, which are the data, Hello, and detection packets. Detection packets will have the same size as the Hello packets. Protection level 0 average of all communicated packet without the presence of any malicious node is 251,529 packets while it averages 236,244 with the presence of 3 malicious nodes. The decrease in communicated packets is 6.1%. Protection level 1 communicated packets averages 299,486, 294,617, and 284,240 packets for the conditions without malicious node, 1 malicious node, 3 malicious nodes respectively. The largest difference between the conditions is 5.1%. Protection level 2 average of communicated packets for all conditions varies with level 1 by 1%. Protection level 3 has 14.6% more communicated packet than level 2, 13.8% more than level 1, and 28% more than level 0. The difference in communicated packets in each round is related to the number of detection packets sent through the network, which has less impact on the lifetime of the network than the data packets. Because of that, while protection level 3 has 28% more communicated data, it has a 5.7% difference in the lifetime of the network.

Packet Loss: In the presence of a 3 malicious node, the network without any protection registered the most packet loss which is 3.2% of all communicated packets which is mostly data packets. In protection levels 1,2, and 3 the largest packet loss average is 74 and the largest packet loss per simulation is 96 out of 282,981. All packets lost in protection levels 1,2, and 3 are Hello and detection packets as all data packets are sent after the detection of malicious nodes.

C. Results Summary

From analysing the findings of the proposed CSARP for MWSNs, the following can be established:

1) The proposed protocol has a detection rate of 100% for all packet dropping attacks. The difference between the protection levels is the speed of detection for malicious nodes with the capability of evading detection by acting legitimately until a specific period inside the TDMA allocated time.
2) As the only few dropped packets in the protection levels 1, 2, and 3 are detection and Hello packets, the protocol has a delivery data package rate of 100% for all legitimate nodes and will not accept any data packets from confirmed malicious nodes.
3) Adaptive protection is helpful in case there is a detection for a malicious node but, the rest of the nodes were already evaluated. When a malicious node is detected, all nodes will be evaluated again to confirm legitimate nodes were not affected by the detected malicious node after being evaluated for the first time.
4) Protection level 1 can consume around 2.5% of the network lifetime but can prevent more than 3.2% of packet loss when there is an attack.
5) The proposed protocol protects the network from packet loss as well as from the capability of malicious nodes to infect other legitimate nodes. The protocol prevents the spread of infection by removing the malicious node out of the network.

6) Despite the type of the packet dropping attack, the attack will be detected by CSARP.

D. Comparing CSARP with LEACH without Security

CSARP is compared to a standard LEACH routing protocol implemented by [38] to compare the lifetime of the network, packet delivery, and packet loss. The simulation conditions are the same as indicated before with a difference only in the number of malicious nodes. The protocols are tested without the presence of any malicious node and with the presence of 10 malicious nodes. Protection level 1 was used for the comparison because it provides basic security with the minimum use of resources. Using 10 malicious nodes was decided to magnify the effect of malicious nodes on the network. Table IV shows the comparison between CSARP and a standard LEACH without security.

TABLE IV
CSARP COMPARISON WITH LEACH

CSARP	Protection Level 1 (Basic Protection, Adaptive Off)			
LEACH	LEACH [38] without security			
Malicious nodes	LEACH None	LEACH 10 node	CSARP None	CSARP 10 nodes
Total Rounds	155	157	154	153
	159	159	154	156
	154	155	153	155
	156	158	153	153
	159	156	154	155
Average	**157**	**157**	**154**	**154**
Detections	0	0	0	10
	0	0	0	10
	0	0	0	10
	0	0	0	10
	0	0	0	10
Average	**0**	**0**	**0**	**10**
All Packets	258176	209373	296698	249750
	252928	206181	297838	245745
	261968	207086	301163	247490
	249114	194800	302753	256434
	249598	204879	298979	250172
Average	**254357**	**294617**	**299486**	**249918**
Packet Loss	0	50440	0	142
	0	46892	0	228
	0	47518	0	248
	0	46598	0	278
	0	43424	0	196
Average	**0**	**46974**	**0**	**218**

The lifetime of the network for LEACH is longer than CSARP with protection by 1.9% on average. The difference in the lifetime is the result of the detection process in the CSARP. LEACH packet loss is 15.944% of all communicated packets, which is mostly data packets. On the other hand, CSARP packet loss is only 0.087% of all packets. All packet loss in CSARP is either detection or Hello packets. All malicious nodes were detected by CSARP and removed from the network while LEACH does not have the ability to detect the presence of malicious nodes. While LEACH has a little longer network lifetime by 1.9%, it has failed to detect any malicious nodes, which resulted in losing 15.944% and added the risk of malicious spread across the network.

Another simulated comparison is conducted between CSARP and LEACH to demonstrate the ability to configure the cluster head ratio in CSARP with comparison to the default setting of cluster head ratio in LEACH [38]. The simulation was conducted with a cluster head ratio of 10% for LEACH and with 1%, 5%, 10%, 15%, and 20% for CSARP. The simulation results are presented in Table V.

TABLE V
CSARP COMPARISON WITH LEACH, CLUSTER HEAD RATIO

CSARP	Protection Level 0 (without protection)		
LEACH	LEACH [38] without security		
Test	LEACH 10%	CSARP 1%	CSARP 5%
Rounds	155	219	174
	159	218	178
	154	220	171
	156	218	174
	159	220	174
Avg.	**157**	**219**	**174**
lifetime	Base 0%	+39.5%	+10.8%
Test	CSARP 10%	CSARP 15%	CSARP 20%
Rounds	156	148	150
	156	148	148
	158	148	148
	158	149	148
	160	148	147
Avg.	**158**	**148**	**148**
lifetime	+0.6%	-6.1%	-6.1%

The simulation results in Table V show improvement in the network lifetime by 0.6% for CSARP without protection against LEACH with similar simulation conditions. CSARP shows improvement by 39.5% when the ratio of the cluster heads is 1%. Changing the cluster head ratio to 15% or 20% resulted in decreasing the network lifetime. The conducted simulation shows that the ability to configure network cluster head ratio could result in significant improvement to the lifetime of the network. Also, the results show that CSARP and LEACH have similar network lifetime with a little improvement for CSARP.

CONCLUSION

This article proposed CSARP protocol that supports different network operating conditions and provides configurable and adaptive detection of packets dropping attacks. The simulations with different conditions showed the ability of CSARP to identify all malicious nodes and remove them from the network. CSARP provided more than 99.97% packets delivery rate with 0% data packet loss in the existence of 3 malicious nodes in comparison with 3.17% data packet loss without using CSARP. When compared with LEACH, CSARP showed an improvement in extending the lifetime of the network by up to 39.5%. The proposed protocol has proven to be better than the available security solutions in terms of configurability, adaptability, optimization for MWSNs, energy consumption optimization, and the suitability for different MWSNs applications and conditions in comparison to the available solutions.

REFERENCES

[1] R. Silva, Z. Zinonos, J. S. Silva and V. Vassiliou, "Mobility in WSNs for critical applications," *2011 IEEE Symposium on Computers and Communications (ISCC)*, 2011. https://doi.org/10.1109/ISCC.2011.5983878

[2] D. Stevanovic and N. Vlajic, "Performance of IEEE 802.15. 4 in wireless sensor networks with a mobile sink implementing various mobility strategies," in *2008 33rd IEEE Conference on Local Computer Networks (LCN)*, 2008. https://doi.org/10.1109/LCN.2008.4664265

[3] A. Al-Nasser, R. Almesaeed and H. Al-Junaid, "A Comprehensive Survey on Routing and Security in Mobile Wireless Sensor Networks," *INTL Journal of Electronics and Telecommunications,* vol. 67, no. 3, pp. 483-496, 2021. https://doi.org/10.24425/ijet.2021.137838

[4] H. Mohapatra and A. K. Rath, "Fault tolerance in WSN through PE-LEACH protocol," *IET wireless sensor systems,* vol. 9, no. 6, pp. 358--365, 2019. http://doi.org/10.1049/iet-wss.2018.5229

[5] L. Zhou, Y. Fang, Q. Wei, Y. Jin and Z. Hu, "LEACH-TLC: a strategy of reducing and uniform energy consumption based on target location constraint," *IET Wireless Sensor Systems,* vol. 9, no. 6, pp. 347--357, 2019. https://doi.org/10.1049/iet-wss.2018.5216

[6] A. Rady, M. Shokair, E.-S. M. El-Rabaie, W. Saad and A. Benaya, "Energy-efficient routing protocol based on sink mobility for wireless sensor networks," *IET Wireless Sensor Systems,* vol. 9, no. 6, pp. 405--415, 2019. https://doi.org/10.1049/iet-wss.2019.0044

[7] H. Al-Behadili, S. AlWane, Y. Al-Yasir, N. Ojaroudi Parchin, P. Olley and R. A. Abd-Alhameed, "The use of multiple mobile sinks in wireless sensor networks for large scale areas," *IET Digital Library,* 2020. https://doi.org/10.1049/iet-wss.2019.0208

[8] H. Mohapatra and A. K. Rath, "Fault tolerance in WSN through PE-LEACH protocol," *IET wireless sensor systems,* vol. 9, no. 6, pp. 358--365, 2019. http://doi.org/10.1049/iet-wss.2018.5229

[9] J. Yin and S. K. Madria, "A hierarchical secure routing protocol against black hole attacks in sensor networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, 2006. http://doi.org/10.1109/SUTC.2006.1636203

[10] S. Shahabi, M. Ghazvini and M. Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack," *Wireless Networks,* vol. 22, no. 5, pp. 1505-1511, 2016. https://doi.org/10.1007/s11276-015-1032-y

[11] L. Teng and Y. Zhang, "SeRA: a secure routing algorithm against sinkhole attacks for mobile wireless sensor networks," in *2010 Second International Conference on Computer Modeling and Simulation*, 2010. https://doi.org/10.1109/ICCMS.2010.95

[12] V. B. Salve, L. Ragha and N. Marathe, "An Enhanced Secure Routing Algorithm Against Sinkhole Attack In Wireless Sensor Networks," *International Journal of Advanced Computational Engineering and Networking,* vol. 2, no. 8, pp. 62-67, 2014.

[13] D. B. Vishwas, C. Chinnaswamy and T. Sreenivas, "An Improved Detection and Mitigation Approach of Sinkhole in," *International Research Journal of Engineering and Technology (IRJET),* vol. 3, no. 6, pp. 808-811, 2016.

[14] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks," *Wksp. Real-World Wireless Sensor Networks*, 2005.

[15] S. Dokurer, "Simulation of Black hole attack in wireless Ad-hoc networks," Atılım University, 2006.

[16] V. V.Kumar and R. R.Kumar, "An adaptive approach for detection of blackhole attack in mobile ad hoc network (ICCC-2015)," *International Conference on Intelligent Computing, Communication & Convergence*, 2015. https://doi.org/10.1016/j.procs.2015.04.122

[17] A. Mathur, T. Newe and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT," *Sensors,* vol. 16, no. 1, p. 118, 2016. https://doi.org/10.3390/s16010118

[18] S. D. Roy, S. A. Singh, S. Choudhury and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management," in *2008 IEEE Symposium on Computers and Communications*, 2008. https://doi.org/10.1109/ISCC.2008.4625768

[19] M. Motamedi and N. Yazdani, "Detection of black hole attack in wireless sensor network using UAV," *2015 7th Conference on Information and Knowledge Technology (IKT)*, 2015. https://doi.org/10.1109/IKT.2015.7288749

[20] H. Gao, R. Wu, M. Cao and C. Zhang, "Detection and defense technology of blackhole attacks in wireless sensor network," in *International Conference on Algorithms and Architectures for Parallel Processing*, 2014. https://doi.org/10.1007/978-3-319-11194-0_53

[21] C. Panos, C. Ntantogian, S. Malliaros and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Computer Networks,* vol. 113, pp. 94-110, 2017. https://doi.org/10.1016/j.comnet.2016.12.006

[22] N. Arya, U. Singh and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in *2015 International Conference on Computer, Communication and Control (IC4)*, 2015. https://doi.org/10.1109/IC4.2015.7375649

[23] D. Virmani, A. Soni and N. Batra, "Reliability analysis to overcome black hole attack in wireless sensor network," *arXiv preprint arXiv:1401.2540,* 2014. https://doi.org/10.48550/arXiv.1401.2540

[24] N. Mistry, D. C. Jinwala, M. Zaveri and others, "Improving AODV protocol against blackhole attacks," *Proceedings of the international multi conference of engineers and computer scientists*, 2010.

[25] P. N. Raj and P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," *arXiv preprint arXiv:0909.2371,* 2009.

[26] L. Tamilselvan and V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET.," *Journal of Networks (JNW),* vol. 3, no. 5, pp. 13-20, 2008. http://doi.org/10.4304/jnw.3.5.13-20

[27] S. S. Ramaswami and S. Upadhyaya, "Smart handling of colluding black hole attacks in MANETs and wireless sensor networks using multipath routing," *IEEE workshop on Info. Assurance. USA*, 2006. http://doi.org/10.1109/IAW.2006.1652103

[28] S. Athmani, D. E. Boubiche and A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," in *2013 World Congress on Computer and Information Technology (WCCIT)*, 2013. https://doi.org/10.1109/WCCIT.2013.6618693

[29] A. A.Dhaka, A. Nandal and R. S. R.Dhaka, "Gray and black hole attack identification using control packets in MANETs," *Procedia Computer Science,* vol. 54, pp. 83-91, 2015. https://doi.org/10.1016/j.procs.2015.06.010

[30] P. Yadav, R. K. Gill and N. Kumar, "A fuzzy based approach to detect black hole attack," *International Journal of Soft Computing and Engineering (IJSCE),* pp. 2231-2307, 2012.

[31] R. Shree, S. K. Dwivedi and R. P. Pandey, "Design Enhancements in ZRP for Detecting Multiple Black Hole Nodes in Mobile Ad Hoc Networks," *International Journal of Computer Applications,* vol. 18, no. 5, pp. 6-10, 2011. http://doi.org/10.5120/2283-2959

[32] D. Virmani, M. Hemrajani, S. Chandel and others, "Exponential trust based mechanism to detect black hole attack in wireless sensor network," *arXiv preprint arXiv:1401.2541,* p. 2014.

[33] V. F. Taylor and D. T. Fokum, "Mitigating black hole attacks in wireless sensor networks using node-resident expert systems," *2014 wireless telecommunications symposium*, 2014. https://doi.org/10.1109/WTS.2014.6835013

[34] C. Wang, T. Feng, J. Kim, G. Wang and W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2009. https://doi.org/10.1109/SAHCN.2009.5168914

[35] S. Misra, K. Bhattarai and G. Xue, "BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks," *2011*

IEEE international conference on communications (ICC), 2011. http://doi.org/10.1109/icc.2011.5962856

[36] J. Shi, X. Wei and W. Zhu, "An efficient algorithm for energy management in wireless sensor networks via employing multiple mobile sinks," *International Journal of Distributed Sensor Networks,* vol. 12, no. 1, 2016. https://doi.org/10.1155/2016/3179587

[37] W. J. Chung and T. H. Cho, "A Multi-Path Routing Determination Method for Improving the Energy Efficiency in Selective Forwarding Attack Detection Based MWSNs," *International Journal of Wireless & Mobile Networks (IJWMN),* vol. 10, no. 4, pp. 9-19, August 2018.

[38] A. Nazari, "Wireless Sensor Networks Simulation," MATLAB Central File Exchange, 2018.

[39] T. C. Hung and H. H. Trung, "Energy Savings in Applications for Wireless Sensor Networks Time Critical Requirements," *International Journal of Computer Networks & Communications (IJCNC),* vol. 8, no. 4, July 2016. http://doi.org/10.5121/ijcnc.2016.8403