REVIEW ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

A Restricted Multipath Routing Algorithm in Wireless Sensor Networks Using a Virtual Cylinder: Bypassing Black hole and Selective Forwarding Attacks

Elham Bahmanih[1], Aso Mohammad Darwesh[2], Mojtaba Jamshidi[2]*, Somaieh Bali[3]

[1]Department of Computer Engineering, Malayer Branch, Islamic Azad University, Malayer, Iran, [2]Department of Information Technology, University of Human Development, Sulaymaniyah, Iraq, [3]Department of Computer Engineering, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran

ABSTRACT

In this paper, a simple and novel routing algorithm is presented to improve the packet delivery in harsh conditions such as selective forwarding and black hole attacks to the wireless sensor networks. The proposed algorithm is based on restricted multipath broadcast based on a virtual cylinder from the source node (SN) to the sink node (SK). In this algorithm, when a packet is broadcast by a SN, a virtual cylinder with radius *w* is created from the SN to a SK. All the nodes located in this virtual cylinder are allowed to forward the packet to the sink. Thus, data are forwarded to sink through multiple paths, but in a restricted manner so that the nodes do not consume a high amount of energy. If there are some compromised nodes in this virtual cylinder, the packets may be forwarded to the sink through other nodes of the virtual cylinder. The proposed algorithm is simulated and evaluated in terms of packet delivery rate and energy consumption. The experiment results show that the proposed algorithm increases packet delivery rate 7 times compared to the single path routing method and reduces energy consumption up to 3 times compared to flooding routing method.

Index Terms: Black hole attack, Restricted multipath, Routing, Selective forwarding attack, Virtual cylinder, Wireless sensor network

1. INTRODUCTION

Today, wireless sensors networks are used in many areas such as environment, military operations, and explorations. Since the sensor nodes have low processing, energy, and memory capabilities and it is important to establish security in such networks due to their application in critical environments especially military, this area has attracted the attention of many researchers Yick *et al.* [1] and Jamshidi *et al.* [2].

So far, various attacks [2]-[11] have been proposed against these networks. Each type of attack has a different mechanism with a different destructive effect and affects various operations and protocols; thus, each one has a different defense mechanism. Two of such dangerous attacks which are very common include black hole (BH) and selective forwarding (*SF*) attacks [10], [11]. To establish these attacks, the adversary enters the network environment, captures one or several legal nodes of the network, reprograms and injects them in the network as

Access this article online

DOI:10.21928/uhdjst.v3n2y2019.pp51-58	**E-ISSN:** 2521-4217 **P-ISSN:** 2521-4209

Corresponding author's e-mail: Mojtaba Jamshidi, Department of Information Technology, University of Human Development, Sulaymaniyah, Iraq. E-mail: jamshidi.mojtaba@gmail.com

Received: 30-07-2019 Accepted: 18-08-2019 Published: 22-8-2019

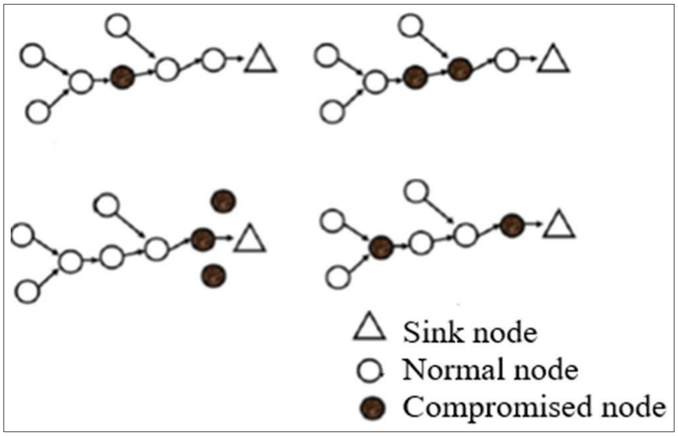

Fig. 1. Different cases of establishing selective forwarding and black hole attacks [11].

compromised nodes. As shown in Fig. 1, such compromised nodes are located along data paths to prevent the packets to reach the sink. That is, the received packets are not forwarded to the sink or base station, but they are dropped. In the *SF* attack, the compromised node only drops some of the received packets, but in the *BH* attack, the compromised node drops all of the received packets.

These two attacks are very destructive for the multi-hop routing algorithms, particularly, if the compromised nodes are located along the data flow paths. On the other hand, establishing these two attacks are very simple and low cost for the adversary. Because the compromised nodes which start these two attacks do not need to perform suspicious operations such as injecting incorrect packet to the network, manipulate data, broadcast false or multiple IDs, and establish a high-speed link; they only need to refuse to forward some of the received packets to the destination. In most cases, even if there is no compromised node in the network, the packets are dropped due to various reasons such as collision [10], [11].

The algorithms which have been proposed to defend against these two attacks like [10], [12]-[23] employ methods such as multiple flow topologies and nodes with special capabilities and multi-hop verification. In general, problems of the presented algorithms include non-scalability, security, complexity, high cost, and slow reaction.

In this paper, a restricted multipath routing algorithm is presented for reliable and low-cost delivery of the data to the destination and defending against *SF* and *BH* attacks in wireless sensor networks such that shortcomings of the previous algorithms are resolved and it can be employed in resource-constraint sensor networks.

2. RELATED WORK

SF attack was first presented in Karlof and Wagner [10], and the first approach to defend against this attack is to use multipath routing protocols. In this method, the packets are forwarded from the source node (SN) to the destination through *n* independent paths. This method is completely robust against *SF* attack until maximum of *n*-1 nodes is captured by the adversary; but, if more than *n*+1 nodes are captured, this method might not operate properly.

It has been mentioned in Satyajayant *et al.* [12] that the *BH* attack is one of the dangerous attacks against wireless sensor networks which can be easily established by the adversary with a low cost. Then, an algorithm has been presented to defend against this attack which is based on multi-sink to protect data flows against *BH* attacks. In this algorithm, sensor nodes employ a set of control messages throughout the network to explore a subset of the sinks. Then, they transmit data to accessible sinks.

In Abasikeleş-Turgut *et al.* [13], an algorithm has been presented to defend against *BH* and sinkhole attacks. This algorithm can be applied to low-energy adaptive clustering hierarchy clustering-based sensor networks. In this study, three different models have been considered, and different mechanisms have been presented to handle them.

In Sheela *et al.* [14], it has been mentioned that *BH* attack is one of the Denial of Service attacks which drops packets. Then, an algorithm based on mobile agents has been proposed to defend against this attack. A mobile agent is a program segment with self-controllability which can be applied to distributed applications, especially dynamic networks. The agents proposed in this study are loaded on several sinks and detect the compromised nodes by patrolling the network.

In Nitesh and Diwaker [15], another algorithm has been proposed based on multiple sinks to defend against *BH* attack. The purpose of this study is to ensure that data are delivered to at least one sink node (SK) by establishing several sinks in different areas of the network and transmitting data to different sinks, simultaneously.

In Deepali and Gupta [16], an adaptive exponential trust-based algorithm has been proposed for calculating the trust factor of each node in each computational cycle for detecting the balckhole *(BH)* attack. Furthermore, it has been claimed that the proposed mechanism not only reduces energy consumption but also it reduces the time required to detect the *BH* attack. Furthermore, an adaptive threshold has been used to reduce false alarm rates.

In Baishali [17], an algorithm has been proposed to defend against *BH* attack in mobile *ad hoc* networks. This algorithm can detect the compromised nodes in a network which employs the *Ad hoc* On-Demand Distance Vector algorithm. In this algorithm, nodes use a timer to wait for the acknowledgment (ACKs) to return. If the timer is reset and the ACK is not received, *BH* attack along data transmission path is detected.

In Shila *et al.* [18], a channel-aware algorithm has been proposed, which detects compromising behavior of the nodes from the bad behavior of the transmission channel. This algorithm is based on channel estimation and traffic monitoring strategies. If the supervised missing rate is higher than the estimated normal missing rate, those nodes are detected as an adversary.

In Li *et al.* [19], an algorithm based on sequential mesh test based has been presented for detection of *SF* attack in sensor networks. This scheme is centralized and operates on cluster-based networks. The sensor node *u* transmits its packets to the next hop, node *v*, and if node *v* does not transmit the packet in constant time, node *u* reports to the cluster head that the packet has been dropped. After receiving packet drop reports, the cluster head applies the sequential mesh test based on the suspicious node.

In Hu *et al.* [20], a secure routing algorithm based on monitoring node and trust mechanism has been proposed. In this algorithm, trust is adjusted based on the transmission rate of the packets and residual energy of the node. This detection and routing algorithm is general because it considers both the lifetime of the network and its security.

In Yu and Xiao [21], another algorithm has been presented in which a multi-hop acknowledgment scheme is used considering the responses received from the intermediate nodes to broadcast the warning messages in the network. In this algorithm, each intermediate node along the data transmission route cooperates in detecting the compromised node. If an intermediate node observes a bad behavior from its upstream or downstream node, it generates an alarm packet and transmits it to the SN or the base station. Then, the SN and the base station can make a decision and respond using a complicated intrusion detection system.

In Xiao *et al.* [22], a technique has been proposed for detecting the compromised nodes in the *SF* attack. This algorithm is the improved version of the previous technique [21]. In this algorithm, some of the intermediate nodes along the route are selected as checkpoint nodes randomly which have to generate ACKs for each received packet. Furthermore, each node requires a one-way hash key chain to ensure that the packets are authenticated. Furthermore, delay mechanisms are used to transmit this one-way hash key. In this algorithm, each intermediate node along the packet transmission route has the potential to explore the packets which are lost abnormally, and if the intermediate node does not receive enough ACKs from the downstream checkpoints, it can detect the compromised nodes.

3. MULTI-SINK ARCHITECTURE

In each wireless sensor network, there is usually one or more sensor nodes called SK which collects total data of the network. Destination of all reported packets in sensor networks is the SKs. When sensor nodes observe a determined event, they generate the required report packets and deliver them to the sink through multi-hop routing algorithms. Considering the number of the SKs, their location, and they are being mobile or stationary, various architectures are created in the network which might change mechanism of the routing algorithms [23,24].

One of the common architectures is multi-sink architecture. In this architecture, as shown in Fig. 2, there are several SKs established on one side of the network. The SKs might either communicate directly with each other or communicate with the base station (where the network manager is located). In this architecture, the sufficient condition for data delivery is that data are delivered to at least one of the sinks. In other words, the packet generated by one sensor node does not have to be delivered to a specific SK, but it is sufficient that is delivered to one of the sinks. This architecture has three main advantages [23,24]:

3.1. Increasing Network Lifetime

If there is only one sink in the network, its neighboring sensor nodes transmit high traffic, and their energy is discharged very soon, which reduces network lifetime. However, if the multi-sink architecture is used, this problem is resolved.

3.2. Load Balancing

Multiple sinks in the network might result in several routing trees in the network which might balance load among nodes of the network.

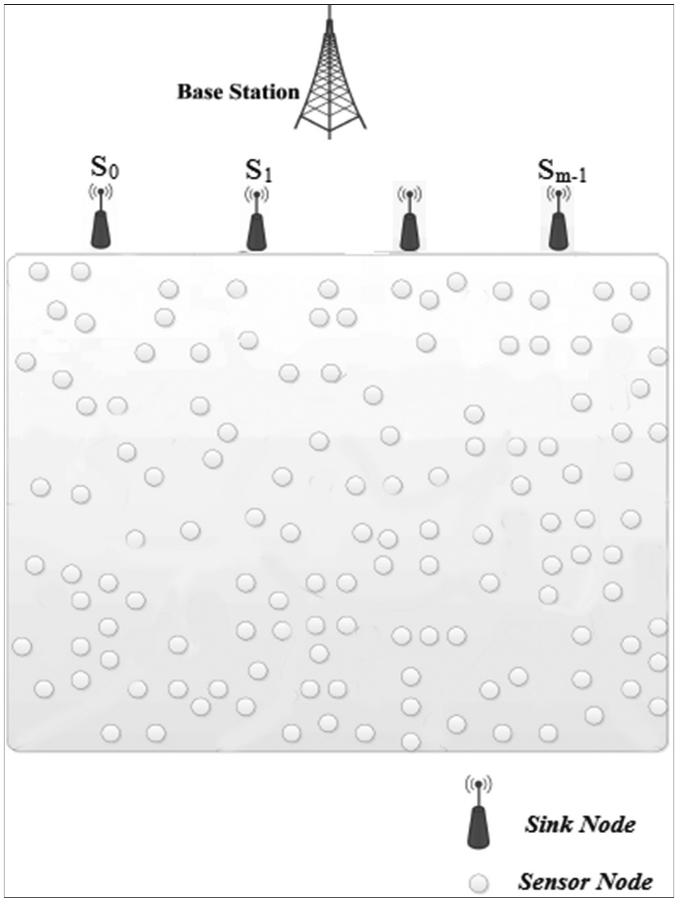

Fig. 2. An example of a sensor network with multi-sink architecture.

3.3. High Packet Delivery Rate

It is obvious that when there are several sinks in the network, the probability of delivering the packets to the destination increases because of the probability that there exists a route from the source to the destination (sink), especially in low-density networks, increases.

Considering the features and advantages of the multi-sink architecture, it is used in this paper to design the proposed routing algorithm to defend against *SF* and *BH* attacks.

4. SYSTEM ASSUMPTIONS

Sensor networks are categorized into three main groups including SKs, SNs, and forwarding nodes (FNs). The SNs generate the report packets. The packets generated by the SNs are delivered to the SKs through FNs. For instance, SNs might be deployed in the boundary areas or the adversary environment and generate the required reports in case of adversary operations and deliver the reports to the sink through multiple hops. Each node has a unique ID and is aware of its location. The network area of interest is a 2D environment in which SNs, SKs, and FNs are deployed randomly. All nodes have the same radio range equal to *r*. Furthermore, it is assumed that the nodes communicate with each other through the wireless radio channel and employ the omnidirectional broadcast. Furthermore, it is assumed that the SNs are not only aware of their location but also they are aware of the location of the SKs. The network environment is not safe, and the adversary can capture some sensor nodes and reprogram them as compromised nodes.

5. THE PROPOSED ALGORITHM

Although using single-path approaches for delivering data to the destination in sensor networks imposes low overhead to the nodes, it cannot ensure that parasite generation, etc., is not established in the network particularly in case of *SF* and *BH* attacks. Also, the flooding method, although more reliable, imposes much overhead on the nodes of the network. Thus, they are not cost-effective. In this section, a restricted multi-path approach is proposed for reliable and cost-effective delivery of data to the destination such that it overcomes *SF* and *BH* attacks in the sensor network and delivers data to the sinks with high reliability.

In the proposed method, a virtual cylinder (with diameter 2*w*) is created from the SN to a SK and only the nodes in this cylinder are allowed to forward packets to the destination. Each SN inserts its spatial coordinate (L_v) in the packet while generating a data packet. Then, the packet is broadcast so that all of its neighbors receive it. However, only the nodes adjacent to the virtual cylinder forward the received packet. Each node which has received the packet, for example, node*v*, first extracts the spatial coordinate of the SN which has generated this packet and compares it with its own spatial coordinate, L_v, to find out if it is in the virtual cylinder or not. If node *v* is inside the virtual cylinder, it forwards the packet; otherwise, it drops the received packet. This process is continued until the packet is delivered to the sink through restricted multiple paths. Therefore, if there is a compromised node along one path, the packets can be delivered to the sink through adjacent paths using the proposed method.

In the following, details of the proposed algorithm are described considering Fig. 3. It is assumed that the SN *A* intends to transmit a report packet to the sink S_1. In this case, the routing vector is defined as AS_1 . The packet is passed

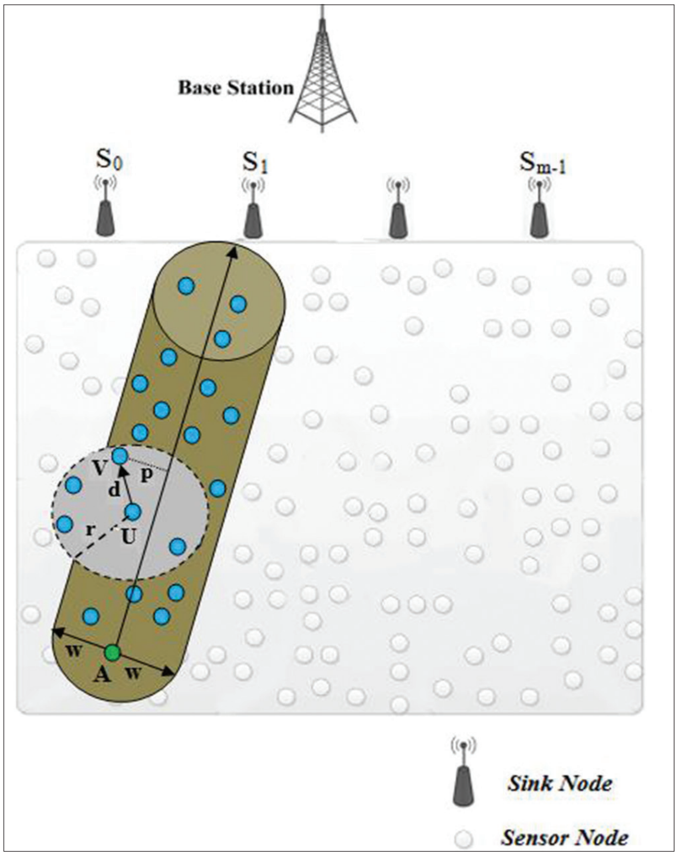

Fig. 3. The proposed virtual cylinder.

in the range of the routing vector from a virtual routing cylinder with a predetermined radius of w to reach the destination.

Assuming that the SK S_1 is located in the spatial coordinate of $(x_s - y_s)$ and the SN A is located in the spatial coordinate of $(x_A - y_A)$, then the equation of the line passing through these points and the vector passing center of the virtual cylinder are calculated as Equation (1):

$$y - y_0 = m(x - x_0) \tag{1}$$

$$y_s - y_A = m(x_s - x_A)$$

Here, m is the slope of the line calculated using Equation (2):

$$m = \frac{y_A - y_s}{x_A - y_s} \tag{2}$$

The SN A calculates the equation of the line passing from itself and the SK S_1 and inserts it along with the report data in a packet and broadcasts it. This packet is forwarded to the sink by the nodes located in the virtual cylinder. Assuming that the radio range of the nodes is r, the packet broadcast by each sensor node is broadcast in the radius of r, and each node which is located in this area receives the packet.

Each node which receives the report packet extracts the equation of the line inserted in this packet and calculates its distance from this line. It should be noted that the line equation is calculated only once by the SN, and it is inserted in the report packets. The FNs do not need to calculate the line equation, but it is sufficient to calculate their distance from the line. When a packet is transmitted by a node inside the virtual cylinder, like node U in Fig. 3, all nodes located in its radio range, receive the packet. Node U has four neighbors where two of them are outside the virtual cylinder and two other nodes are inside the virtual cylinder. Each node adjacent to node U, like node V, calculates its distance from the central line of the virtual cylinder, P, according to theorem 1.

Theorem 1: Assuming that $\vec{A}$ and $\vec{B}$ are two points on the 2D space of the line $\vec{L}$ and $\vec{P}$ is an independent point which is not on this line, the line vector equation is as (3):

$$\vec{A} + t\vec{M} \tag{3}$$

Here,

$\vec{M}$ is the direction vector obtained using (4):

$$\vec{M} = \vec{B} - \vec{A} \tag{4}$$

And t is a running parameter calculated according to (5):

$$t = \frac{\left(\vec{P} - \vec{A}\right)\bullet\vec{M}}{\vec{M} \bullet \vec{M}} \tag{5}$$

Now, the distance of $\vec{P}$ from line $\vec{L}$ is calculated as (6):

$$p = \left|\vec{P} - (\vec{A} + t\vec{M})\right| \tag{6}$$

Proof of this theorem is given in Equation [25].

For each node V which receives the report packet, if its distance from the central line of the virtual cylinder is smaller than w, means $p \leq w$, the receiver node V is inside the virtual cylinder and it is allowed to forward the received packet. Otherwise, $p > w$, node V is outside the virtual cylinder and should not forward the received packet.

Furthermore, in the proposed algorithm, each sensor node has a buffer which stores the ID of the last packet forwarded from each SN as a result of which the sensor node refuses to repetitive packets. Since all the SNs located in the virtual cylinder forward the packets, a packet moves toward the corresponding sink through multiple paths (inside the cylinder). Thus, if some of the nodes located inside the cylinder are compromised by an adversary and drop the report packets (*SF* and *BH* attacks), it is still probable that the packets are delivered to the sink through other paths. On the other hand, multipath is controlled by the virtual cylinder to prevent a packet from being broadcast in the whole network and prevent high energy consumption.

6. SIMULATION RESULTS

In this section, the proposed algorithm is evaluated and its simulation results are presented. MATLAB is used to simulate the proposed algorithm.

6.1. Simulation Model

In the simulation model, the network is comprised of $N = 300$ sensor nodes which are deployed in a 100 × 100 m area, randomly. The network includes three SNs where each SN generates a packet at each simulation instant and transmits it to the sink. The nodes have GPS and are aware of their location. SNs are located in a fixed and specific location of the boundary area of the network. The network includes $m = 3$ SKs which are located in the network environment. SNs are aware of the location of the SKs. The radio range of the nodes is $r = 10$ m. The radius of the virtual cylinder is w meters. Furthermore, it is assumed that the network is comprised of *SF* compromised nodes which establish the SF attack and *BH* compromised nodes which establish the *BH* attack. The compromised nodes which establish the *BH* attack drop all the received packets but the compromised nodes which establish the *SF*, drop only 50% of the received packets. The initial energy of every node is set to be 10 Joules. Energy consumption for transmission and reception of the packet is 0.016 and 0.0016 joules. Each experiment is repeated 50 times, and the final result is the average of these 50 runs.

6.2. Evaluation Metrics and Compared Algorithms

The evaluation metrics are as follows:

6.2.1. Packet delivery rate

Packet delivery rate is the number of the packets received by the sinks to the number of the packets generated by the SNs.

6.2.2. Average residual energy

Average residual energy is the average residual energy of sensor nodes after simulation time. To calculate this metric, the energy of the compromised nodes and SKs is not considered. It is assumed that the compromised nodes and SKs have no energy limitation.

Since the proposed algorithm is a restricted multipath algorithm; that is, packets are only transmitted to the sinks through the nodes located on the virtual cylinder. Thus, its efficiency is compared with the single-path and flooding methods. In the single-path algorithm, the SN transmits data to a SK through one path (shortest path). In the flooding method, packets are broadcasted in the whole network to reach the SKs. It is clear that in the single-path method, the minimum energy is consumed, but the packet delivery rate might be low especially if the compromised nodes of the *SF* or *BH* attack exist along the data path. However, in the flooding method, the data delivery rate is high even when there is a large number of compromised nodes in the network, but the energy consumption of this algorithm is very high. The proposed algorithm is between these two algorithms. That is, it tries to control energy consumption and keep the packet delivery rate at an acceptable level when there exist *SF* and *BH* attacks, by adopting a restricted multipath method.

6.3. Experiment Results

6.3.1. Experiment 1

In this experiment, the efficiency of the proposed algorithm is evaluated in terms of packet delivery rate and energy consumption, and the results are compared with single-path and flooding methods. In this experiment, $SF = 25$, $BH = 25$, and w=15, this experiment is executed for periods of 25–100 s. At each simulation instant, each SN generates and broadcasts a packet.

The results of this experiment in terms of packet delivery rate and average residual energy are given in Figs. 4 and 5, respectively. The results show that the packet delivery rate of the flooding algorithm is almost 100% while it is 90% and 12% for the proposed algorithm and the single-path algorithm, respectively. In the flooding algorithm, since each packet is broadcast in the network, it is forwarded to the sinks through different paths. Thus, despite *SF* and *BH* attacks, at least one version of this packet reaches one of the sinks. However, as shown in Fig. 5, the flooding algorithm discharges energy of the nodes significantly because there are a large number of transmission and reception operations for one packet in the network.

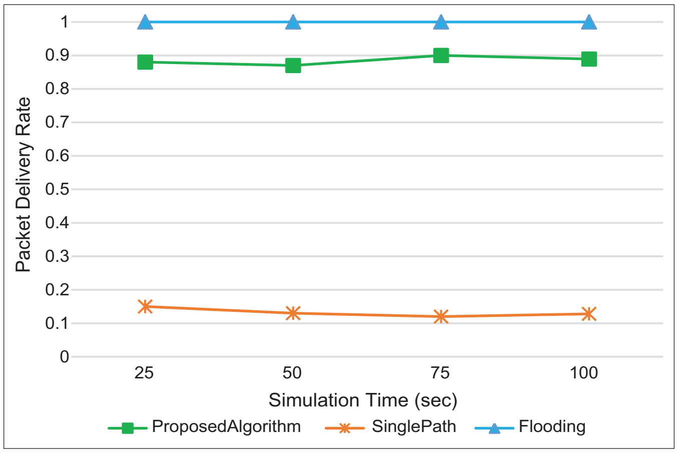

Fig. 4. Comparing the efficiency of the proposed algorithm with the single-path and the flooding algorithms in terms of the packet delivery rate.

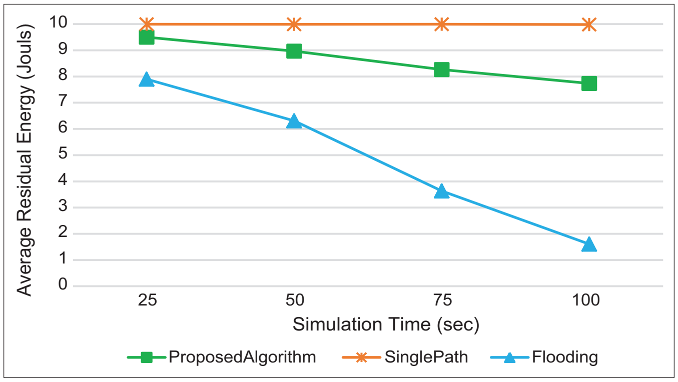

Fig. 5. Comparing the efficiency of the proposed algorithm with the single-path and the flooding algorithm in terms of the average residual energy.

In the single-path algorithm, packets are forwarded to a SK through the shortest path greedily. Thus, if there is a compromised node along this path, it prevents the packet to reach the destination as a result of which the packet delivery rate is reduced significantly. However, as shown in Fig. 5, this method is very optimal in terms of energy consumption because no additional or repetitive packet is broadcast in the network.

However, the proposed algorithm tries to forward the packets through restricted multiple paths and the virtual cylinder toward a SK. Hence, even if there exist compromised nodes, the packets can be delivered through different paths. Therefore, the packet delivery rate is acceptable. On the other hand, energy consumption is much less than the flooding algorithm.

6.3.2. Experiment 2

In this experiment, the effect of the radius of the virtual cylinder, *w*, on the efficiency of the proposed algorithm in terms of packet delivery rate and the energy consumption is investigated. In this experiment, *SF* = 25, *BH* =25, and *w* = 5~20 and its effect on the efficiency of the proposed algorithm are investigated. The simulation time is considered to be 50 s. The results of this experiment are given in Fig. 6 and Fig. 7 for the packet delivery rate and average residual energy of the nodes, respectively.

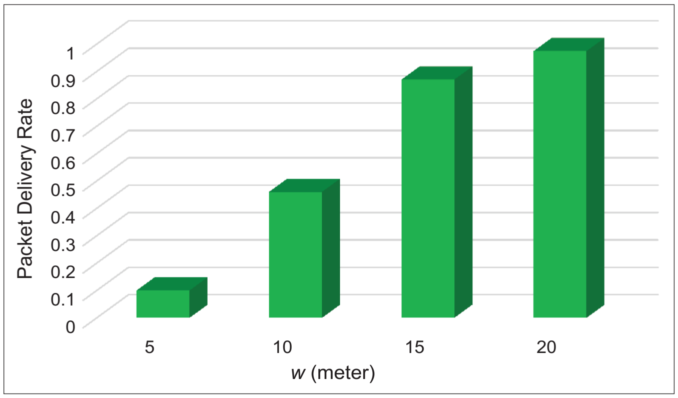

Fig. 6. The effect of the radius of the virtual cylinder, *w*, on the packet delivery rate of the proposed algorithm.

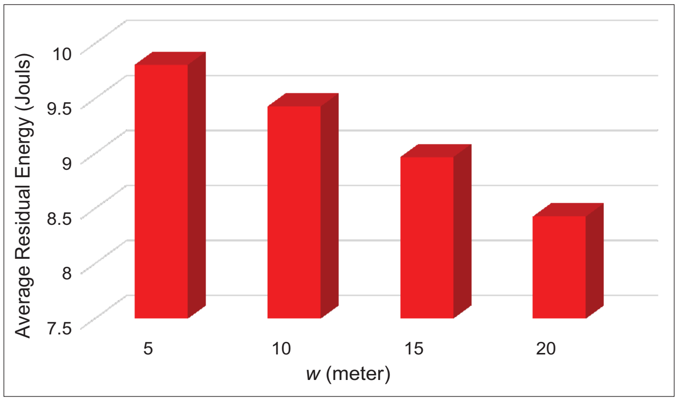

Fig. 7. The effect of the radius of the virtual cylinder, *w*, on the average residual energy of the proposed algorithm.

As can be seen, *w* affects the efficiency of the proposed algorithm, significantly. By increasing *w*, the radius of the virtual cylinder becomes larger and covers more nodes as a result of which, packets are forwarded to the sink through more paths which increase packet delivery rate and energy consumption.

7. CONCLUSION

In this paper, a novel and simple routing algorithm is presented to reduce the destructive effects of these attacks.

The proposed algorithm is based on restricted multipath broadcast based on a virtual cylinder from the SN to the SK. In this algorithm, when a packet is broadcast by a SN, a virtual cylinder is created from the SN to one of the SKs of the network. All the nodes located on this virtual cylinder are allowed to forward packets to the sink. Thus, data are forwarded to the sinks through multiple restricted and adjacent paths. The proposed algorithm is simulated and evaluated in terms of packet delivery rate and energy consumption. The results of the proposed algorithm are compared with single-path and flooding algorithms. The comparison results show that the proposed algorithm is 7 times better than the single-path algorithm in terms of packet delivery rate, and it is 3 times better than the flooding algorithm in terms of energy consumption.

REFERENCES

[1] J. Yick, B. Mukherjee and D. Ghosal. Wireless sensor network survey. *Computer Networks*, vol. 52, no. 12, pp. 2292-2330, 2008.

[2] M. Jamshidi, M. Esnaashari, A. M. Darwesh and M. R. Meybodi. Detecting sybil nodes in stationary wireless sensor networks using learning automaton and client puzzles. *IET Communications*, vol. 13, no. 13, pp. 1988-1997, 2019.

[3] M. Jamshidi, E. Zangeneh, M. Esnaashari and M. R. Meybodi. A lightweight algorithm for detecting mobile sybil nodes in mobile wireless sensor networks. *Computers and Electrical Engineering*, vol. 64, pp. 220-232, 2017.

[4] M. Jamshidi, S.S.A. Poor, N.N. Qader, M. Esnaashari and M.R. Meybodi. A lightweight algorithm against replica node attack in mobile wireless sensor networks using learning agents. *IEIE Transactions on Smart Processing and Computing*, vol. 8, no. 1, pp. 58-70, 2019.

[5] M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh and M. R. Meybodi. A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it. *Wireless Personal Communications*, vol. 105, no. 1, pp. 145-173, 2019.

[6] M. Jamshidi, M. Ranjbari, M. Esnaashari, A.M. Darwesh and M.R. Meybodi. A new algorithm to defend against sybil attack in static wireless sensor networks using mobile observer sensor nodes. *Adhoc and Sensor Wireless Networks*, vol. 43, pp. 213-238, 2019.

[7] M. Jamshidi, M. Ranjbari, M. Esnaashari, N. N. Qader and M. R. Meybodi. Sybil node detection in mobile wireless sensor networks using observer nodes. *JOIV: International Journal on Informatics Visualization*, vol. 2, no. 3, pp. 159-165, 2018.

[8] A. Andalib, M. Jamshidi, F. Andalib and D. Momeni. A lightweight algorithm for detecting sybil attack in mobile wireless sensor networks using sink nodes. *International Journal of Computer Applications Technology and Research*, vol. 5, no. 7, pp. 433-438, 2016.

[9] M. Jamshidi, A.M. Darwesh, A. Lorenc, M. Ranjbari and M.R. Meybodi. A precise algorithm for detecting malicious sybil nodes in mobile wireless sensor networks. *IEIE Transactions on Smart Processing and Computing*, vol. 7, no. 6, pp. 457-466, 2018.

[10] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, vol. 1, pp. 299-302, 2003.

[11] *L. K.* Bysani *and A. K. Turuk.* A Survey On Selective Forwarding Attack in Wireless Sensor Networks. *Proceedings of the International Conference on Device and Communications (ICDeCom)*, Mesra, India, Feb. 2011.

[12] M. Satyajayant, K. Bhattarai and G. Xue. BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. In *2011 IEEE International Conference on Communications (ICC)*, IEEE, 2011, pp. 1-5.

[13] I. Abasikeleş-Turgut, M. N. Aydin and K. Tohma. A realistic modelling of the sinkhole and the black hole attacks in cluster-based WSNs. *International Journal of Electronics and Electrical Engineering,* vol. 4, no. 1, pp. 74-78, Feb. 2016.

[14] D. Sheela, V. R. Srividhya, B. A. Asma and G. M. Chidanand. Detecting Black Hole Attacks in Wireless Sensor Networks Using Mobile Agent. *In International Conference on Artificial Intelligence and Embedded Systems (ICAIES*, 2012, pp. 15-16.

[15] G. Nitesh and C. Diwaker. Detecting blackhole attack in WSN by check agent using multiple base stations. *American International Journal of Research in Science, Technology, Engineering and Mathematics,* vol. 3, no. 2, pp. 149-152, 2013.

[16] V. Deepali and P. Gupta. Adaptive exponential trust-based algorithm in wireless sensor network to detect black hole and gray hole attacks. In: *Emerging Research in Computing, Information, Communication and Applications*. Springer, Singapore, 2016, pp. 65-73.

[17] G. Baishali. A novel intrusion detection system for detecting black-hole nodes in manets. *Networks (GRAPH-HOC)*, vol. 8, no. 2, pp. 1-13, 2016.

[18] D. M. Shila, Y. Cheng, T. Anjali. Mitigating selective forwarding attacks with a channel-aware approach in WMNs. *IEEE Transaction on Wireless Communications*, vol. 9, no. 5, pp. 1661-1675, 2010.

[19] G. Li, X. Liu and C. Wang. A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks. In: *Proceeding of the International Conference on Networking, Sensing and Control (ICNSC)*, 2010, pp. 554-558.

[20] Y. Hu, Y. Wu and H. Wang. Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN. *Wireless Sensor Network*, vol. 6, pp. 237-248, 2014.

[21] B. Yu and B. Xiao. *Detecting Selective Forwarding Attacks in Wireless Sensor Networks*. In: Proceeding of the Second International Workshop on Security in Systems and Networks (IPDPS Workshop), 2006.

[22] B. Xiao, B. Yu and C. Gao. CHEMAS: Identify suspect nodes in selective forwarding attacks. *Journal of Parallel and Distributed Computing*, vol. 67, no. 11, pp. 1218-1230, 2007.

[23] W. K. Seach, H. X. Tan. Multipath Virtual Sink Architecture for Underwater Sensor Networks. In: *Proceeding of OCEANS*, 2006.

[24] M. Jamshidi, A. A. Shaltooki, Z. D. Zadeh and A. M. Darwesh. A dynamic ID assignment mechanism to defend against node replication attack in static wireless sensor networks. *JOIV: International Journal on Informatics Visualization*, vol. 3, no. 1, pp. 13-17, 2019.

[25] Available from: https://www.monkeyproofsolutions.nl/how-to-calculate-the-shortest-distance-between-a-point-and-a-line. [Last accessed on 2019 Jul 10 July].