# Eliminating Selective Dropping Attack in Mobile Ad Hoc Network

**Mahdi Bounouni** ( bounouni@gmail.com )
University of Setif2
**Louiza Bouallouche-Medjkoune**
LaMos research Unit, Faculty of exact sciences, University of bejaia
**Abderrahmane Beraza**
LaMos research Unit, Faculty of exact sciences, University of bejaia
**Adel Daoud**
University of Bejaia

**Research Article**

**Keywords:** Mobile Ad Hoc networks, Malicious node, Selective Packet dropping attack, Reputation, Performance evaluation

**Posted Date:** March 23rd, 2021

**DOI:** https://doi.org/10.21203/rs.3.rs-190407/v1



**Version of Record:** A version of this preprint was published at Wireless Personal Communications on November 10th, 2021. See the published version at https://doi.org/10.1007/s11277-021-09289-z.

**Noname manuscript No.**
(will be inserted by the editor)

# Eliminating Selective Dropping Attack in Mobile Ad Hoc Network

**Mahdi Bounouni [1] · Louiza Bouallouche-Medjkoune [2] · Abderrahmane Beraza [2] · Adel Daoud [2]**

Received: date / Accepted: date

**Abstract** In this paper, we propose a new reputation approach, called I-WG (improved Watchdog). The aims is to eliminate selective dropping attack that occurs when malicious nodes drop packets at low rate to damage the network, while at the same time to avoid to be detected. The proposed approach is structured around four modules. The monitoring module overhears the forwarding activities of neighbors nodes using the promiscuous mode. The reputation module evaluates the nodes reputation values. We have have proposed a new reputation method that enable nodes to evaluate their neighbors in multiple monitoring sessions. Thus, the computed reputation value is used to determine the increment and decrement reputation rate. The exclusion module is responsible for excluding nodes with reputation values below the reputation threshold. The route selection module make restriction about discovered forwarding routes. Only forwarding routes satisfying the route incorporation threshold are accepted. The simulation results demonstrate that I-WG improves the success rate and reduces the number of packets dropped by malicious nodes, while increases the end-to-end delay.

**Keywords** Mobile Ad Hoc networks · Malicious node · Selective Packet dropping attack · Reputation · Performance evaluation

Mahdi Bounouni [2] · Louiza Bouallouche-Medjkoune [1] · Abderrahmane Beraza [1] · Adel Daoud [1]
[1] Faculty of Law and Political Sciences, University of Setif 2, Algeria

[2] LaMOS Research Unit, Faculty of Exact Sciences, University of Bejaia, Bejaia 06000, Algeria
E-mail: Bounouni@gmail.com
E-mail: louiza_medjkoune@yahoo.fr
E-mail: bihmen-2008@hotmail.fr
E-mail: adel.da06@gmail.com

## 1 Introduction

An ad hoc Mobile Network (MANET) is a cooperative network that consists on a set of mobile nodes, able to communicate without relying on an existing infrastructure or centralized administration. In a MANET, each node acts as a host and router. Mobile node can directly communicate if they are situated within the transmission range. Otherwise, the communication is done based on the cooperation of intermediate nodes (Multi-hop communication). Then, to deliver correctly data packets, the cooperation of intermediate nodes is essential and critical [1–3], which is not easy to guarantee due to the specific's characteristics of MANET, such as the open wireless medium and dynamic topology. In a real world, nodes could adopt a malicious behavior, being unwilling to drop data packet destined to be forwarded in order to disrupt the well-functioning of network operations. Thus, they could behave selfishly to save their energy-resources since nodes are resources-constrained.

Reputation-based approaches [4–20] have been proposed to deal with the malicious and selfish behaviors of nodes. They aim to punish nodes refusing to cooperate. One of the most reputable approach in which almost all existing reputation approaches relies, is the watchdog approach [4]. In this approach, each node monitors the behavior of its neighbors in the data forwarding process by overhearing their transmissions. The watchdog approach employs the promiscuous mode. This later permits to the nodes to overhear the communications of neighbors even when they are not implied in these communications. Thus, the behavior of nodes in the data forwarding process is quantified with reputation values. This later reflects the trustworthiness of nodes. Nodes having reputation values smaller than the reputation threshold are considered as uncooperative.

Although the reputation approaches [4–20] relying on the watchdog approach permit to punish malicious nodes that drop data packets, they are not able to thwart selective dropping attack [21]. Almost of these approaches are vulnerable to two mains security threats:

1. Most of these approaches can be circumvented by malicious nodes acting intelligently. These nodes can cooperate in the route discovery process but once they are part of a forwarding route, they drop only a fraction of data packets destined to be forwarded. The aim is to maintain their reputation values greater than the reputation threshold (selective dropping attack), while at the same time evicting to be considered as malicious. Following this behavior, intelligent malicious nodes will never be detected and they are always implied in the route discovery process. We argue that this threat may affect the performance of the whole network. To support this argument, we consider the case of network applications such, video streaming or file sharing, that require a certain quality of service (QoS). Then, if a node drops data packets without been detected, the forwarding activity may be affected because the packets will never reach their destination. Therefore, the destination may require to retransmit the packets which rises the

end-to-end delays transmission, and therefore, causing a substantial loss in term of QoS.
2. Depending on the manner of updating reputation values of nodes, the nodes with high reputation values and the nodes with low reputation values are treated with the same way when they are involved in a forwarding activity (+1 packet forwarded, -1 packet dropped). This is an injustice toward cooperative nodes that behave well.

This paper aims to handle the aforementioned threats of watchdog reputation-based approaches for more packet forwarding reliability. This paper introduces I-WG (improved Watchdog) as a new reputation-based approach for detecting selective packet dropping attack. The proposed approach is structured around four modules: monitoring, reputation, exclusion and route selection. The monitoring module is responsible for monitoring the activities of neighboring nodes in the process of forwarding data packets. Similarly, to watchdog approach, this module uses use the promiscuous mode as a surveillance technique. The reputation update module calculates and updates the reputation values of the nodes according to the type of event detected by the monitoring module. In our approach, we proposed a new method to update reputation values of nodes. The behavior of a node is evaluated in a multiple monitoring session. Then, these reputation values are combined to obtain the past reputation of a node which is used to determine the increment and decrement rates of the node's current reputation. The exclusion module is responsible for excluding nodes having the reputation values below the reputation threshold from all network activities. The route selection module is responsible for choosing the best route in terms of reputation. Only nodes with high reputation values are involved. We evaluated the performance of our approach using the NS-2.34 network simulator. The simulation results obtained demonstrate that our approach improves the success rate and reduces the number of packets dropped by malicious nodes.

The rest of this paper is organized as follows. In Sect. 2, we describe background and related Works. The problem statement is depicted in section 3. In Sect. 4, we present the proposed approach I-WG. The performance evaluation of I-WG approach is given in Sect. 4. Section 5 concludes the paper.

## 2 Background and Related Works

The watchdog is one of the most reputable approach dealing against the malicious behaviors of nodes. It is proposed to detect malicious nodes that drop data packet destined to be forwarded by monitoring the forwarding activities of neighbor's nodes. The watchdog approach relies on the use of the promiscuous mode. Using this mode, if a node A is in the transmission range of node B, the node A can overhear the communications of the node B even in the case where these communications do not involve this node directly.

The authors incorporate both Watchdog and Pathrater modules [4] in the DSR protocol [22]. The watchdog monitors and checks whether the next node

on the forwarding route forwards correctly the data packet recently sent. Each node maintains a buffer of data packets recently sent. If the overheard packet exists in the buffer, the node considers that the packet has been forwarded and the packet is removed from the buffer. However, if the data packet has remained in the buffer without been overheard for a longer time than a predefined threshold, the packet is removed from the buffer. Thus, the node increments the failure counter associated to the node responsible to forward the packet. If the failure counter exceeds a certain threshold, the node is considered as malicious. The Pathrater uses the information collected by the Watchdog module to select the most reliable routes by avoiding malicious nodes.

Many security approaches [4–20] employ the watchdog approach to unmask malicious nodes. However, although the use of the watchdog approach allows to detect malicious nodes, it has several limitations [4] and All security approaches using this technique inherit these limitations. The approaches using this technique fail to detect malicious nodes in the following cases:

- **Ambiguous Collision:** This problem prevents the node from overhearing the forwarding activities of the next hop node on a forwarding route;
- **Receiver collision:** in this case, the node can overhear the communication of the of the next hop node, but it is not able to confirm the good reception of the packet;
- **Limited transmission power:** a node can adjust its transmission power so that the signal is loud enough to be overheard by the previous node, but it is too weak to be received by the next node.
- **False accusation attack:** a malicious node may falsely accuse other cooperative nodes to be malicious in order to evict to forward packets.
- **Collusion attack (Misbehavior):** When two malicious nodes succeed in a forwarding route, they can collaborate in order to hide their dropping activities (misbehavior's);
- **Partial dropping attack:** A node can circumvent the watchdog by dropping packets at a low rate in order to be detected.

## 3 Problem statement

Almost of existing reputation approaches [4–20] based on the watchdog approach cannot detect malicious nodes when they launch selective dropping attack, which is one of the important limitations of watchdog approach. These nodes drop data packet at low rate in order to:

- Maintain its reputation value above the tolerated threshold
- Evict be considered as malicious nodes
- Use network resources freely without restriction which results an injustice toward cooperative nodes that fully cooperate

Therefore, these nodes will be never detected which disrupt the well-functioning of the network activities, because they continue to drop packets without been punished.

**Table 1** Notations

| Parameter | Value |
|---|---|
| $D$ | Data packet |
| $P$ | Forwaring route |
| $T1$ | Timeout of monitoring data packet |
| $R_A^B(T_i)$ | Current reputation value of Node $B$ |
| $T_i$ | Monitoring Session $i$ |
| $REP_0$ | Initial reputation value |
| $REP_{max}$ | Maximum node reputation value that can have |
| $PREP_A^B(T_{i-1})$ | The past reputation value of node $B$ |
| $GREP_A^B$ | Overall reputation value of node $B$ |
| $\alpha$ | Increment reputation rate |
| $\beta$ | decrement reputation rate |
| $REP_{th}$ | Reputation threshold |
| $BlackL_A$ | List of detected malicious nodes |
| $RIT$ | Route requirement threshold |

In addition to this limitation, almost all existed reputation approaches employing the watchdog approach treat equally all nodes in the network in the process of updating the nodes reputation, without taking into account the past behavior (forwarding activities) of nodes. They use the same increment and decrement rates of reputation. Then, there is no difference between low reputed nodes and high reputed nodes when they are involved in forwarding activities. Therefore, this process of updating nodes reputation is unfair toward cooperative nodes that forward correctly all data packet passing through them.

Manet is a dynamic network. The network topology changes frequently which means that the neighborhood of each node change accordingly. Then, the established forwarding routes between the source and destination nodes may be broken. In this case, the source node should launch the route discovery process to search others active forwarding routes. Almost of these approaches treat all nodes in the route discovery process equally. They do not exploit the nodes reputation values to make a best decision. They do not make any restriction about the nodes incorporated in the forwarding routes. Then, nodes with reputation value just above the predefined threshold may be included in forwarding routes, which minimize the probability to deliver data packets successfully.

## 4 I-WG approach

In this section, we present a new approach, called Improved-Watchdog (I-WG), that aims to thwart the selective dropping attack which is one of the most important limitations of the watchdog approach. The I-WG approach is organized around four modules: monitoring, reputation, exclusion and route selection. All notation employed in this paper are presented in Table 1.

### 4.1 Monitoring Module

The monitoring module is responsible for monitoring the forwarding activities of data packets by the neighbor's nodes. In our approach, the monitoring module employs the watchdog principle [4] as a monitoring technique. Then, each node in a forwarding route monitors the forwarding of each data packets forwarded by overhearing the communications of the neighbor's nodes using the promiscuous mode.

To illustrate the functioning of monitoring module, let us consider $P$ a forwarding route between a source node $S$ and a destination node $D$ and $(A, B, C)$ intermediate nodes. When the node $A$ forwards a data packet $D$ to the node $B$, it adds a copy of the packet $D$ in its buffer. Thus, it launches its monitoring module to overhear the transmissions of the node $B$ to verify whether it forwards the packet $D$. The monitoring module intercepts all data packets forwarded by the node $B$, and it compares them to the packets maintained in the buffer.

If the packet overheard by the monitoring module of node A corresponds to the packet maintained, this latter is removed from the buffer. Thus, the node $A$ concludes that the node $B$ has forwarded the packet recently sent. In this case, the node $A$ registers a positive event against the node $B$. Otherwise, if $T1$ expires and the packet is maintained in the buffer without been overheard, the node $A$ removes the packet from the buffer and it concludes that the data packet has been dropped by the node $B$. In this case, the node $A$ registers a negative event against the node $B$.

### 4.2 Reputation Module

The reputation module is responsible for managing the reputation values of the nodes in the data forwarding process based on the events recorded by the monitoring module.

The reputation value is incremented if the monitoring module detects a positive event. On the other hand, it is decremented if a negative event is detected. Most existing reputation approaches use the same increment and decrement rates to update the reputation values of nodes. Following this approach, nodes with a high reputation and nodes with low reputation values are treated equally when they are involved in an event, which leads to injustice towards high-reputed nodes that fully cooperate. However, in our approach, the rate of increment and decrement of a node's reputation changes according to their past reputation values. Thus, the goal is to treat nodes differently when they are involved in positive and negative events.

The reputation module of node A computes the reputation value $R_A^B(T_i)$ of node B over different monitoring sessions, where $T_i$ denotes the monitoring session in which the reputation value is computed. At start-up (first monitoring session $T_0$), the reputation value $R_A^B(T_i)$ of the node B is initialized to the

value $REP_0$ and it varies between 1 and $REP_{max}(REP_{max} <= 1)$.

For example, let: $R_A^B(T_0)$, $R_A^B(T_1)$, $R_A^B(T_2)$, ....., $R_A^B(T_n)$ the reputation values of node B over different monitoring sessions (it reflects the history of changing the reputation of a node), and the monitoring sessions $< T_0, T_1, T_2, ....., T_n >$ in which the reputation values are calculated . The reputation module of node $A$ aggregates the reputation values of the node $B$ $R_A^B(T_0)$, $R_A^B(T_1)$, $R_A^B(T_2)$, ....., $R_A^B(T_n)$ and computes its past reputation value $PREP_A^B(T_{i-1})$ as follows:

$$PREP_A^B(T_{i-1}) = \frac{R_A^B(T_0) + R_A^B(T_1) + R_A^B(T_2) + ...R_A^B(T_n)}{n}$$

$$= \frac{\sum_{i=0}^{n-1} R_A^B(T_i)}{n} \quad (1)$$

To compute the global reputation $GREP_A^B$ of node B, the reputation module of node A combines the past reputation value $PREP_A^B(T_{i-1})$ and the current reputation value $R_A^B(T_i)$ computed at time $T_i$ as follows:

$$GREP_A^B = (1 - \mu)PREP_A^B(T_{i-1}) + \mu R_A^B(T_i) \quad (2)$$

Where $\mu \in [0, 1]$ determines the importance given to the past reputation in comparison to the current reputation. Since $PREP_A^B(T_{i-1})$ is computed over multiple time periods, $\mu$ should be greater than 1- $\mu$.

The current reputation value of node B is updated after each event recorded by the monitoring module. Based on the type of event detected, $R_A^B(T_i)$ is updated as follows:

*4.2.1 Positive event*

If the monitoring module of node A detects a positive event against the node B in the time interval $[T_{i-1}, T_i]$, its reputation value will be incremented by a value $\alpha$

$$R_A^B(Ti) = R_A^B(T_i) + \alpha \quad (3)$$

The rate of incrementation $\alpha$ is calculated based on the global reputation of node B, and it is determined as follows:

$$\alpha = \frac{\theta}{1 - \frac{GREP_A^B}{REP_{max}}} \quad (4)$$

Where $\theta$ is a constant that controls the increment rate.

*4.2.2 Negative event*

In this case, the reputation value of node B over the time interval $[T_{i-1}, T_i]$ is decremented by a value $\beta$ as follows:

$$R_A^B(T_i) = R_A^B(T_i) - \beta \tag{5}$$

The decrement value $\beta$ is calculated based on the global reputation $GREP_A^B$:

$$\beta = \frac{\theta}{\frac{GREP_A^B}{REP_{max}}} \tag{6}$$

Where $\theta$ is a constant that controls the decrement rate.

*4.2.3 Discussion*

In our approach, the reputation value of a node is updated according to its behavior. If the node forwards correctly a data packet, its reputation value is incremented, otherwise its reputation value is decremented. To ensure equality between the nodes, we have opted to use different increment and decrement rates in term of reputation. These rates are determined based on the past reputation of a node. So, a node with a high reputation sees its reputation value: incremented with a high value $\alpha$ and decremented with a low value $\beta$. On the other hand, the reputation value of a node that drops data packets is decremented with a high value $\beta$ and incremented with a low value $\alpha$. This property does justice to cooperative nodes that behave well. Thus, malicious nodes will be unmasked quickly as their reputation values deteriorate rapidly due to their dropping activities.

If the reputation value $R_A^B(T_i)$ of node B falls below reputation threshold $REP_{th}$, the exclusion module is invoked for its punishment.

## 4.3 Exclusion module

The exclusion module is responsible for punishing malicious nodes and isolating them from the network. If a node A finds that the reputation $R_A^B(T_i)$ of its neighbor node B is lower than the reputation threshold $REP_{th}$, the node B is regarded as malicious, and it is added to the list of malicious nodes detected $BlackL_A$ by the node A. Then, the node A sends a malicious report to the source node to notify them about the malicious node detected. Each node receiving the malicious report as a receiver or in the promiscuous mode proceeds to the following exclusion process:

- Add the detected node to its blacklist
- Invalidate all forwarding routes involving the detected node
- Refuse to route all the RREQ initiated by the detected node.

### 4.4 Route selection module

The route selection module is involved in the route discovery process. It is responsible for choosing reliable forwarding routes based on the reputation values of the nodes.

A new field, denoted the route incorporation threshold $RIT$, is added to the header of the RREQ and RREP packets. The incorporation of $RIT$ enables nodes to put restrictions on the nodes implied in a forwarding route. The value of $RIT$ determines whether a node can be included in a forwarding route based on its reputation value. The value of $RIT$ represents the minimum reputation value of a node which should have to be implied in a forwarding route. It is determined based on the requirement of the MANET applications. The purpose of this strategy is to include only the high reputed nodes in forwarding routes in order to ensure the correct transmission of data packets. Following this strategy, we ensure that data packets are forwarded through high reputation nodes that behaved well in the past.

When a source node S wishes to establish a forwarding route to a destination node D (See Fig. 1), it broadcasts a route request RREQ which contains: the addresses of the source and the destination nodes, a list of intermediate nodes addresses and the field $RIT$. Each intermediate node receiving the RREQ packet checks whether the source is a neighbor. In this case, it simply rebroadcasts the RREQ packet. Otherwise, it compares the reputation value of the intermediate node (That forwards the RREQ) with the value of the $RIT$ field of the RREQ packet. Thereof, two cases arise:

- If the reputation of the intermediate node is below the $RIT$ value, and there is an interaction in the past between these two nodes, the route request RREQ is ignored.
- If the reputation of the intermediate node is greater than $RIT$ value, the node adds its address in the RREQ packet, and it rebroadcasts the RREQ to its neighbors.

Once the route request RREQ reaches the destination node D, this latter creates and sends an RREP packet to the source node using the route included in the RREQ packet. Each intermediate node checks whether the source of the RREP packet is a neighbor. In this case, it simply forwards the RREP. Otherwise, it compares the reputation value of the intermediate node with $RIT$ value. If the reputation is below $RIT$ value, the RREP is ignored and dropped. Otherwise, the node simply forwards the RREP. When an RREP packet reaches the source node S, a reliable route is established between the source and the destination nodes. Among all the discovered routes, the shortest in terms of the number of hops is selected. However, if the route discovery process does not find any forwarding routes, the source node decrements the value of the $RIT$, and it restarts again the route discovery process. The process of discovering routes in I-WG approaches are depicted in the Fig. 2

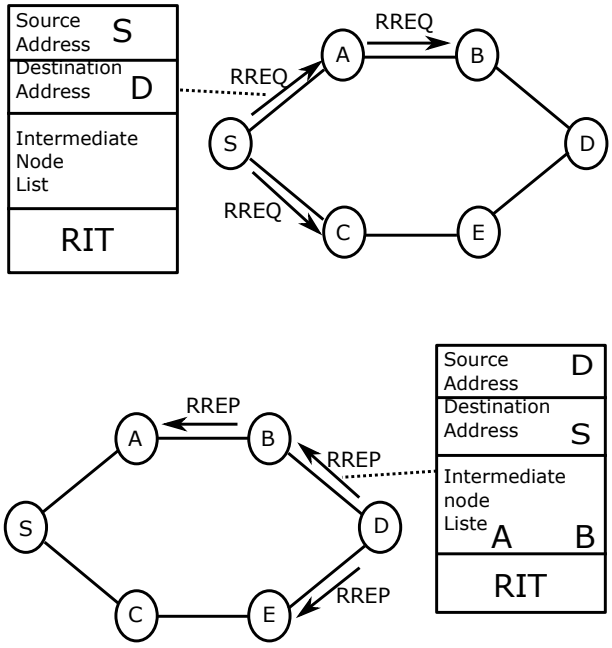



**Fig. 1** Example of discovering forwarding routes

## 5 Simulation and performance evaluation

In this section, we performed a series of simulations using the NS-2.34 simulator to study the performance of our I-WG approach. We compare the performance of I-WG approach with the standard watchdog approach [4]. The reasons for selecting Watchdog approach for comparison are: Firstly, almost of all existed reputation approaches employ watchdog approach as underlying reputation approach. Secondly, similarly to watchdog, almost of existed reputation approaches select the shortest forwarding routes in all situations and they have not made in restriction about the nodes implied in the route discovery.

### 5.1 Simulation environment

We simulated 40 mobile nodes randomly deployed in an area of 700mm $\times$ 700mm. The IEEE 802.11 MAC is used. While, the UDP traffic with CBR (constant bit rate) is used, The transmission range of each node is set to 250 m, and the simulation time is fixed at 600 s. We denote by $P_d$ the probability of dropping data packets. When the value of $P_d$ is set to 1, malicious nodes drop all the data packets. On the other hand, if $P_d$ is lower than 1, malicious nodes drop only a fraction of the data packets following the probability of $P_d$.

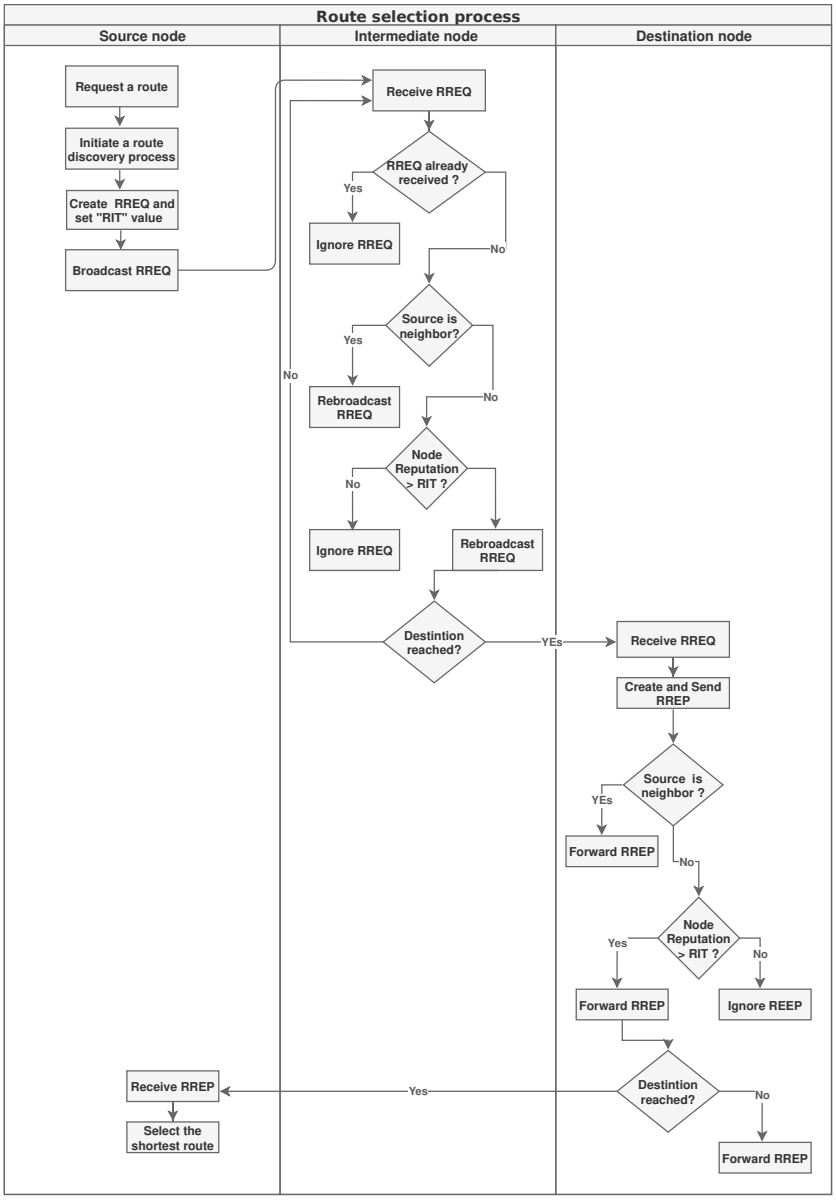



**Fig. 2** Route selection process

At start up, the reputation value $REP_0$ assigned to each node is set to 50 and it varies between 1 and 100. Table 2 shows the rest of the parameters used in the simulation.

**Table 2** Simulation parameters

| Parameter | Value |
|---|---|
| Number of nodes | 40 |
| Routing protocol | DSR |
| Simulation area | 700 m × 700 m |
| Transmission range | 250 m |
| Node speed | 10 m/s |
| Pause time | 0 s |
| Number of malicious nodes | 2,4,6,8,10 |
| Mobility model | Random Way Point |
| Mamicious node ID | 9, 12 and 14 |
| Number of CBR | 10 connections with 4 packets per second |
| $P_d$ | 0.5, 0.75 and 1 |
| $REP_0$ | 50 |
| Simulation time | 600 s |

We have used the following two metrics to evaluate the performance of our approach

- **Success rate:** is the ratio between the number of data packets received by the destination to the number of packets sent by the sources
- **Number of dropped packets:** represents the number of data packets dropped by malicious nodes.
- **End-to-End Delay (ms):** represents the average time taken by all packets to reach successfully their destinations after they are created at their sources

## 5.2 Simulation results

In our simulation, the performance metrics are obtained by varying $P_d$.

### *5.2.1 Case 1: $P_d$ is set to 1*

In this case, we set the dropping probability of node $P_d$ to 1 and we plot the evaluations metrics across varying the number of malicious nodes.

Fig. 3 shows the success rate of the I-WG and Watchdog approaches. We can observe that the success rate of the two approaches decreases by increasing the number of malicious nodes. This is logical because when the number of malicious nodes increases, there is a low chance to select forwarding routes without involving malicious nodes. However, we can remark that the success rate with the I-WG approach is higher than the success rate of the Watchdog approach. This is due to the fact that the I-WG approach is able to unmask and isolate malicious nodes quickly. As malicious nodes drop data packets, their reputation values degrade. Therefore, they receive high decrement in term of the reputation for each dropping activity, which causes their identifications.

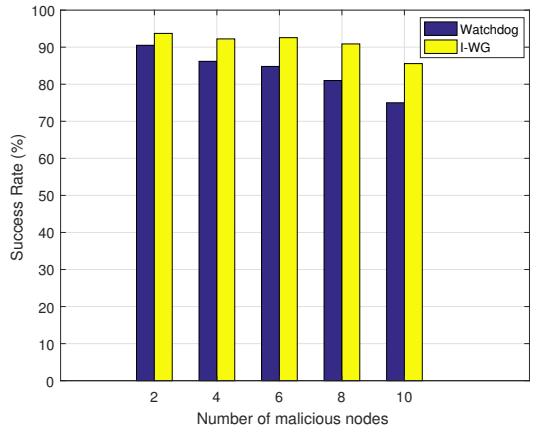



**Fig. 3** Success rate with $P_d = 1$

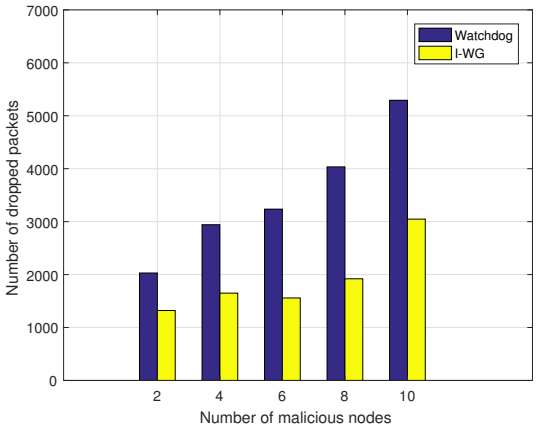



**Fig. 4** Number of packet dropped with $P_d = 1$

On other hand, the Watchdog approach treats all nodes in the same way regardless of their reputation values.

Fig. 4 shows the number of data packets dropped by the malicious nodes. It is plotted by varying the number of malicious nodes. The results show that the number of packets dropped in all approaches increases with the increase in the number of malicious nodes in the network. Nevertheless, we can observe that the I-WG approach reduces the number of packets dropped by malicious nodes in comparison to the watchdog approach. For this reason, with I-WG approach, the reputation values of malicious nodes degrade rapidly, which permits to identify them rapidly. So, malicious nodes are detected quickly, and they are avoided in the process of the selection of forwarding routes, which minimizes the number of packets dropped before their exclusions.

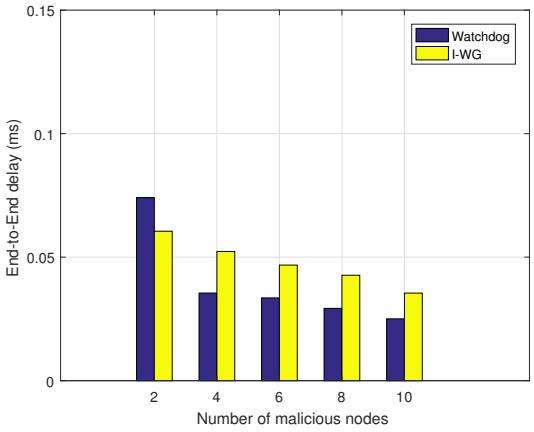



**Fig. 5** End-to-end delay with $P_d = 1$

As shown in Fig. 5, the I-WG approach increase the end-to-end delay in comparison to watchdog approach. This is because I-WG approach incorporates a reputation restriction in the route discovery process. In I-WG approach, only reputed nodes behaving-well are involved in a forwarding route. So, the selected forwarding route is more reliable, but it may be not the shortest route which increase obviously the end-to -end delay. However, the watchdog approach selects the shortest forwarding route in all cases independently to the reputation values of nodes implied.

### *5.2.2 Case 2: varying $P_d$*

To evaluate the impact of the selective dropping activities of nodes on the performance of I-WG and Watchdog approaches, we have varied the dropping probability $P_d$.

Fig. 6 shows the number of packets dropped by malicious nodes with $P_d = 0.75$. We can observe that the I-WG approach minimizes the number of packets dropped compared to the Watchdog approach. This can be explained with two reasons: (1) First, The I-WG approach can detect and isolate malicious nodes, even in the case when they act intelligently by dropping only a fraction of data packets, because the I-WG approach uses the past reputation of a node to determine the rates of incrementation and decrement of reputation. (2) Second, the I-WG approach routes data packets through the nodes that satisfy the reputation requirement, which improves the probability to deliver the data packets correctly.

As shown in Fig. 7, we choose three malicious nodes adopting selective dropping attack according to $P_d$. We can observe that I-WG reduce the number of packets dropped by malicious nodes in comparison to Watchdog approach. This is because, I-WG approach puts reputation restriction about the nodes that can be implied in a forwarding route. When a node drops packets, its

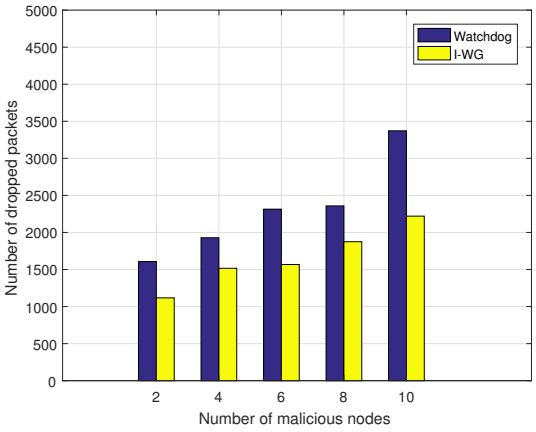



**Fig. 6** Number of packet dropped with $P_d = 0.75$

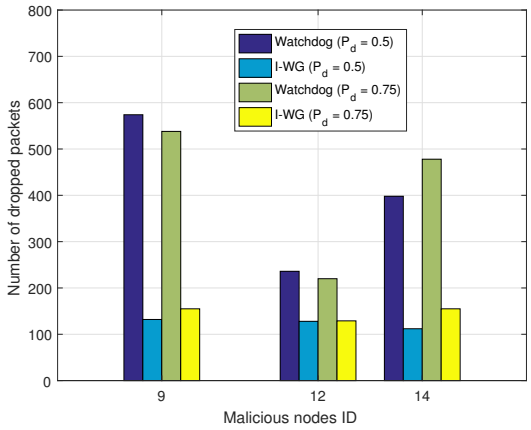



**Fig. 7** Number of packet dropped Vs Malicious node ID

reputation value degrades which leads to evict this node in the route discovery process. On the other hand, in watchdog approach, if the reputation value of node doesn't fall below the threshold, it continues to drop data packets without been detected which cause a damage on network performance.

## 6 Conclusion

In this paper, we have proposed a new approach denoted I-WG which is an extension enhancement of the watchdog approach. The enhancement consists on the thwarting the limitation that consists on the incapacity to detect smart malicious nodes that selectively drop data packets to cause damage on the

forwarding activities while at the same time to avoid to be unmasked. The proposed approach employs the watchdog approach as monitoring technique. Thus, we have proposed a new reputation computation method that permits to evaluate the node reputation by taking account the past behaviors of nodes. Thus, we have made a difference between the increment and decrement rate in term of reputation in order to differentiate between a high-reputed node and a low reputed node when they are involved in a forwarding activity, which ensures equality between nodes. The simulation results show that the proposed approach permit to ameliorate the success rate and to reduce the number of data packets dropped by malicious nodes before their identification, while at the same time increase the end-to-end delay.

As future work, we plan to extend our approach to be able to cope with the collusion attack that occurs when two consecutive nodes along the forwarding routes collaborate in order to hide their malicious behaviors.

## Funding

Not applicable.

## Conflict of interest

Not applicable.

## Availability of data and material

Not applicable.

## Code availability

Not applicable.

## Authors' contributions

Not applicable.

## References

1. Thangaraj, K., & Dharma, D. (2020). Optimized Fuzzy System Dependent Trust Score for Mobile AdHoc Network. Wireless Personal Communications, 1-15.
2. Nabou, A., Laanaoui, M. D., & Ouzzif, M. (2020). New MPR Computation for Securing OLSR Routing Protocol Against Single Black Hole Attack. Wireless Personal Communications, 1-20.

3. Bounouni, M., & Bouallouche-Medjkoune, L. (2018). Acknowledgment-based punishment and stimulation scheme for mobile ad hoc network. The Journal of Supercomputing, 74(10), 5373-5398.
4. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265).
5. Bansal, S., & Baker, M. (2003). Observation-based cooperation enforcement in ad hoc networks. arXiv preprint cs/0307012.
6. Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (pp. 226-236).
7. Michiardi, P., & Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced communications and multimedia security (pp. 107-121). Springer, Boston, MA.
8. Channa, M. I., & Ahmed, K. M. (2011). A reliable routing scheme for post-disaster ad hoc communication networks. JCM, 6(7), 549-557.
9. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2016). A trust aware routing protocol for energy constrained wireless sensor network. Telecommunication Systems, 61(1), 123-140.
10. Ahmed, A., Kumar, P., Bhangwar, A. R., & Channa, M. I. (2016, December). A secure and QoS aware routing protocol for Wireless Sensor Network. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 313-317). IEEE.
11. Sharma, R., & Gupta, D. V. (2018, January). A Reputation-Based Mechanism to Detect Selfish Nodes in DTNs. In International Conference on Communications and Cyber Physical Engineering 2018 (pp. 55-61). Springer, Singapore.
12. Manikandan, R., Mangayarkarasi, R. (2019). Evaluation to Perform a Scattered for Detecting Selfish Nodes in MANET using Collabrative Watchdog Algorithm. International Journal of Computer Sciences and Engineering, 7(6), 788-792.
13. Ragunathan, R., & Vadivel, R. (2018). COCOWA MODEL: WATCHDOG MECHANISM USED TO PROPAGATE SELFISH NODES IN CELLULAR NETWORKS OF MOVING VEHICLES. International Journal of Advanced Research in Computer Science, 9(2).
14. Preetha, M., & Sugitha, S. (2016, February). Identifying selfish nodes using mutual neighbor based watchdog mechanism for DTN. In 2016 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-5). IEEE.
15. Hernandez-Orallo, E., Olmos, M. D. S., Cano, J. C., Calafate, C. T., & Manzoni, P. (2014). CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes. IEEE transactions on mobile computing, 14(6), 1162-1175.
16. Hernandez-Orallo, E., Serrat, M. D., Cano, J. C., Calafate, C. T., & Manzoni, P. (2012). Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Communications letters, 16(5), 642-645.
17. Lal, N. (2014). An effective approach for mobile ad hoc network via I-Watchdog protocol. arXiv preprint arXiv:1412.8013.
18. Lal, N., Kumar, S., Saxena, A., & Chaurasiya, V. K. (2015). Detection of malicious node behaviour via I-watchdog protocol in mobile Ad Hoc network with DSDV routing scheme. Procedia Computer Science, 49, 264-273.
19. Kollati, V. K. (2017). IBFWA: Integrated Bloom Filter in Watchdog Algorithm for hybrid black hole attack detection in MANET. Information Security Journal: A Global Perspective, 26(1), 49-60.
20. Kumar, S., & Dutta, K. (2018). Trust based intrusion detection technique to detect selfish nodes in mobile ad hoc networks. Wireless Personal Communications, 101(4), 2029-2052.
21. Derhab, A., Bouras, A., Belaoued, M., Maglaras, L., & Khan, F. A. (2020). Two-Hop Monitoring Mechanism Based on Relaxed Flow Conservation Constraints against Selective Routing Attacks in Wireless Sensor Networks. Sensors, 20(21), 6106.
22. Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Springer, Boston, MA.

# Figures

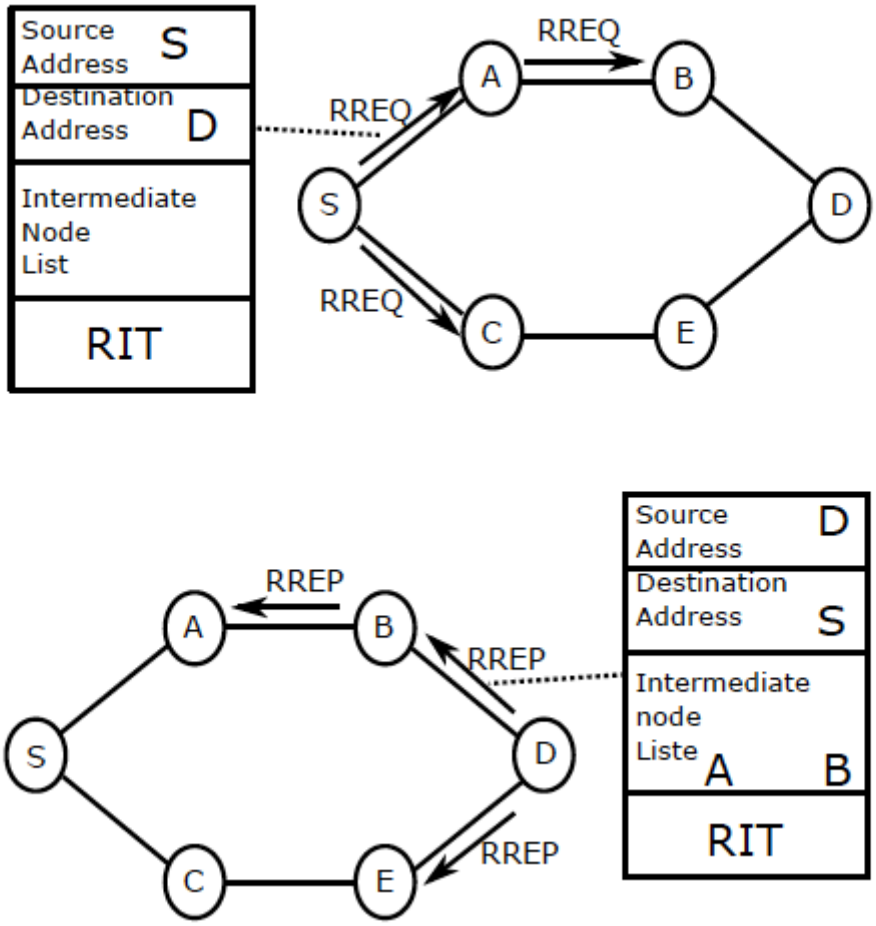
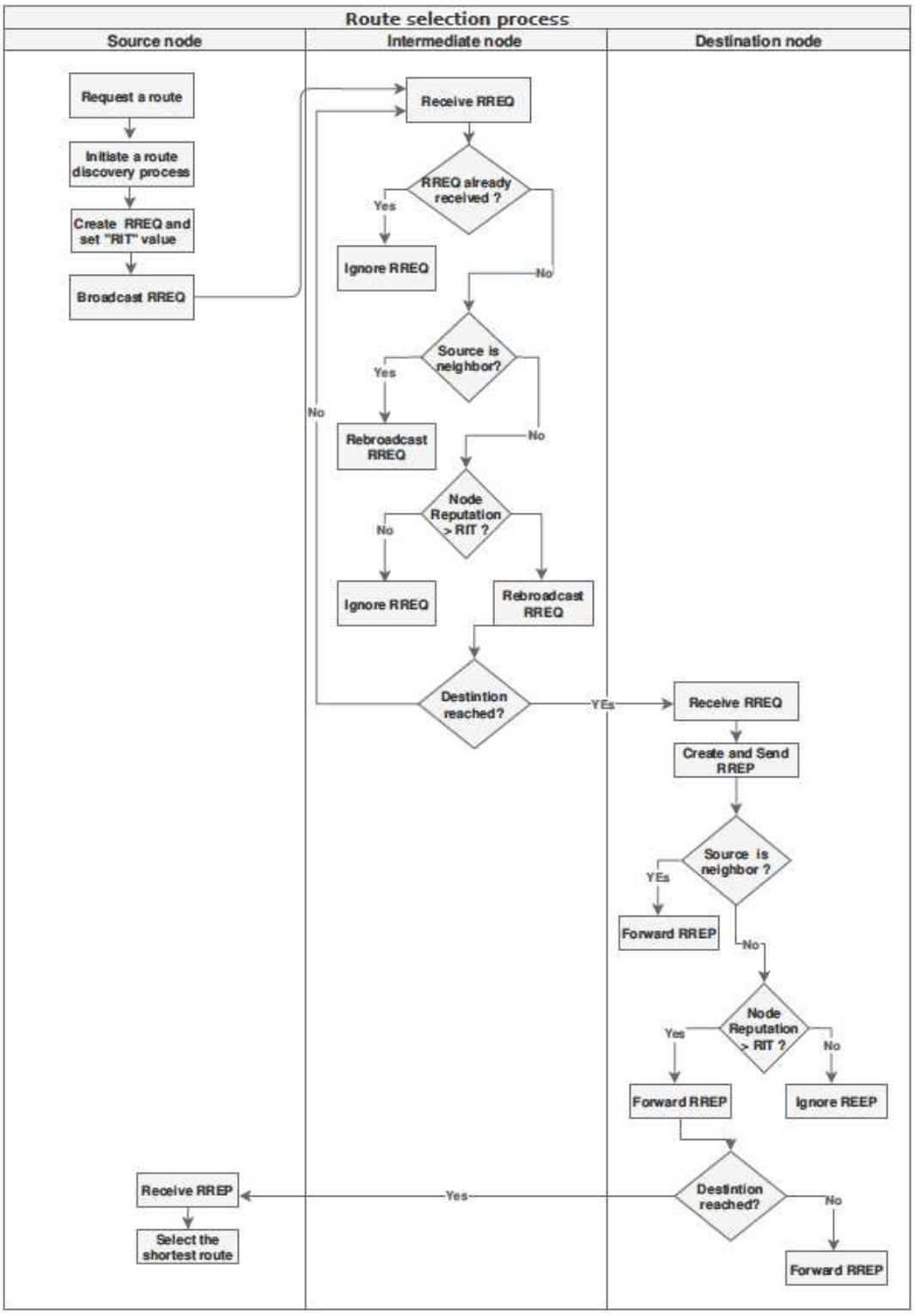



**Figure 1**

Example of discovering forwarding routes




## Figure 2

Route selection process

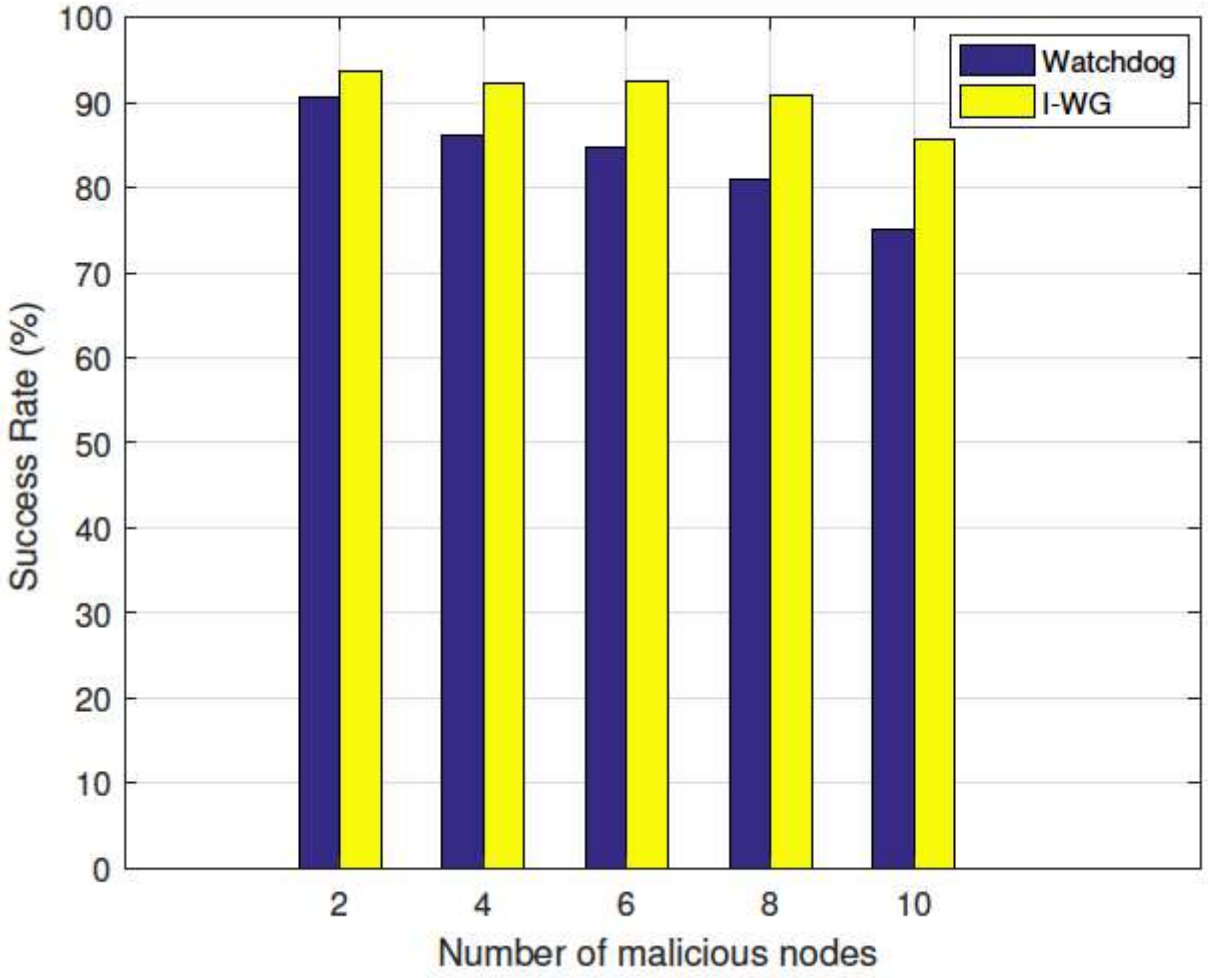



**Figure 3**

Success rate with Pd = 1

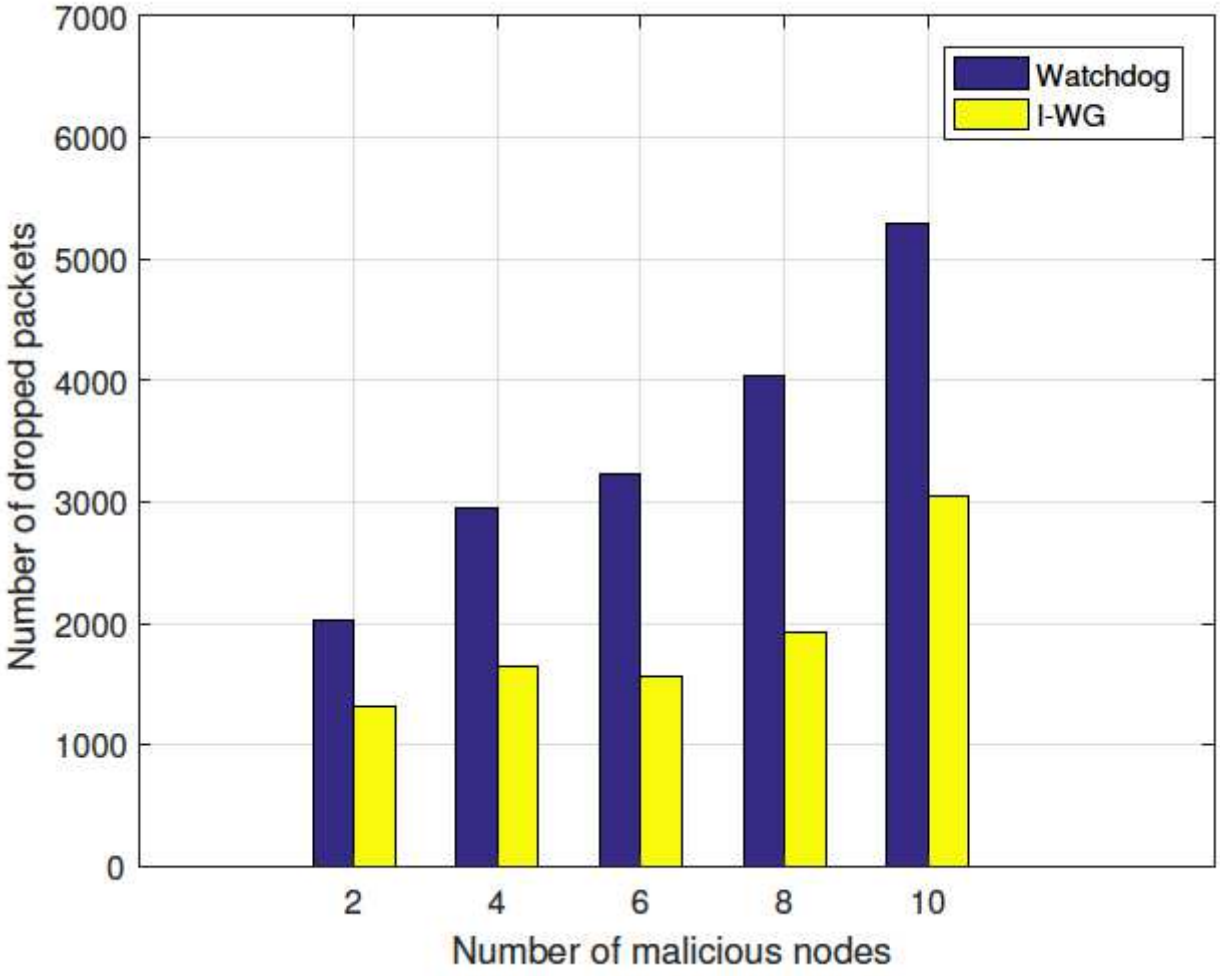



**Figure 4**

Number of packet dropped with Pd = 1

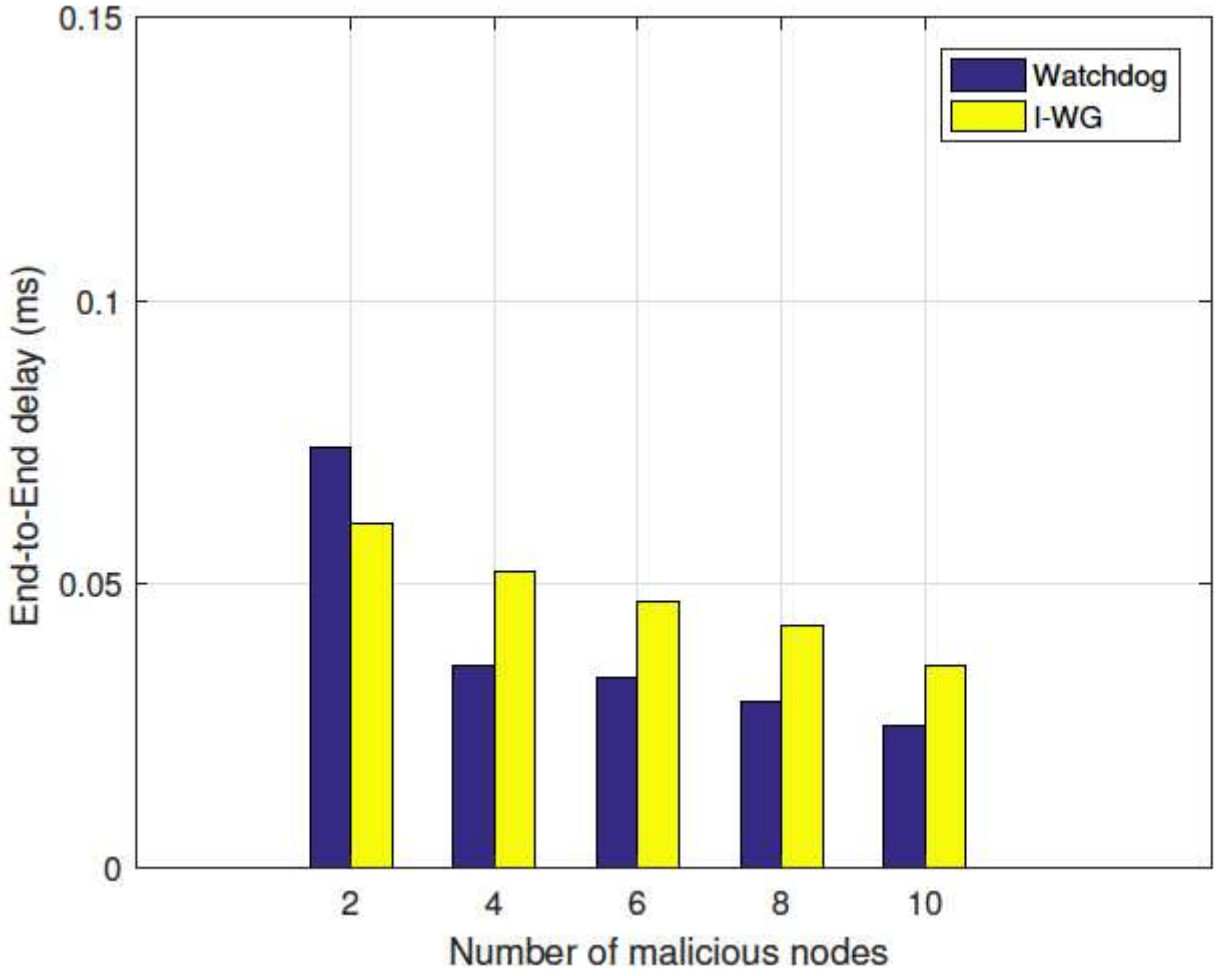



**Figure 5**

End-to-end delay with Pd = 1

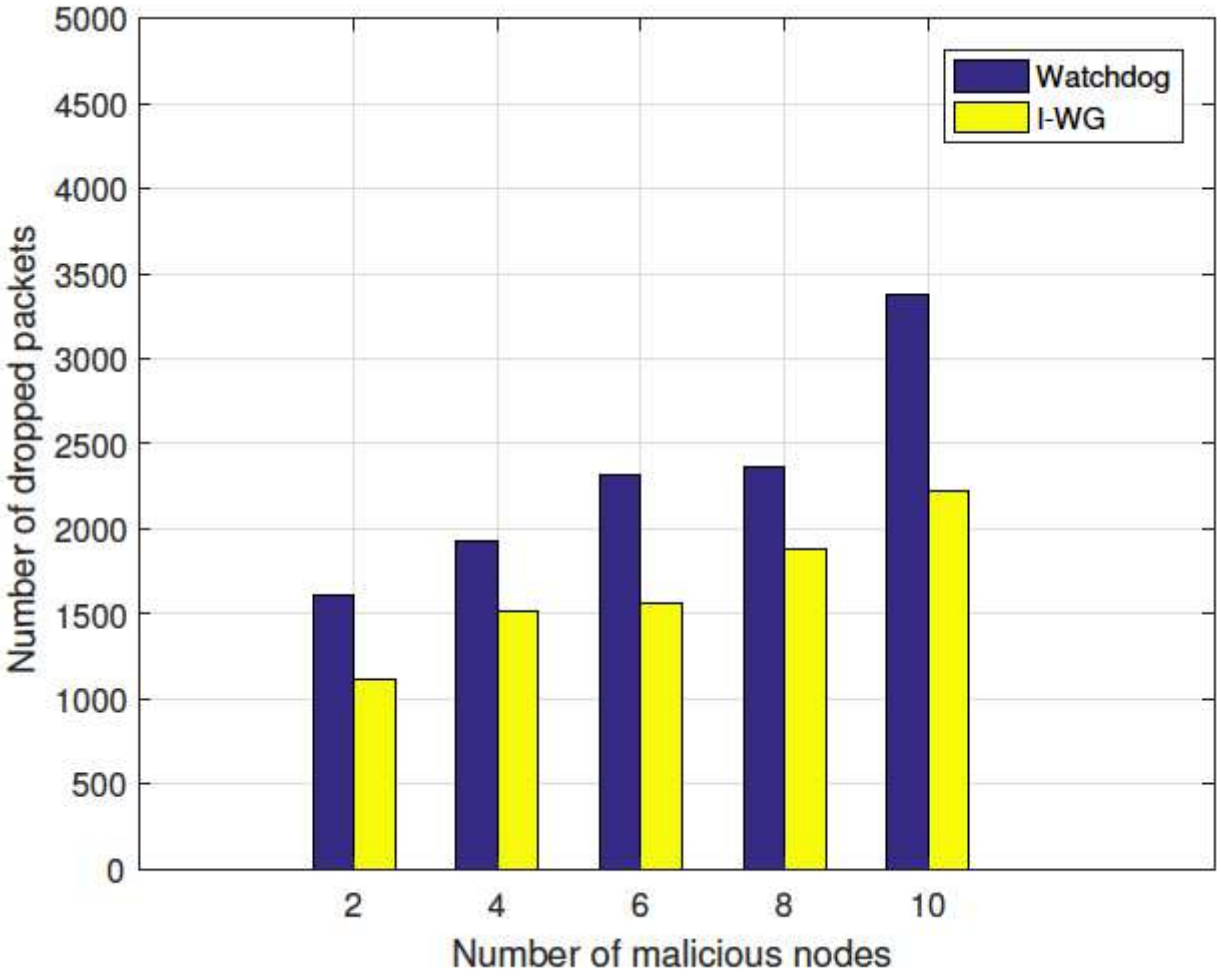



**Figure 6**

Number of packet dropped with Pd = 0:75

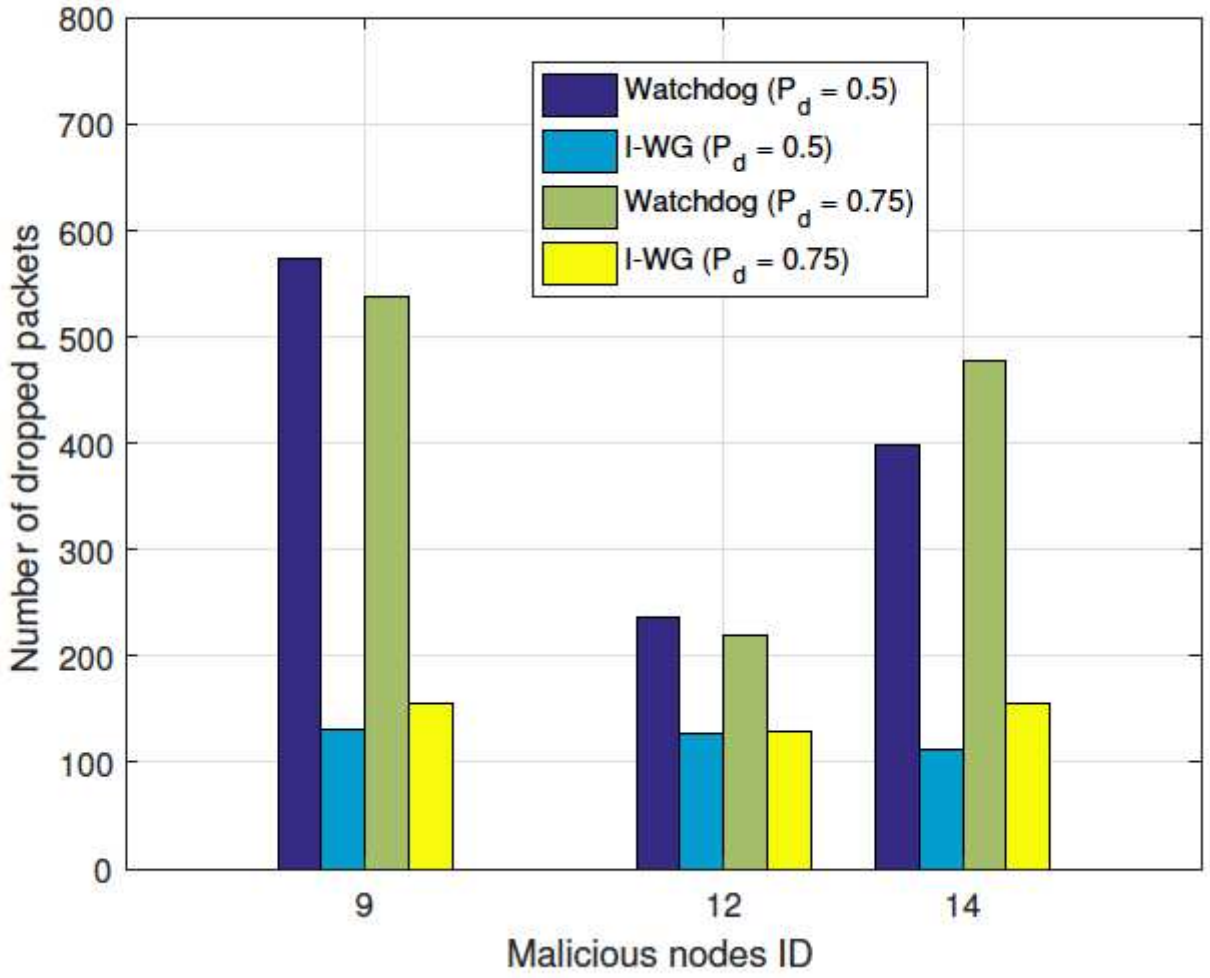



**Figure 7**

Number of packet dropped Vs Malicious node ID