1-1-2024

# A Reputation-Based AODV Protocol for Blackhole and Malfunction Nodes Detection and Avoidance

Qussai M. Yaseen
*Ajman University*

Monther Aldwairi
*Jordan University of Science and Technology*

Ahmad Manasrah
*Yarmouk University*

Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.051179

ARTICLE

# A Reputation-Based AODV Protocol for Blackhole and Malfunction Nodes Detection and Avoidance

**Qussai M. Yaseen[1,2,*], Monther Aldwairi[2,3] and Ahmad Manasrah[4,5]**

[1]Artificial Intelligence Research Center (AIRC), College of Engineering and Information Technology, Ajman University, Ajman, 346, United Arab Emirates

[2]Department of Computer Information Systems, Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid, 22110, Jordan

[3]College of Technological Innovation, Zayed University, Abu Dhabi, 144534, United Arab Emirates

[4]Faculty of Information Technology and Computer Science, Yarmouk University, Irbid, 21163, Jordan

[5]Computer Information Systems, Higher Colleges of Technology, Sharjah, 341214, United Arab Emirates

*Corresponding Author: Qussai M. Yaseen. Email: q.yaseeen@ajman.ac.ae

Received: 28 February 2024 Accepted: 11 June 2024 Published: 15 August 2024

## ABSTRACT

Enhancing the security of Wireless Sensor Networks (WSNs) improves the usability of their applications. Therefore, finding solutions to various attacks, such as the blackhole attack, is crucial for the success of WSN applications. This paper proposes an enhanced version of the AODV (Ad Hoc On-Demand Distance Vector) protocol capable of detecting blackholes and malfunctioning benign nodes in WSNs, thereby avoiding them when delivering packets. The proposed version employs a network-based reputation system to select the best and most secure path to a destination. To achieve this goal, the proposed version utilizes the Watchdogs/Pathrater mechanisms in AODV to gather and broadcast reputations to all network nodes to build the network-based reputation system. To minimize the network overhead of the proposed approach, the paper uses reputation aggregator nodes only for forwarding reputation tables. Moreover, to reduce the overhead of updating reputation tables, the paper proposes three mechanisms, which are the prompt broadcast, the regular broadcast, and the light broadcast approaches. The proposed enhanced version has been designed to perform effectively in dynamic environments such as mobile WSNs where nodes, including blackholes, move continuously, which is considered a challenge for other protocols. Using the proposed enhanced protocol, a node evaluates the security of different routes to a destination and can select the most secure routing path. The paper provides an algorithm that explains the proposed protocol in detail and demonstrates a case study that shows the operations of calculating and updating reputation values when nodes move across different zones. Furthermore, the paper discusses the proposed approach's overhead analysis to prove the proposed enhancement's correctness and applicability.

## KEYWORDS

AODV; blackhole; malfunction nodes; pathrater; reputation system; wireless sensor networks (WSNs); watchdogs

## 1 Introduction

Wireless Sensor Networks (WSNs) utilize affordable, battery-operated, and straightforward processing sensors, which are composed of wireless radio devices and operate by creating widely distributed wireless sensor networks. These sensor nodes are commonly deployed for numerous purposes, including monitoring weather conditions such as temperature and humidity, as well as physical phenomena, in the military, in building industrial monitoring, and in automation [1]. WSNs have dynamic topology and can be formed and run quickly, which reduces time and money requirements. To communicate, WSNs sensors may use a multi-hop communication approach, which requires collaboration among sensors to send packets to destinations.

Sensors in WSNs can be static or mobile. A node works as a sender or a receiver of a packet or as a router. WSNs have special uses in dynamic environments such as disaster areas, military fields, personal area networks, etc. In addition, Unmanned Aerial Vehicles (UAVs) communication is a very important and sensitive example of WSNs [2–4]. Therefore, improving communication in a wireless network environment directly impacts UAVs' usability and their numerous military and civilian applications. The dynamic topology and sensor mobility in WSNs provide some advantages, such as the absence of a single point of failure. Nonetheless, WSNs need special protocols to send and receive packets because the dynamic topology changes frequently [3,5]. There are three classes of WSNs protocols, which are table-driven (proactive), on-demand (reactive), and hybrid protocols.

Table-driven or proactive protocols, such as the Optimized Link State Routing Protocol (OLSR) [6] and the Virtual Routing Protocol (VRP) [7], maintain an up-to-date topology of the entire network, allowing source nodes to have prior knowledge and store the route to the destination in their table when they need to send a packet. Link-state and distance vector protocols are classes of proactive protocols. Link-state protocols have an important advantage over distance vector protocols, which is fast convergence. However, link state protocols need more control traffic packets.

Reactive routing protocols, such as the Ad Hoc On-Demand Distance Vector protocol (AODV) and the Dynamic Source Routing protocol (DSR) [8], do not use a map of the network as in proactive protocols. Instead, they build routes to destinations on demand. To achieve that, when a source node wants to send a message to a destination, the source node broadcasts a request searching for a route to the destination. The request is forwarded by intermediate sensors until finding the destination, which helps discover and build a route to the destination. Hybrid protocols, such as the Zone Routing Protocol (ZRP) [9], merge proactive and reactive approaches in a hybrid approach. This protocol type utilizes a proactive approach to establish neighboring zones and a reactive approach to discover and construct routes between zones. To determine whether neighboring nodes are alive, a *hello* message is sent regularly to maintain neighboring zones, which ensures that routes to neighbors are readily available. Hybrid protocols aim to minimize the delay and traffic required to build a route when sending packets to nearby nodes, while routes to distant nodes are created only on demand. This assertion assumes that the majority of traffic in WSNs is directed towards nearby nodes.

Securing WSNs' routing protocols, such as AODV, DSR, Geographic Routing Protocol (GRP), and OLSR, is crucial in many communications systems. Therefore, their security issues should be addressed and resolved to avoid attacks. WSNs have many security problems, such as poisoning, routing table overflow, packet replication, wormholes, snooping, and denial of service (DoS) attacks [10]. The blackhole problem is considered a popular security issue in WSNs. A blackhole node claims itself as the shortest path to the destination when it receives a path broadcast request; however, when it receives a packet to forward to the destination, it drops it. Blackhole attacks are classified into single or collaborative attacks. In single blackhole attacks, blackhole nodes work independently and drop

packets without collaborating with other blackhole nodes. However, in collaborative blackhole attacks, two or more blackhole nodes collaborate to drop packets, which makes detection more difficult.

This paper discusses the problem of blackhole detection in WSNs. The contribution of the paper is as follows:

1. The paper proposes an enhanced version of the AODV protocol that considers the moving Blackholes problem when routing packets in WSNs.
2. The enhanced AODV protocol mitigates the problem of blackhole nodes or misbehaving nodes by maintaining and using a reputation table for all nodes in WSNS.
3. The enhanced AODV mitigates blackhole problem with reasonable traffic and processing overhead with the help of reputation aggregators.
4. An algorithm for the proposed protocol and the approach has been added and discussed in detail.
5. A case study that proves the correctness of the proposed enhanced AODV in detecting and avoiding blackholes is provided.
6. An overhead analysis that proves the applicability of the enhanced AODV is provided.

We should mention here that this work is a continuation of the research initiated in [11], aiming to develop a reliable and effective protocol for selecting the best and safest routes in mobile networks. This work significantly enhances and improves the AODV protocol, provides a detailed discussion of the proposed protocol, and presents a comprehensive algorithm for the enhanced AODV. Furthermore, this work analyzes the enhanced AODV protocol through a case study demonstrating how it enhances the detection of blackholes and malfunctioning nodes. Additionally, this work evaluates the overhead of the proposed protocol and demonstrates its applicability.

The rest of the paper is organized as follows. The next section discusses some related work. Section 3 provides some preliminaries to understand the contents of the paper better. Section 4 introduces the proposed protocol. Section 5 discusses the case study. Section 6 provides the overhead analysis. Section 7 compares some related work and the proposed approach. Finally, Section 8 concludes the work.

## 2 Related Work

Many approaches have been proposed to mitigate the problem of single and collaborative blackhole attacks. Sun et al. [12] proposed an approach to detect blackhole nodes based on node feedback and a routing recovery mechanism that builds a good path to the destination. However, the proposed approach is used for detecting single blackholes in the AODV protocol, and it is not appropriate for detecting collaborative blackhole attacks. Similarly, Al-Shurman et al. [13] suggested two methods to discover single blackholes in the AODV protocol. The first method takes advantage of the multiple paths to a destination. Their work is based on the existence of multiple paths to select a safe path, but the authors did not specify how they identify a safe route from redundant paths. In the second method, the authors claimed that they could detect blackhole nodes based on a unique sequence number in packets, where accumulated data can be utilized by sender nodes to discover malicious nodes. However, in their work, no reputation values are shared among nodes in WSNs, enabling blackholes to avoid detection when moving to new locations.

Yang et al. [14] proposed TADR-EAODV, a Trust-Aware Dynamic Routing algorithm based on the Extended AODV protocol. The proposed protocol was developed to assess the distributed safety level of nodes in routing using AODV. TADR-EAODV considers criteria such as direct trust, suggested

trust, connectivity strength, energy rate, and worthiness score. TADR-EAODV employs centralized ensemble clustering for node grouping, which enables clustering-based routing to improve WSN performance. The authors tested the proposed protocol against denial-of-service attacks to evaluate its effectiveness. Based on their experiments, the results demonstrated that the high-performance TADR-EAODV can identify attackers by identifying unusual activity.

Quincozes et al. [15] proposed a machine learning model to defend WSNs against denial-of-service attacks. The authors considered three feature selection strategies and covered supervised and unsupervised ML (Machine Learning) techniques. The evaluations were based on DoS attacks, including Flooding, Grayhole, and Blackhole, using a publicly available dataset derived from WSNs. Additionally, they investigated adjustable parameters to enhance the performance of unsupervised approaches. The measures of accuracy, recall, precision, F1-Score, and processing time were used to direct experimental comparison. The results showed that among the analyzed ML algorithms, supervised techniques outperform unsupervised ones; the REPTree with the OneR feature selection algorithm had the greatest F1-Score (95.69%) for identifying blackhole assaults.

Tamilselvan et al. [16] introduced an approach for detecting single blackhole nodes in AODV. Their approach relies on utilizing a sequence number stored in packets and the receiving time of packets to calculate the request timeout. This information can determine the validity of routes by applying a time threshold value. Similarly, Djenouri et al. [17] introduced a two-phase methodology for monitoring and detecting single blackhole nodes in AODV. For monitoring purposes, a random two-hop ACK was employed in the monitoring phase to watch the sent and received packets among nodes, while the detection process is based on a Bayesian approach.

Raj et al. [18] suggested DPRAODV (Detection, Prevention and Reactive AODV), which is a new control packet used to detect single blackhole nodes in the AODV protocol. Similarly, Jaisankar et al. [19] introduced a new field called 'field_next_hop' and added it to the Route Reply (RREP) packet. Furthermore, they employed a blacklist to identify malicious nodes in AODV. However, Mistry et al. [20] introduced a new table, timer, and variable in the AODV protocol and modified the functions to identify blackhole nodes. Su [21] proposed an intrusion detection approach that used an anti-black countermeasure injected into some IDS nodes. Similarly, Talukdar et al. [22] proposed an Intrusion Detection System (IDS) and digital signature-based approach to enhance the accuracy of AODV in WSNs.

Kozma et al. [23] proposed a mechanism for detecting single blackholes in the DSR protocol. Their proposed approach utilizes audit nodes and bloom filters. Similarly, Selvan et al. [24] proposed an intrusion detection system to detect blackholes in WSNs. In their approach, the authors detected malicious nodes using a method similar to the watchdogs' approach and a voting system. When a node is confirmed as malicious, it will be eliminated from the network. However, their approach did not account for the possibility that some nodes may have malfunctions.

Jamaesha et al. [25] proposed a location-aware approach to predict the future location of nodes. The prediction process in their proposed protocol helps identify malicious nodes and reduce packet loss. Kumaravel et al. [26] proposed a new method that extracts features from both benign and malicious nodes using a machine learning approach. They utilized an adaptive neuro-fuzzy inference system (ANFIS) classifier to identify and avoid malicious nodes. They claimed that their approach achieved an accuracy rate of about 92.5% in identifying malicious nodes. However, their approach achieved average throughput and packet loss ratio. Gurung et al. [27] studied smart gray-hole attacks and sequence number-based gray-hole attacks, testing them against the AODV, IDS-AODV, and

Multi-Objective Bat Algorithm-Based Dynamic Path Planning for AODV (MBDP-AODV) protocols. They showed that MBDP-AODV is unable to detect smart grey-hole attacks.

Panos et al. [28] proposed an approach to detect both parts of blackhole attacks targeting AODV. The authors focused on the effects of the attack and the exploitation of the route discovery process, utilizing a dynamic threshold cumulative sum to detect abnormal packet-sending behaviors using AODV.

The approaches discussed previously dealt with detecting single blackholes only. Some approaches were proposed to detect collaborative blackhole nodes such as [29–33]. Ramaswamy et al. [29] modified the AODV protocol, using a cross-checking method and a data routing information table to detect cooperative blackholes. However, they did not provide simulations or experiments that validate their claims. Similarly, Weerasinghe et al. [30] utilized data routing tables and cross-checking methods and tested the modified AODV protocol against cooperative blackholes. The results showed that the proposed approach achieved a 50% higher throughput performance than AODV. Yu et al. [31] used a distributed cooperative mechanism in AODV protocol. They claimed that their approach achieved a detection rate of higher than 98%. Wang et al. [32] and Min et al. [33] used a hash-based scheme for detecting cooperative blackholes in DSR and AODV protocols, respectively. The authors in [32] did not provide experiments to validate their claims, while the experiments in [33] showed that the packet delivery ratio in their proposed approach is higher than the original AODV. Hammamouche et al. [34] proposed an approach to tackle the problem of simple and cooperative blackhole attacks. The authors addressed that their approach is comparable to AODV and OLSR regarding the delivery ratio and the detection rates of packets.

## 3 Preliminaries

This section introduces AODV and OLSR protocols and the problem of blackhole nodes. Moreover, it discusses some existing approaches to mitigate the problem of blackholes as well as the weaknesses of those approaches.

### *3.1 AODV Protocol Blackhole Problem and Mitigation*

AODV is an on-demand protocol, that creates routes when needed by the source node. When a source node, say X, needs a route to a destination, say Y, X initiates and broadcasts a route request (RREQ) packet to its neighbors. Next, X's neighbors forward X's request to their neighbors, and so on. The RREQ is forwarded until it reaches the destination Y or an intermediate node with a "fresh enough" route to Y, as shown in Fig. 1. If X's RREQ reaches Y, Y responds by sending a reply (RREP) packet to the neighbor from which it received the first X's RREQ. Next, the neighbor sends back the RREQ to the neighbor from which it received the X's RREQ, and so on, as shown in Fig. 2. If X's RREQ reaches an intermediate node, say C, that has a "fresh enough" route to Y, C unicasts an RREP packet back to X, telling that it has a good route to Y. In this case, X's RREQ is not forwarded by C. Then, X sends its packets to Y through C.

AODV is vulnerable to blackhole attacks. When using the AODV protocol, an intermediate node can respond to an RREQ if it has a fresh route to the destination. However, this feature may be exploited by malicious nodes that can behave as benign nodes that have a fresh route to the destination and may send RREP to the source before any other intermediate nodes. This may happen often since malicious nodes do not need to check routing tables like benign nodes. In this case, the malicious node will drop some or all packets from the source to the destination. Fig. 3 shows the blackhole problem in AODV, where B is the malicious node.

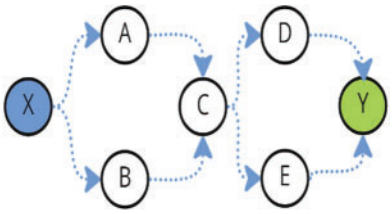


**Figure 1:** AODV RREQ propagation

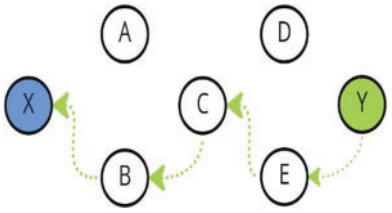


**Figure 2:** AODV RREP propagation

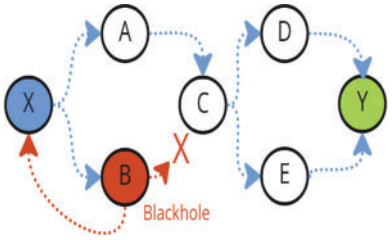


**Figure 3:** Blackhole problem in AODV

Several approaches have been proposed to mitigate the blackhole problem in AODV, as discussed in the related work section. Avoiding blackholes by revoking the permission from intermediate nodes to send RREP, which have a fresh route to destinations, may degrade the performance of AODV tremendously, especially in large WSNs. This solution forces the source to wait until the RREQ reaches the destination and until the RREP travels back from the destination, which poses a high routing delay. Meanwhile, close intermediate nodes may have a fresh route to the destination.

The approach of *Watchdogs* and *Pathrater* proposed by Marti et al. [35] and its enhanced versions [36] depends on monitoring the traffic sent by a node using the node's neighbors. For example, suppose that the neighbors of a node X are as shown in Fig. 4. When node A sends a packet to the destination E, the packet is forwarded by C to X, which in turn should send the packet to D. If X forwards the packet to D, this transmission should be heard by C since it is in the transmission area of X. This enables C to check whether X has sent the packet or not. Similarly, when E wants to send a packet to A, the packet should be forwarded by D to X. If X forwards the packet to C, the transmission is heard by D, enabling D to check whether X forwarded the packet that D sent. To conclude, neighbor nodes that exist in the transmission range of X can monitor X's behavior regarding sending or dropping packets. These neighbors are called *Watchdogs*. The watchdogs of a node, say X, can maintain the ratio of the forwarded packets to X to the received packets by X. The watchdogs in WSN maintain a table that consists of reputation values (number of forwarded packets/numbers of received packets) of their monitored nodes. These reputation values are used when a node chooses a path to forward packets to a destination. Generally speaking, nodes with high reputation values are preferred when a source node

has more than one path to a destination. The aforementioned algorithm is called *Pathrater*. Interested readers can refer to [36] for more details.

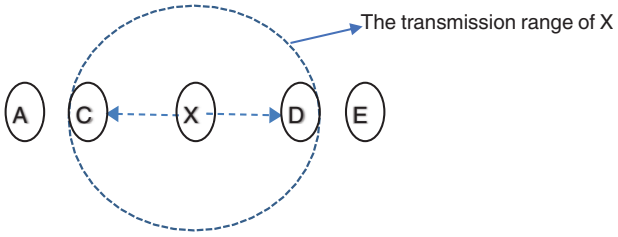


**Figure 4:** The watchdogs of X

One of the problems with *Watchdog*/*Pathrater* algorithms is the continuous movement of nodes in WSN. The watchdogs of a node may vary over time. Therefore, the history of reputation values is lost as the node moves. This history is crucial for precise reputation values of nodes in WSNs. Moreover, smart malicious nodes may behave normally at the beginning when they move to new locations, or they may drop partial information to keep their reputation values good enough to be selected to forward packets.

One of the challenges with *Watchdog*/*Pathrater* algorithms is the continuous movement of nodes in WSNs. The watchdogs of a node may change over time. Therefore, the history of reputation values is lost as the node moves. This historical data is crucial for maintaining accurate reputation values of nodes in WSNs. Additionally, smart malicious nodes may behave normally when they move to new locations or selectively drop information to maintain sufficiently high reputation values for packet forwarding selection.

### *3.2 OLSR Protocol Blackhole Problem and Mitigation*

OLSR is a table-driven and proactive protocol for WSNs. With OLSR, each node builds its routing table by exchanging routing information periodically with other nodes. Therefore, contrary to AODV, when a node needs to send a packet to a destination, it has an available route immediately in its routing table since it has the whole network topology. However, exchanging information among all nodes in a WSN produces high traffic and degrades WSN performance. Therefore, OLSR uses Multi Point Relaying nodes (MPR) to reduce network flooding. The MPRs of a node, say X, are a minimal subset of X's neighbors that can reach all X's 2-hop neighbors. Fig. 5 shows an example of MPRs in a WSN, with green nodes representing the set of MPRs in the given WSN.

Two types of routing messages are utilized to build the network topology in WSNs: HELLO messages and Topology Control (TC) messages. HELLO messages are periodically broadcast by all nodes to their local neighbors. It is important to note that a HELLO message is not forwarded to all other nodes but is instead limited to local neighbors. These HELLO messages are used to discover neighbors and to select MPRs. To achieve this purpose, a HELLO message sent by a node, such as X, consists of the following components:

1. X's identity.
2. List of X's neighbors from which control traffic has been received.
3. List of X's neighbors that have bi-directional connections with X.
4. List of X's MPRs.

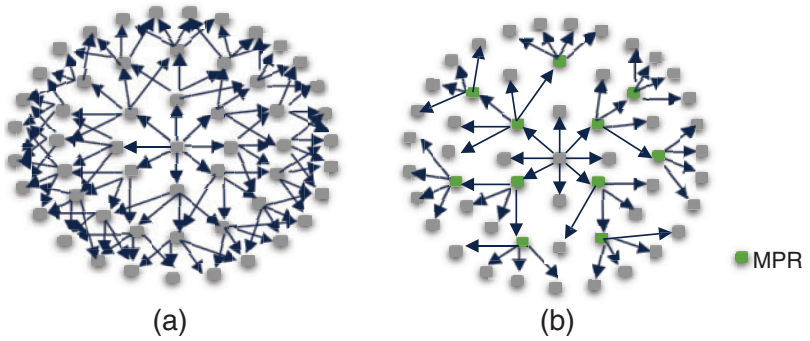


**Figure 5:** Exchanging routing information in OLSR (a) Without using MPR (b) With using MultiPoint Relay (MPR)

TC messages are generated and transmitted periodically by MPR nodes only. A TC message comprises a sender's MPR selector set, which includes the neighbors that have designated the sender as an MPR. Transmitting TC messages from MPR nodes to other nodes in a WSN helps nodes learn a partial network topology of the WSN and select a route to any node in the WSN.

The OLSR protocol begins by sending HELLO messages; each node in the network periodically broadcasts HELLO messages to its 1-hope neighbors. Next, the MPR set for each node is selected. Moreover, each MPR node maintains a set containing all nodes that have selected it as MPR, known as an MPR selector set. After that, MPR nodes broadcast TC messages, which are also forwarded solely by MPRs. The routing table in each node is constructed using these messages. Upon convergence, each node in the network can establish the routing protocol and relay it to other nodes.

As discussed in the related work section, several approaches have been proposed to mitigate blackhole in OLSR. An interesting approach was proposed by Abdalla et al. [37]. In their research, the authors suggested that each node builds a blacklist of potential malicious nodes and forwards this list to its 1-hope neighbors. Subsequently, the receiving nodes verify whether the nodes in the blacklist are indeed malicious. After that, these neighbors propagate the blacklist to their neighbors, and so on. Although this approach offers an obvious advantage, it floods the network with many packets, thereby exacerbating the already heavy packet traffic caused by the OLSR protocol.

### *3.3 Watchdogs and Pathrater Approach Limitations in AODV and OLSR*

Proactive protocols, such as OLSR, encounter scalability issues, which make them suitable for small networks only; OLSR must maintain the routing table for all possible routes. Consequently, maintaining such a table becomes more challenging as the number of mobile nodes increases. Moreover, the high volume of HELLO and TC messages, utilized for table maintenance, floods the network and degrades its performance. Furthermore, in scenarios with high node mobility, these problems become severe due to the increased messages required to achieve convergence. Defending WSNs in OLSR by rating nodes and sharing ratings with all the nodes in the network, as proposed by some researchers such as [27], makes the aforementioned approach even worse, significantly deteriorating WSN performance, especially under high mobility conditions.

Reactive protocols like AODV generate much less traffic than proactive protocols. Moreover, they require less computation and storage than proactive protocols. However, implementing the *Watchdogs/pathrater* approach in AODV, as proposed by some authors [32], presents significant challenges,

particularly regarding the localization of watchdogs' lists of malicious nodes. The watchdogs of a node, say X, store the reputation values of X based solely on their monitoring process. That is, when a node, such as Y, intends to forward a packet to a destination via an intermediate node, say K, Y consults its reputation table to determine whether K is a blackhole suspect. These table entries are based on Y's listening to its neighbors, which is measured by computing the ratio of received/forwarded packets by Y's neighbors. For example, the reputation value of K in Y's table is calculated as the ratio of packets sent to K by Y and those forwarded by K. However, if K is continuously moving, its watchdogs change accordingly. In this case, K obtains a fresh reputation value wherever it relocates, allowing it to drop more packets before detection. Furthermore, if K selectively drops information to maintain a high reputation and evade detection, it can transition between locations without being detected, as its history is not shared among all nodes.

## 4 The Proposed Protocol

This paper proposes a new version of the AODV protocol that leverages the advantages of AODV and OLSR protocols while addressing their respective drawbacks when employing the *Watchdogs and Pathrater* mechanism. The proposed protocol consists of three phases: Collecting Reputations, Updating Reputations, and Choosing the Best Route.

### *4.1 Collecting Reputations*

Individual monitoring by a node's neighbors using *Watchdogs and Pathrater* mechanisms aims to collect and compute the nodes' reputations. These gathered values are used later to determine whether the node is malicious or not. This decision (whether a node is blackhole or not) can be made by exchanging reputation values among all network nodes to build a comprehensive reputation table. However, sharing the monitoring information, including local reputations, about nodes should be applied with minimal impact on the network and performance. Fig. 6 illustrates the proposed model for exchanging reputations. The steps for collecting reputations are as follows:

1. Each node monitors both the traffic it sends to and the traffic it receives from its neighbors, computes the reputation of monitored nodes, and stores the calculated reputations. As measured by node B, the reputation value of node A is determined as follows [36]:

$$R(\mathrm{A}) = FP(A)/SP(A) \tag{1}$$

where $R(A)$ indicates A's reputation, $SP(A)$ indicates the number of packets sent to A by B, and $FP(A)$ indicates the number of forwarded packets (from those received by B) by A. For example, if A received 10 packets from B and forwarded 8 packets from them during a preset time slice, its reputation will be 80%.

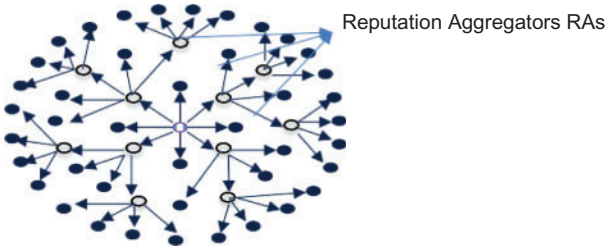


**Figure 6:** The proposed protocol involves exchanging reputation information between nodes

2. Every node selects its RA set, which is the group of Reputation Aggregators from its first hop-neighbors. The transmission ranges of the RA of node A should cover all second-hop neighbors of A. Moreover, none of A's neighbors can forward A's table of reputation values to other nodes except the nodes in A's RA set. The goal of the aforementioned process is to avoid sending redundant traffic, which may happen if all A's neighbors are allowed to send A's reputation table. After this process, every node in the 2-hop neighborhood of A receives a copy of A's reputation table. This procedure is carried out until every node in the WSN receives a copy of all other nodes' reputation tables.
3. Every node in the WSN updates its reputation table according to the new reputation tables received from Reputation Aggregators. Following convergence, every node is expected to have a comprehensive picture of all nodes' reputations in the network.
4. When the reputation value of a node changes, the reputation change (updated value) should be broadcast. This paper proposes three approaches to broadcast the updates of reputations, which are as follows:
    - *The Prompt Broadcast*: In this method, the watchdog of node X sends the updated reputation value of X immediately when a change occurs in the reputation values. This method offers high accuracy in blackhole detection because the reputation tables in nodes are always up-to-date. However, it imposes high network traffic because of the frequency of broadcasting of updates.
    - *The Regular Broadcast*: In this method, the updates are collected and transmitted at every predetermined time value, such as every 5 min. This approach reduces network traffic overhead compared to the previous approach. However, it may allow some blackhole to operate and drop packets before being detected. The severity of this disadvantage is contingent on the duration of the predetermined time value. Hence, one must consider the trade-off between decreasing network traffic and detecting blackholes.
    - *The Lite Broadcasting*: This approach collects updates and transmits them during periods of low network traffic. Implementing this method is not expected to degrade network performance, as the broadcasting frequency scale scales with the level of network traffic. Furthermore, blackhole node detection precision is enhanced when network traffic is minimal. However, during high network traffic periods, this method may have reduced effectiveness in accurately detecting blackhole nodes.

The selection of a suitable broadcasting approach could depend on the network conditions. For instance, the immediate broadcasting method may be utilized when the node transmission rate is low, as the updating frequency of reputation values is also slow.

### *4.2 Updating Reputations*

The proposed approach in this paper deals with two issues of handling reputation updates, which are:

- How to calculate the updated value of a node's reputation given the new and old values?
- When two or more watchdogs transmit the updated reputation of a node, which reputation values from them should be considered?

To answer the first question, consider Fig. 7 which shows a monitored node Z, which is monitored by the watchdogs Y and L. The task of Y and L is to compute the updated reputation value of Z. Hence, the watchdogs Y and L have a stored (old) reputation value of Z that was computed previously, and they have computed a new (current) reputation value for Z depending on the current receiving and

forwarding packets by Z. Y and L calculate the current reputation value of Z using formula (1). After that, the watchdogs Y and L use the current reputation value they computed about Z and the old reputation value of Z, which is stored in their reputation tables, to calculate the updated reputation value of Z. Formula (2) shows how to compute the updated value.

$$\text{UpdR(Z)} = Wtc * NewR(Z) + Wto * OldR(Z) \tag{2}$$

where $UpdR(Z)$ indicates Z's updated reputation value, $Wtc$ indicates the weight of the newly computed reputation value of Z, $NewR(Z)$ indicates the newly computed reputation value of Z, $Wto$ indicates the weight of the old reputation value of Z, $OldR(Z)$ is the old reputation value of Z. Hence, $Wtc + Wto = 1$. For example, suppose that the reputation value (old) of node Z in another node's reputation table, say Y, is 70%. However, in another time slice, Y computed the reputation value of Z as 50%. In this case, Y should update Z's reputation value in its table. Assume that the weights $Wtc = 0.3$ and $Wto = 0.7$, then the new reputation value is $UpdR(Z) = 0.3 * 0.5 + 0.7 * 0.7 = 0.64$.

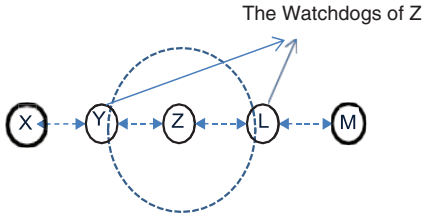


**Figure 7:** Watching the Received/Sent packets of a node using watchdogs

The values $Wtc$ and $Wto$ are fundamental in detecting blackhole nodes. Selecting the appropriate values may be crucial in enhancing the accuracy of blackhole detection. Assigning an extremely high value to $Wtc$ and a low value to $Wto$ may enable blackholes to get a high reputation when moving to new locations and start dropping packets, especially when a blackhole increases its reputation by not dropping packets at the beginning or from time to time. On the other hand, assigning an extremely high value to $Wto$ and a low value to $Wtc$ may prevent some benign nodes that had malfunctions due to environmental conditions (i.e., temporal fading that causes fluctuating bandwidth, mobility changes that cause variable network topology, etc.), from participating rapidly in sending readings. Therefore, the values $Wtc$ and $Wto$ should be selected carefully.

The second question addresses the problem of receiving several reputation values from watchdogs. When watchdogs compute the updated reputation of node A, they send these values to other network nodes, as discussed previously. An aggregator node B may receive multiple updated reputation values for A from different watchdogs. In this case, B computes the average of the received reputation values.

### *4.3 Choosing the Best Route*

The main goal of the proposed approach is to enable a node to select the best path to send or forward a packet. In many cases, there may be many paths to the destination. The proposed approach selects the most reliable route to the destination. The reliability of a path is computed based on the reputation values of the nodes in the path. This process avoids blackholes and malfunction nodes, which is the aim of the proposed approach. Algorithm 1 shows the enhanced version of AODV that uses the reputation system discussed previously.

The algorithm starts by determining the watchdog selectors for each node, as shown in steps 1–3. Next, each watchdog computes the reputation values of each node it monitors (steps 5–8). Reputation values are updated using a time window determined according to the rate of the sending value. After

these steps, watchdogs should have a complete reputation values table of all monitored nodes. Hence, after these steps, all nodes in the WSN should have a reputation value stored in one or more watchdog reputation value tables. Next, each watchdog broadcasts its reputation table to its neighbors (step 9). When an aggregator receives different reputation values about the same node, the aggregator computes the average of these reputations (steps 10–13). From all neighbors of a watchdog, only the reputation aggregators of the watchdog are allowed to forward the reputation table of the watchdog (steps 15–18). At the end of this phase, each node in the WSN should have the reputation values of each node. Therefore, the reputation table at each node should converge at the end of this phase (steps 19–21). During the convergence process, different reputation values about the same node may be received from different sources. In this case, formula (2) is used to compute the updated value. Steps 22–37 show that when node S needs to send a message to node D, it checks its table to see if it has a good path to D. A good path here means that all nodes on the path have good reputation values, which are already stored in S's reputation table. If there is a good path, S uses this path to send a message to D. If S does not have a good path to D, it searches for a new path. First, S broadcasts a PREQ (step 28). The same process used in the AODV is used in this phase. Different paths may be received by S as the result of the aforementioned process. In this case, S computes the reputation value of each path, which equals the minimum reputation value among the path nodes (step 31). This is because one malicious or malfunctioned node may break the path to the destination. The path with the highest reputation is chosen to send the message to D, and this path is stored in S's table (steps 33–35).

**Algorithm 1:** An Enhanced AODV Protocol for Blackhole Avoidance

**Data:** A WSN M = {$M_1$, $M_2$, $M_3$, $M_4$, …, $M_n$}, Source node S ∈ M, Destination node D ∈ M, the set of Reputation Aggregators RA, Watchdog Selectors sets WS, Watchdogs of a node $L$ WS($L$), Reputation Table RT

**Result:** The Best Route from S to D.

**1. For** $i = 1$ *to* $n$ **do**

**2.** $WS(M_i) \leftarrow WS(M_i) \cup M_j$, *where* $M_j \in M$ *and* $M_j$ *is a watchdog of* $M_i$ *//Fill the set of watchdog selectors for each node*

**3.End**

**4.For** $w = 1$ *to* $n$ **do** // all nodes

**5.** **Foreach** $M_k \in WS(M_w)$ *// the watchdogs that monitor* $M_w$

**6.** **do**

**7.** $RT(M_k).M_w = FP(M_w)/SP(M_w)$ *// compute the reputation values according to formula (1)*

**8.** **end**

**9.** $M_k$ .*Broadcast*$(RT(M_k))$ // $M_k$ *broadcasts its reputation table to its neighbors*

**10.** **Foreach** $r \in RA(M_w)$ // *the reputation aggregators of watchdogs that monitor node* $M_w$

**11.** **do**

**12.** reps($M_w$) >1 → RT.$M_w$ = Sum(RT.$M_w$)/ reps($M_w$) //reps($M_w$) is the number of reputations received for $M_w$

**13.** **end**

**14.End**

**15.Foreach** $r \in RA$ *// all reputation aggregators*

**16.do**

(Continued)

**Algorithm 1 (continued)**

**17.** ***r.Broadcast(r.RT)*** *// broadcast the reputation tables by Aggregators*
**18.end**
**19.For** $j = 1$ *to* $n$ *// all nodes in the network*
**20.** *Update* $M_j.RT$ according to formula (2) *// update the reputation tables of* $M_j$
**21.End**
**22.IF** $S.communicate(D)$ *// if Source S wants to communicate with a Destination D*
**23.then**
**24.** **IF** $S.route(D) \neq \emptyset \wedge S.route(D).reputation = Good$ *// if S has a good route to D*
**25.** **then**
**26.** $Return\ S.route(D)$ *// starting sending packets to D using the stored route*
**27.** **else**
**28.** $S.broadcast(PREQ(D))$ *// S broadcasts an RREQ to find a route to D*
**29.** **Foreach** $P \in S.route(D)$ *// for all received routes to D*
**30.** **do**
**31.** $P.reputation = min_{a \in ;P} reputation(a)$ *// the reputation of P equals the minimum reputation of its nodes*
**32.** **end**
**33.** $BP = max_{t \in ;P.route(D)} reputation(t)$ *// choose the highest reputation routes to D*
**34.** *Update* $S.route(D)$ *// Update the routing table*
**35.** $Return\ BP$ *// starting sending packets to D using the selected route*
**36. End**
**37.End**

## 5 Case Study

Fig. 8 shows a case scenario of a network that has two states, which are S1 and S2. In S1, a mobile network device S would like to send a packet to another mobile network device D. However, a blackhole B exists in this zone and tries to drop the packet. Fig. 9 shows the possible routes of the packet using OLSR routing protocol. As discussed in Section 3, OLSR protocol is a table-driven and proactive protocol. Therefore, each node has its routing table built using the information exchanged with other nodes. If the nodes use these routing tables without rating the nodes in the paths, the packet in the given scenario may be received and dropped by the blackhole as shown in Path A. Meanwhile, using the rating approach, the nodes may have information about the blackhole in the network and may choose a different path to avoid the blackhole as shown in Path B. Therefore, using the *Pathrater*/*Watchdog* method with the OLSR protocol can mitigate the problem of the blackhole. However, OLSR poses a huge overhead on the network since it is a table-driven and proactive protocol. Therefore, adding this feature (*Pathrater*/*Watchdog* method) adds more overhead and may make using OLSR infeasible.

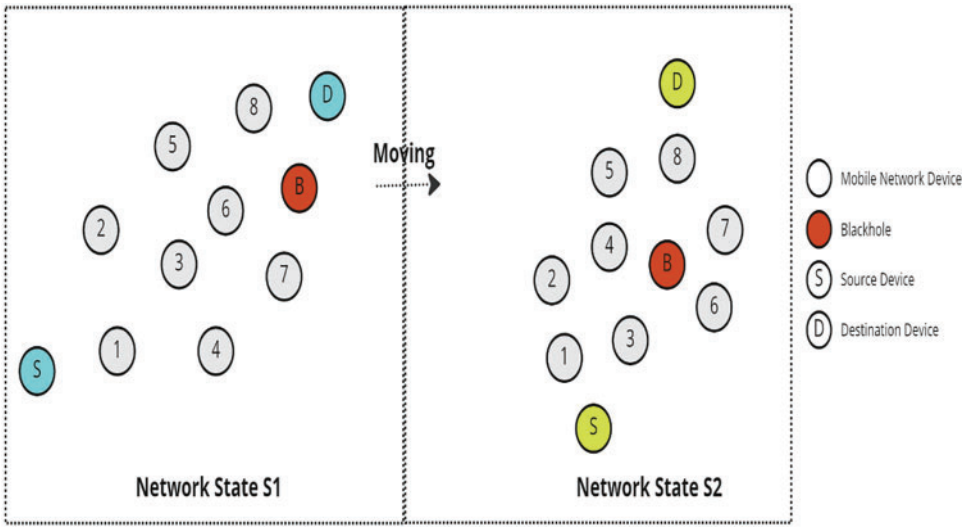


**Figure 8:** Moving blackhole scenario

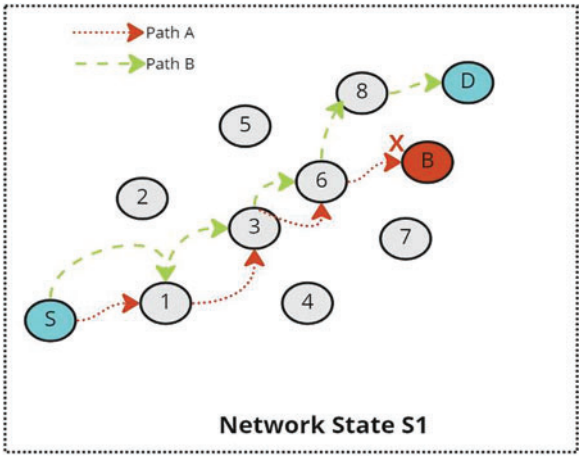


**Figure 9:** Possible routing paths using OLSR Protocol

Fig. 10a shows the process of sending a packet using the original AODV protocol but without using the *Pathrater*/*Watchdog* approach. As discussed before, AODV is an on-demand protocol; it creates routes when needed by sending an RREQ query to retrieve a path to the destination. However, the scenario in Fig. 10a shows that there is a blackhole B in the discovered route by the source S. B received the RREQ and sent a reply telling S that it had a fresh route to the destination D. When S sent the packet through the discovered route, B dropped the packet and did not send it to D. However, when using AODV protocol with the *Pathrater*/*Watchdog* approach as shown in Fig. 10b, node 6, which is a watchdog of B, used its reputation table to decide whether B is a blackhole or not. That is, using its reputation table, node 6 will not forward back B's reply about having a fresh route to destination D since it knows that B is a blackhole based on its reputation value, which is 0.25. Therefore, S selected the path received from node 8, which is safe. In this case, S avoided B and sent the packet safely to D. However, when B and/or other nodes move, as shown in S2 in Fig. 10c, B gets a fresh reputation value, which depends on the adopted configuration. That is, B does not get the old reputation, which is 0.25,

it had in S1. Therefore, B was enrolled in the routing path selected by S and dropped S's packets since the new neighbors of B, including node 4, do not have information about B's low reputation value it had in S1.

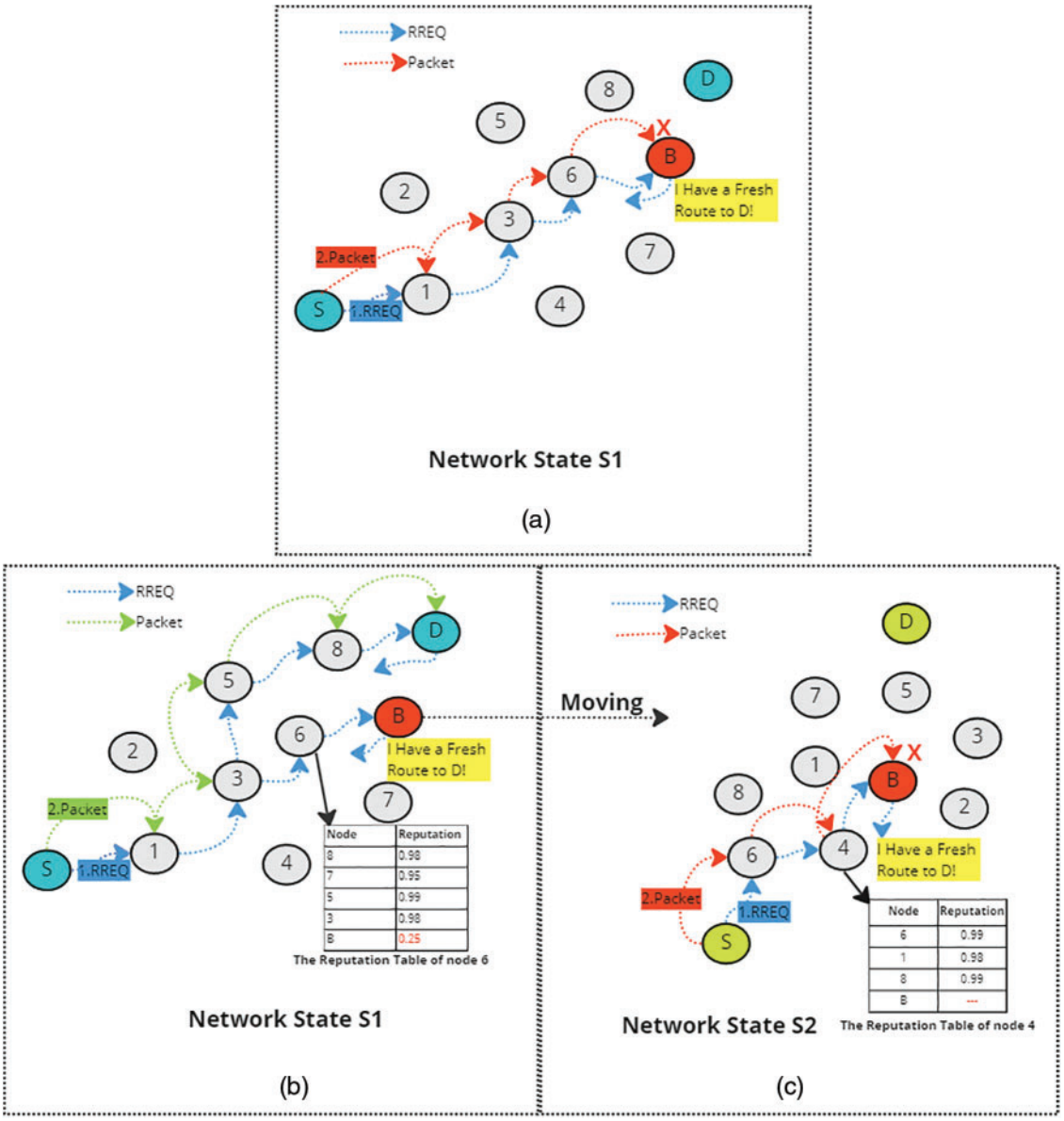


**Figure 10:** Possible routing paths using the original AODV protocol (a) without using *Pathrater/Watchdog* approach in Network State S1 (b) with using *Pathrater/Watchdog* approach in Network State S1 (c) using *Pathrater/Watchdog* approach in Network State S2

Fig. 11 shows the process of using the proposed Enhanced AODV protocol. In Fig. 11a, when S sent an RREQ to find a path to D in S1, it discovered two paths. Based on the reputation table and the *Pathrater/Watchdog* approach, S avoided the path that contains B, which is similar to the original AODV that uses the *Pathrater/Watchdog* approach. Furthermore, when B moved to S2, it did not get

a fresh reputation value as in the previous state, S1. Instead, B's reputation, which is 0.25, exists in the reputation tables in all nodes in the network because the proposed Enhanced EODV distributes and updates the reputation tables among all nodes as discussed in the methodology. Therefore, when S sends an RREQ to find a path to D, it will avoid the path that has B, and its packet will arrive safely at D.

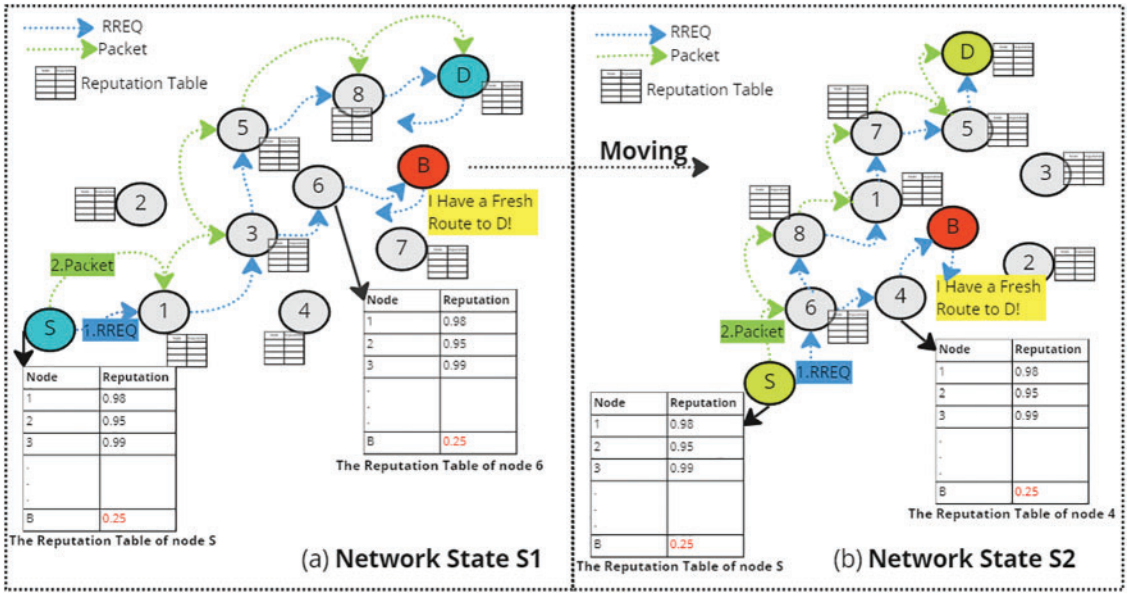


**Figure 11:** Possible routing paths using the proposed enhanced AODV protocol (a) using the *Pathrater*/*Watchdog* approach in Network State S1 (b) using the *Pathrater*/*Watchdog* approach after B moves to Network State S2

## 6 Overhead Analysis

The effectiveness of the proposed Enhanced AODV protocol in avoiding blackholes has been discussed and proved in the previous sections. However, using the *Pathrater*/*Watchdog* approach and the proposed propagation approach of reputation tables adds some overhead to the network. To discuss the overhead level added by the proposed protocol, let $\nu$ be the number of nodes in a network, $\alpha$ the average number of aggregators for each node, $\eta$ the average number of hops needed for each packet to be broadcasted to every node in the network, $\sigma$ is the average size of the reputation table in packets, $\tau$ is the time needed to process a packet in an aggregator, $\phi$ is the average frequency of sending updates by nodes, $\beta$ is the average size of an update in packets. The average number of packets each node adds to the network, $\lambda$, is computed as follows:

$$\lambda = \sigma + \phi \times \beta \tag{3}$$

The formula shows that the network overhead added by the Enhanced AODV depends on the size of the reputation table. However, a node builds its reputation table about its monitored nodes in its transmission range, which should not be large. Therefore, the overhead added by sending a reputation table of a node should not decrease the performance of the network. Furthermore, the size of the reputation table of a node is not affected by the size of the network. Therefore, the scalability of the proposed protocol is good enough, given this constraint only. However, the formula shows

that the added overhead depends on the frequency of updates and their sizes too. The reputation of a node changes when the node is a blackhole or when a malfunction happens in the node. Therefore, this overhead depends on the percentage of these nodes in the network. In normal conditions, the frequency of the updates or their sizes in packets is small and should not add large overhead to the network. That is, the proposed protocol, given this constraint, may add little overhead when the network gets a blackhole or a malfunctioning node. However, the added overhead in this case is leveraged in avoiding these nodes and delivering the packets safely to destinations. The processing overhead added by the Enhanced AODV protocol is computed as follows:

$$\delta = \lambda \times \alpha \times \nu \times \tau \tag{4}$$

This formula shows that the processing overhead on aggregators depends on different factors, which are the packets about reputations sent by each node ($\lambda$), the average number of aggregators of each node ($\alpha$), the number of nodes in the network ($\nu$), and the time needed to process each packet by each aggregator ($\tau$). Although increasing the network size increases the processing overhead on aggregators, it does not overwhelm specific aggregators since the number and distribution of aggregators increase when the network size increases. Therefore, the added processing overhead by the proposed protocol on aggregators is acceptable. The aforementioned discussions show that the network and the processing overhead added by the Enhanced AODV are acceptable, and the proposed protocol does not affect the scalability of networks.

## 7 Comparison with the Related Work

The proposed approach adds value by extending the Watchdogs and Pathrater approaches to work in dynamic environments and avoid blackholes and malfunctioning nodes. In addition, it builds and distributes a reputation table for all nodes in WSNS, resulting from accumulated voting by many nodes about all nodes in WSNs. This increases the trust in the proposed approach and greatly increases the packet delivery ratio. Table 1 compares between some related work discussed in Section 2 and the proposed approach.

**Table 1:** Comparing the proposed approach with the related work

| Authors | Protocol | Detection method | Effectiveness |
|---|---|---|---|
| Sun et al. [12] | AODV | Node feedback and routing recovery | Detects single blackholes, not suitable for collaborative blackhole attacks |
| Al-Shurman et al. [13] | AODV | – Exploits multiple paths to a destination<br>– Unique sequence number in packets | – Difficulty in identifying safe routes<br>– No reputation values shared among nodes |
| Yang et al. [14] | Extended AODV | TADR-EAODV algorithm | – Considers various trust criteria<br>– Centralized ensemble clustering |

(Continued)

**Table 1 (continued)**

| Authors | Protocol | Detection method | Effectiveness |
|---|---|---|---|
| Quincozes et al. [15] | N/A | Machine learning ML model | – Supervised ML outperforms unsupervised ML<br>– REPTree with OneR feature selection achieves the highest F1-Score |
| Tamilselvan et al. [16] | AODV | Time-based detection using sequence numbers | – Determines validity of routes using time threshold<br>– Utilizes packet sequence numbers |
| Djenouri et al. [17] | AODV | Two-phase methodology-Monitoring with two-hop ACK-Detection using Bayesian approach | Effective monitoring and detection of single blackhole nodes |
| Raj et al. [18] | AODV | DPRAODV (Detection, Prevention, and Reactive AODV) | Used DPRAODV, a new control packet to detect single blackhole nodes in the AODV protocol |
| Jaisankar et al. [19] | AODV | Modification of RREP packet and blacklist | Identification of malicious nodes using additional fields and blacklist |
| Mistry et al. [20] | AODV | New table, timer, and variable | Modified functions for blackhole node detection |
| Talukdar et al. [22] | AODV | IDS and digital signature-based approach | Enhances accuracy of AODV using digital signatures |
| Kozma et al. [23] | DSR | Audit nodes and bloom filters | Detects single blackholes in DSR protocol |
| Gurung et al. [27] | AODV | Smart gray-hole attack detection | MBDP-AODV fails to detect smart gray-hole attacks |
| Panos et al. [28] | AODV | Dynamic threshold cumulative sum | Detects both parts of blackhole attacks targeting AODV |
| Ramaswamy et al. [29] | AODV | Cross-checking method and data routing information table | Detects cooperative blackholes |
| Weerasinghe et al. [30] | AODV | Data routing tables and cross-checking | Achieves higher throughput compared to AODV |
| Yu et al. [31] | AODV | Distributed cooperative mechanism | Claims a detection rate higher than 98% |
| Wang et al. [32] | DSR | Hash-based scheme | No analysis provided |

(Continued)

**Table 1 (continued)**

| Authors | Protocol | Detection method | Effectiveness |
|---|---|---|---|
| Min et al. [33] | AODV | Hash-based scheme | Higher packet delivery ratio than the original AODV |
| The proposed approach | AODV | – Build comprehensive reputation tables for the network<br>– Use the Watchdogs/Pathrater approach | – Builds and broadcasts comprehensive reputation tables<br>– Detects blackholes and malfunctioning nodes in dynamic networks<br>– Uses a new light overhead approach to distribute reputation tables among nodes |

## 8 Conclusions and Future Work

The paper has proposed an Enhanced AODV protocol to avoid blackholes and malfunctioning nodes in WSNs, especially in dynamic networks where nodes move continuously. The proposed method builds a reputation table about all nodes in the network in each node. The reputation table guides nodes when selecting routes to send or forward packets. To build and update reputation tables, the proposed approach uses a light method to distribute and broadcast updated reputation values. The paper has discussed a case study that shows the correctness of the Enhanced AODV protocol in avoiding moving blackholes. Furthermore, the paper has analyzed the overhead added by the Enhanced AODV. The analysis has shown that the proposed version adds some extra overhead to the network because of the messages needed to distribute and update reputation values. However, the analysis has shown that the added traffic and processing overhead does not affect its applicability and does not affect the scalability of the proposed enhanced AODV protocol.

The Enhanced AODV protocol uses aggregator nodes responsible for broadcasting reputation tables. An aggregator could be a blackhole, posing more harm than ordinary blackhole nodes. Therefore, the selection of aggregators should be based on a secure voting system that can prevent blackholes from being selected as aggregators. The future work will focus on developing a secure voting system to enhance the security of aggregators against blackholes problem.

**Acknowledgement:** We would like to thank Ajman University for the support provided in covering the APC. In addition, we would like to thank the reviewers for the valuable comments that enhanced the paper's quality.

**Funding Statement:** Not applicable.

**Author Contributions:** The authors confirm contribution to the paper as follows: methodology conception and design: Qussai M. Yaseen, Monther Aldwairi, draft manuscript preparation: Qussai M. Yaseen, Monther Aldwairi, Ahmad Manasra. All authors reviewed and approved the final version of the manuscript.

**Availability of Data and Materials:** Not applicable.

**Ethics Approval:** No human or animal was included in the work.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References


[1] M. Stehlik, V. Matyas, and A. Stetsko, "Towards better selective forwarding and delay attacks detection in wireless sensor networks," in *2016 IEEE 13th Int. Conf. Netw., Sens., and Control (ICNSC)*, Mexico, 2016, pp. 1–6.

[2] V. Sharma, R. Kumar, and N. Kumar, "DPTR: Distributed priority tree-based routing protocol for FANETs," *J. Comput. Commun.*, vol. 122, no. 3, pp. 129–151, 2018. doi: 10.1016/j.comcom.2018.03.002.

[3] W. Aldosari, "Received power based unmanned aerial vehicles (UAVs) jamming detection and nodes classification using machine learning," *Comput. Mater. Contin.*, vol. 75, no. 1, pp. 1253–1269, 2023. doi: 10.32604/cmc.2023.036111.

[4] A. Ahmad, S. Din, A. Paul, G. Jeon, M. Aloqaily and M. Ahmad, "Real-time route planning and data dissemination for urban scenarios using the Internet of Things," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 50–55, 2019. doi: 10.1109/MWC.001.1900151.

[5] A. Albeshri, "An image hashing-based authentication and secure group communication scheme for IoT-Enabled MANETs," *Future Int*, vol. 13, no. 7, pp. 1–14, 2021. doi: 10.3390/fi13070166.

[6] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," *RFC*, vol. 3626, pp. 1–75, Oct. 2003.

[7] L. Albini, A. Caruso, S. Chessa, and P. Maestrini, "Reliable routing in wireless ad hoc networks: The virtual routing protocol," *J. Netw. Syst. Manage.*, vol. 14, no. 3, pp. 335–358, 2006. doi: 10.1007/s10922-006-9035-8.

[8] A. Chopra and R. G. Vishwakarma, "Comparison of ad hoc reactive routing protocols: AODV and DSR with respect to performance parameters for different number of nodes," in *2014 Conf. IT in Business, Ind Gov. (CSIBIG)*, Indore, India, 2014, pp. 1–4.

[9] A. Dang, T. Nguyen, T. Cong-Doan, N. Van-Hau, and V. Quy, "Performance analysis of routing protocols for mobile ad hoc networks in urban scenarios," *J. Commun*, vol. 16, pp. 545–552, 2021.

[10] M. Abdelhaq *et al.*, "The resistance of routing protocols against DDOS attack in MANET," *Int. J. Elect. Comput. Eng.*, vol. 10, pp. 4844–4852, 2020.

[11] Q. Yaseen and M. Aldwairi, "An enhanced AODV protocol for avoiding black-holes in MANET," presented at the 5th Int. Symp. Emerg. Inter-Networks, Commun. Mobil., Gran Canarias, Spain, Jun. 21–23, 2018.

[12] B. Sun, Y. Guan, J. Chen, and W. Pooch, "Detecting black-hole attack in mobile ad hoc networks," presented at the 5th Eur. Personal Mob. Commun. Conf., Glasgow, UK, Apr. 22–25, 2003.

[13] M. Al-Shurman, S. M. Yoo, and S. Park, "Blackhole attack in mobile ad hoc networks," presented at the 42nd Annual ACM Southeast Reg. Conf. (ACM-SE'42), Huntsville, Alabama, Apr. 2–3, 2004.

[14] Z. Yang, L. Li, F. Gu, X. Ling, and M. Hajiee, "TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks," *J. Int. Things*, vol. 20, no. 4, pp. 100627, 2022. doi: 10.1016/j.iot.2022.100627.

[15] S. E. Quincozes, J. F. Kazienko, and V. E. Quincozes, "An extended evaluation on machine learning techniques for denial-of-service detection in wireless sensor networks," *J. Int. Things*, vol. 22, no. 4, pp. 1–16, 2023. doi: 10.1016/j.iot.2023.100684.

[16] L. Tamilselvanand and V. Sankaranarayanan, "Prevention of blackhole attack in MANET," presented at the 2nd Int. Conf. Wire. Broadband and Ultra Wideband Commun., Sydney, Australia, Aug. 27–30, 2007.

[17] D. Djenouri, and N. Badache, "Struggling against selfishness and blackhole attacks in MANETs," *J. Wire. Commun. Mobile Comput.*, vol. 8, no. 6, pp. 689–704, 2008. doi: 10.1002/wcm.493.
[18] P. Raj and P. Swadas, "DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET," *Int. J. Comput. Sci.*, vol. 2, pp. 54–59, 2009.
[19] N. Jaisankar, R. Saravanan, and K. D. Swamy, "A novel security approach for detecting blackhole attack in MANET," presented at the Int. Conf. Recent Trends in Business Admin. Inform. Process., Thiruvananthapuram, India, Mar. 26–27, 2010.
[20] N. Mistry, D. C. Jinwala, and M. Zaveri, "Improving AODV protocol against blackhole attacks," presented at the Int. MultiConf. Eng. Comput. Sci., Hong Kong, China, Mar. 17–19, 2010.
[21] M. Su, "Prevention of selective blackhole attacks on mobile ad hoc networks through intrusion detection systems," *J. IEEE Comput. Commun.*, vol. 34, no. 1, pp. 107–117, 2011. doi: 10.1016/j.comcom.2010.08.007.
[22] I. Talukdar, R. Hassan, S. Hossen, K. Ahmad, F. Qamar and A. Ahmed, "Performance improvements of AODV by black hole attack detection using IDS and digital signature," *J. Wireless Commun. Mobile Comput.*, vol. 2021, no. 3, pp. 1–13, 2021. doi: 10.1155/2021/6693316.
[23] W. Kozma and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," presented at the Second ACM Conf. Wireless Netw. Secur., Zurich, Switzerland, Mar. 16–19, 2009.
[24] M. Selvan and S. Selvakumar, "Malicious node identification using quantitative intrusion detection techniques in MANET," *Cluster Comput.*, vol. 22, no. S3, pp. 7069–7077, 2019. doi: 10.1007/s10586-018-2418-2.
[25] S. Jamaesha and S. Bhavani, "A secure and efficient cluster-based location-aware routing protocol in MANET," *Cluster Comput.*, vol. 22, no. S2, pp. 4179–4186, 2019. doi: 10.1007/s10586-018-1703-4.
[26] A. Kumaravel and M. Chandrasekaran, "Performance analysis of malicious node detection in MANET using ANFIS classification approach," *Cluster Comput.*, vol. 22, no. S6, pp. 13445–13452, 2019. doi: 10.1007/s10586-018-1955-z.
[27] S. Gurung and S. Chauha, "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET," *J. Wireless Netw.*, vol. 25, no. 3, pp. 975–988, 2019. doi: 10.1007/s11276-017-1639-2.
[28] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *J. Comput. Netw.*, vol. 113, no. 1, pp. 94–110, 2017. doi: 10.1016/j.comnet.2016.12.006.
[29] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attack in wireless ad hoc networks," presented at the Int. Conf. Wireless Netw., Las Vegas, NV, USA, Jun. 23–26, 2003.
[30] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," presented at the Fut. Gen. Commun. Netw., Jeju-Island, Republic of Korea, Dec. 6–8, 2007.
[31] C. Yu, T. Wu, R. Cheng, and S. Chang, "A distributed and cooperative blackhole node detection and elimination mechanism for ad hoc network," presented at the Pacific-Asia Conf. Know. Disc. Data Min. (PAKDD), Nanjing, China, May 22–25, 2007.
[32] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," presented at the 2nd Int. Work. Depend. Netw. Comput. Mobile Syst. (DNCMS 2009), New York, NY, USA, Sep. 27–30, 2009.
[33] Z. Min and Z. Jiliu, "Cooperative blackhole attack prevention for mobile ad hoc networks," presented at the Int. Symp. Inf. Eng. Elect. Commerce, Ternopil, Ukraine, May 16–17, 2009.
[34] A. Hammamouche, M. Omar, N. Djebari, and A. Tari, "Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET," *J. Inf. Secur. Appl.*, vol. 43, no. 3, pp. 12–20, 2018. doi: 10.1016/j.jisa.2018.10.004.
[35] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," presented at the 6th Annual Int. Conf. Mobile Comput. Netw., Boston, MA, USA, Aug. 6–11, 2000.

[36] T. Varshney, T. Sharma, and P. Sharma, "Implementation of watchdog protocol with AODV in mobile ad hoc network," in *2014 Fourth Int. Conf. Commun. Syst. Netw. Technol.*, Bhopal, India, 2014, pp. 217–221.
[37] A. M. Abdalla, I. A. Saroit, A. Kotb, and A. H. Afsari, "Misbehavior nodes detection and isolation for MANETs OLSR protocol," *Procedia Comput. Sci.*, vol. 3, pp. 115–121, 2011. doi: 10.1016/j.procs.2010.12.020.