Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET

Assia Hammamouche, Mawloud Omar, Nabil Djebari, Abdelkamel Tari

Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET

Assia Hammamouche[(1)], Mawloud Omar[(2)], Nabil Djebari[(1)], and Abdelkamel Tari[(1)]

(1) Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes
Université de Bejaia, 06000 Bejaia, Algérie.

(2) Unité de Recherche LaMOS, Faculté des Sciences Exactes
Université de Bejaia, 06000 Bejaia, Algérie.

Abstract

Ad hoc network is a set of mobile nodes interconnected by wireless communication. It is easily and less expensive to deploy, but it is vulnerable against various attacks. The node data should cross a set of intermediate nodes in order to reach the intended destination. An intermediate node, which takes part of the routing process, can behave maliciously and drop the packets passing through it instead of transferring them to its successor, which leads to what is called black hole attack. Several solutions have been proposed in the literature review. However, these solutions suffer from the imbalance between robustness and overhead. In this context, we propose a solution based on reputation of nodes and multi-hop acknowledgment. The reputation of nodes increases or decreases depending on the situation and the observation condition. When the node reputation passes below the threshold, then it will be considered as a black hole node. The proposed approach detects and excludes simple and cooperative black hole attackers and enforces the cooperation among the network nodes. Through simulation, we compare the proposed approach to a concurrent protocol and we show its efficiency in terms of detection ratio and communication overhead.

Keywords: Wireless ad hoc network, Routing protocol security, Black hole attack, Trust, Reputation.

1. Introduction

Mobile ad hoc network (MANET) is easily installable and thus, a very economical and popular computing environment; however, it is highly constrained and challenging too. A portable node possesses limited computing power processors, small stable storage, thin battery for energy backup, and a short communication range. They can communicate only via message passing over wireless links. Nodes that are not in the transmission range of each other can communicate via message relay. The nondeterministic mobility pattern incurs concurrent and arbitrary topological changes. The topological changes become more frequent because of the dynamism in wireless links and limited availability of bandwidth. A highly performance retarding offshoot of this phenomena is the variable message delay. Hence, the distributed algorithms developed for static domain are not directly implementable in MANETs [1]. They are mostly employed in the military applications where their mobility is attractive, but have also a high potential for use in civilian applications such as coordinating rescue operations in the infrastructure-less areas, sharing content and network gaming in the intelligent transportation systems, surveillance and control in wireless sensor networks, etc. [2]. One of the most challenging issues in these networks is the security.

Security is one of the main issues for networks. It becomes more challenging in ad hoc networks due to the lack of central access point to monitor node behavior and to manage node membership. Any network security system aims to satisfying the following goals: privacy and confidently, authenticity, integrity, and access control. All security attacks on any system are a violation of one or more of these goals. An ad hoc network is vulnerable to the following types of attacks: denial of service (DoS) which influences the availability of a given node or even the services of the entire network, impersonation attacks which occurs when external nodes exploit the weak authentication of the network to join it as a normal node and begin to carry out its malicious behavior such as propagating fake routing information, eavesdropping to obtain some confidential information that should be kept confidential during the communication, and attacks against routing which include network partitioning, routing loops, and route hijacks [3]. In mobile ad hoc networks, the data packets are forwarded through intermediate nodes over a specific path. An intermediate node participating in the routing process can be malicious and drops the packets instead to forward them. This misbehavior is due to a selfish attack if the latter is happened to preserve the attacker resources. However, an attacker could perform such attack, called black hole, in order to compromise the communication among the network nodes. One or several cooperative attackers can execute the black hole attack.

The literature offers a large amount of works against the black hole attack. These solutions are either preventive or detective. A preventive approach tries to constrain the packet dropping by forcing on the cooperation among the network nodes [13]. However, the main disadvantage of this type of solutions is that a malicious node could announce a false report on its neighbors or spreading false alarms. Prevention mechanisms, by themselves cannot en-

sure a complete cooperation among the network nodes [22]. A detective approach detects and eventually eliminates a black hole node when it appears in the network [13]. The multihop acknowledgment identifies the black hole nodes, however, it generates an important overhead. To minimize the latter, it is primordial to use one and two hop-acknowledgment when the packet routing proceeds incorrectly. The solutions based on the acknowledgments detect only the simple black hole attack. Nevertheless, the approaches based on the reputation detect also the cooperative black hole attack. The main limitation regarding this type of solutions is the efficiency. The existing solutions prevent simple and cooperative black hole attack by keeping less attention to the communication overhead. The main purpose of this work is to address this important aspect. In this paper, we propose a lightweight trust-based approach against the black hole attack. The proposed approach is detective, preventive, and is efficient against both simple and cooperative black hole attacks. It is based on multi-hops acknowledgment and reputation mechanism. Through simulation, we compare the proposed approach to a concurrent protocol and we show its efficiency in terms of detection ratio and communication overhead.

The rest of this paper is organized as follows. In Section 2, we present a background of black hole attack in the context of mobile ad-hoc networks. In Section 3, we present the related work. In Section 4, we give the detailed description of the proposed approach. In Section 5, we present the simulation results, and in Section 6, we conclude the paper.

2. Black hole attack

To perform the black hole attack, a malicious node should belong to the routing path, and then it drops the messages passing through it instead of transferring them to its successor. To do this, two possibilities are distinguished. In the first case, to lead the attack without violating the routing protocol specifications, the black hole node is inserted into the routing path by executing correctly the routing protocol. In the second case, the attack can be performed by violating the routing protocol specifications. Therefore, the attacker must exploit the routing protocol vulnerabilities. The manner in which the black hole node is inserted over the routing path is different from a routing protocol to another. Regarding the number of malicious nodes, black hole can be studied on two different types of attack, namely simple and cooperative black hole.

2.1. Simple black hole attack

In the black hole attack, a malicious node uses the routing protocol in order to publicize itself for having the shortest route to the destination node. It offers its availability for fresh routes regardless of checking its routing table. The attacker node has always the accessibility in replying to the route request in order to get the data packet and drop it [4]. In the flooding-based protocols, the malicious node reply will be received by the requesting node

before the reception of a reply from any other node. Therefore, a faked route will be created, and depending on the node whether to drop the packets or forward them to an unknown address [5].

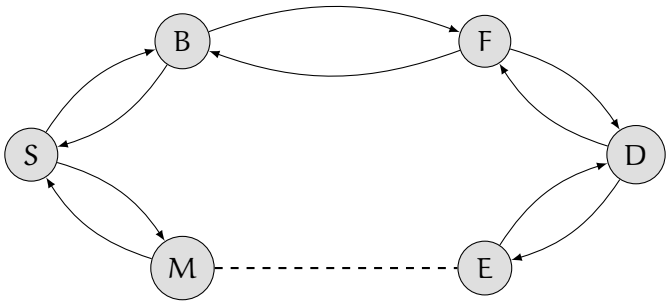

Figure 1: Simple black hole attack

Figure 1 shows how the black hole attack is performed. A source node S want to send data packets to a destination node D and initiates the route discovery process. So, if the node M is malicious, then it will claim that it has active route to the specified destination as soon as it receives the request packet. Then, it will send the response to the node S before any other node. The node S will ignore all the other replies and will start sending the data packets to the node M.

2.2. Cooperative black hole attack

The black hole attack can be also conducted in a cooperative manner, where multiple malicious nodes act in coordination to violate the routing protocol specification or the implemented security mechanism [6]. As depicted in Figure 2, when malicious nodes M_1 and M_2 act together, M_1 refers to M_2 as its next hop. Following the scenario of [6], the source node S sends a Further Request packet (FReq) to M_2 through another route other than via M_1 (e.g., S–C–E–M_2). The node S asks M_2 if it is the next hop of M_1 and if it has a valid route to the destination node D. Since the node M_2 is cooperating with M_1, its Further Reply (FRep) will be positive. Consequently, the source node S assumes that the route S–M_1–M_2 is secure, and over which starts sending the data packets. Once intercepted, the packets will be dropped by M_1.

3. Related work

There are hundreds consistent works which address the security issues in MANETs. The authors of [7, 8, 9] summarize a good representative part of them. In this section, we focus on the black hole attack and we present from the literature some relevant solutions, which we compare in Table 1.

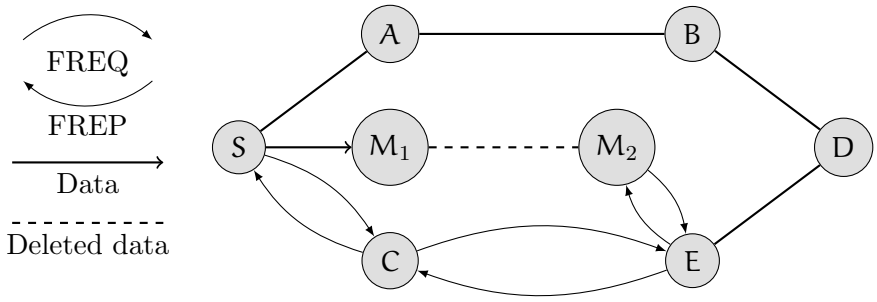

Figure 2: Cooperative black hole attack

Many works have been done for detective approaches by focusing on multi-hops acknowledgment. In [10], Marti et al. have proposed an approach in which the watchdog monitors the successor node after sending to it a packet. This is performed by overhearing the channel and checking whether it relays or drops the packet. The pathrater accuses a monitored node for misbehaving if the latter drops more than a given number of packets. Although simple to implement, but this technique cannot detect the black hole node in some cases [11]. In [6], Deng et al. have proposed an improvement of AODV (Ad hoc On demand Distance Vector), in which a further route request (FRREQ) has sent to the next hop of route reply (RREP). If the FRREQ replies back with further route reply (FRREP) confirming that the node is its neighbor and it has a route to the destination, it is considered as a truthful node. In [21], Li and Lee have proposed PLRSA (Promiscuous Listening Routing Security Algorithm), where each node constructs the LCL (Local Connectivity List). LCL maintains trust level values updated dynamically for any node. If the value of the trust level is lower than an already defined threshold, the node will be considered malicious. PLRSA does not generate communication overhead and can be easily added to existing routing protocols, however, it cumulates the watchdog limits. Djenouri and Badache [12] have proposed an approach based on 2HAck that overcomes some watchdog's shortcomings including ambiguous collisions, receiver collisions, and limited transmission powers. Consider three successive nodes A, B and C in the end-to-end path, in which the node C acknowledges the A's message sent through B. In order to prevent 2HAck packets from being falsified, the authors use an authentication technique based on asymmetric encryption. The 2HAck packets are forwarded by an intermediate node. Without proper protection, a malicious node B can simply fabricate 2HAck packets and claim that they were sent by node C. However, the cooperative black hole attack cannot be avoided. Alem and Xuan [17] have proposed IDAD (Intrusion Detection using Anomaly Detection). In this method, the audit data must be collected and provided. Then, the IDAD detection process is to compare every activity with the audit data. If any node activity is out of the activities listed in the audit data, the IDAD isolates the suspected node from the network. Su et al. [18] have proposed ABM (Anti-Black hole Mechanism), in which IDS nodes are deployed in the network monitoring. Their role is to estimate the suspicious value of a node

according to the amount of abnormal difference between the transmitted RREQs and RREPs from the node. Baadache and Belmehdi [13] have proposed Merkle tree-based approach. All the intermediate nodes need to acknowledge the reception of the packet. Using these acknowledgments, the source node constructs a Merkle tree and compares the value of the tree root with a precalculated one. If both values are equal, then the end-to-end path is packet droppers free. According to the authors, this method generates an additional overhead due to the acknowledgments exchanged between the source and the intermediate nodes. In [25], Khan et al. have proposed an algorithm makes use of the sequence number to identify the black hole nodes. A node is considered as a malicious node if its sequence number does not lie between the minimum and maximum of the specified sequence numbers. The collaborative attacks are handled in a way if all the nodes whose sequence numbers are higher than the specified maximum allowed sequence numbers and smaller than that of the sequence number allowed in the MANETs routing protocol. Panda and Pattanayak [26] have proposed an agent-based technique that relies on the ACO (Ant Colony Optimization) metaheuristics to find out the optimal path during routing, along with the security is provided using digital signatures, and Watchdog and Pathrater mechanism [10] to detect and avoid the black hole attacks.

There are also several works in the context of preventive approaches based on the reputation of nodes. Each node maintains a degree of confidence, and the value of the latter is calculated and stored with other nodes that monitor the behavior of the given node. In [19], Michiardi et al. have proposed CORE (COllaborative REputation). The system is based on three techniques subjective assessment, indirect observation, and functional reputation calculation. Based on this combination, the result is made to isolate the node or not. A similar approach is conducted by Buchegger et al. in [20] with the CONFIDANT system. This approach integrates the trust manager and the reputation system to Watchdog and Pathrater [10]. The trust manger evaluates the reported events by watchdog and reports alarm to the neighbor regarding the malicious node. In [14], Tamilselvan et al. have proposed PCBHA (Prevention of a Cooperative Black Hole Attack). This method makes use of a "Fidelity Table" wherein every participating node will be assigned a fidelity level that acts as a measure of reliability. In case of the level of any node drops to 0, it is considered to be a black hole node and is eliminated. In [3], Khamayseh et al. have introduced a data structure referred as a trust table in each node. The RREP packet is extended with one more field called trust field. This field indicates the reliability of nodes. Source nodes send their data only if the reply is from the trusted node, otherwise, they wait for other RREPs from nodes having to pass behavioral analysis filter. In [15], Gurung and Chauhan have proposed MBDP-AODV (Mitigating Black Hole effects through Detection and Prevention) based on a dynamic threshold value of the destination sequence number. In [24], Dorri has proposed a table based approach to mitigate the cooperative black hole attack in the context of MANETs. The idea is to use data control packet to ensure the authenticity of all the nodes in the selected path. The

concept of extended DRI table is used to detect and eliminate the malicious black hole nodes. The main drawback of the proposed approach is the packet drop due to high end-to-end delay [25]. In [16], Sathish et al. have proposed two security solutions against the black hole attacks to detect single and collaborative black hole attacks. The key idea of the first is the use of fake route request, destination sequence number and next hop information to identify the malicious nodes. The second solution is a preventive approach to reduce the black hole impact using digital signatures and trust value helps.

Protocol	**Category**	**Routing protocol**	**Attack type**
[10]	Detective	DSR	Simple
[6]	Detective	AODV	Simple
[19]	Preventive	DSR	Cooperative
[20]	Preventive	DSR	Cooperative
[12]	Detective	AODV	Simple
[21]	Preventive	DSR	Simple
[14]	Preventive	AODV	Cooperative
[17]	Detective	DSR	Simple
[18]	Detective	AODV	Cooperative
[21]	Detective	AODV	Simple
[3]	Preventive	AODV	Simple
[13]	Detective	AODV & OLSR	Cooperative
[16]	Preventive & Detective	AODV	Simple & Cooperative
[15]	Preventive	AODV	Cooperative
[24]	Preventive	AODV	Cooperative
[25]	Detective	AODV	Cooperative
[26]	Detective	AODV	Cooperative

Table 1: Comparison of the reviewed solutions

4. The proposed approach

In this section, we present the proposed approach. First, we give explanations about the general ideas of the solution, and then the detailed description of its different operations.

4.1. Rational solution

We consider a network composed of a set of mobile nodes. The wireless links are bidirectional, i.e., for each pair of nodes, A and B, if A can communicate with B, then the latter is able to do the same. We assume that a public key certification service is set for encrypting messages and ensuring the data integrity, and the source node trusts the destination node. We note that these assumptions are reasonable and practically feasible.

The proposed approach is based on the trust model proposed in [23]. Our approach uses multi-hops acknowledgment and reputation mechanism against black hole attack. Each node has a reputation that reflects its behavior. This value is quantified and stored by the other nodes that monitor the behavior of the given node. The proposed approach stimulates the cooperation between the network nodes in the routing process. However, the presence of malicious nodes could noise the correct forwarding of the packets. In such case, we will face mainly two kinds of attacks. A malicious node could be either uncooperative or dropper node. The proposed approach focuses on the attacks that are performed by the dropper nodes, which we call black hole attackers. In order to localize the exact position of the black hole attacker in the routing path of a message having not reached its destination, we use two-hops and one-hop acknowledgements so that it makes the indictment of a node more precise, in the case where the number of acknowledgement-hops is more than two.

Each node n_i, $i = 1, 2, \cdots, |P|$, keeps in its locally the table TrustTable, which stores the reputation values of the other nodes. Whenever a node obtains information on another, it updates the value of its reputation if it has already an entry for this node. If no entry exists into the table corresponding to this node, then it creates a new one and saves this value inside. Initially, each node gives an initial reputation Θ_0 to the other nodes (refer to Table 2, which illustrates the data structure of TrustTable).

Node identity	Reputation of the node j in the i's eye
n_1	$\Theta_i(1)$
n_2	$\Theta_i(2)$
$\cdots$	$\cdots$
n_S	$\Theta_i(S)$

Table 2: Data Structure of TrustTable (S denotes the network size)

Each node n_i, $i = 1, 2, \cdots, |P|$, maintains in its locally the table PostTable, which stores the message identifiers that it routes and the path that it footprints. When the destination sends an acknowledgment to the source confirming its reception, all the nodes receiving this acknowledgment, check in their PostTable if they have packets corresponding to the acquitted one, and remove the corresponding line in this case. The nodes do the same when they receive the Blackhole_Alert packet. If during the time Ω, no acknowledgment is received for a given message, the corresponding line for this message will be deleted after sending the packet 2HAck to the back two-hops of nodes for clearing the back one-hop node (refer to Table 3, which illustrates the data structure of PostTable).

The tables TrustTable and PostTable do not generate an important storage overhead. In the worst case, when each node stores the reputation of all the other network nodes, the

Message identifier	Message path
M_1	n_1–n_2–$\cdots$–$n_{\lvert P_1 \rvert}$
M_2	n_1–n_2–$\cdots$–$n_{\lvert P_2 \rvert}$
$\cdots$	$\cdots$

Table 3: Data Structure of PostTable

TrustTable size in bits equals to

$$|\mathsf{TrustTable}| = (S-1) \cdot \Big(\log_2(S) + 32 \Big), \tag{1}$$

in the case of simple precision representation of real numbers. Furthermore, when each node stores the messages being routed, in the worst case, through paths of size S, the PostTable size in bits equals to

$$|\mathsf{PostTable}| = N \cdot \Big(\log_2(N) + S \cdot \log_2(S) \Big), \tag{2}$$

where N represents the number of the simultaneously transmitted messages per node.

The notations used in this paper are summarized in Table 4.

4.2. Detailed solution

4.2.1. Monitoring component

This component is responsible for monitoring and observing the behavior of neighboring nodes involved in a forwarding path to detect whether a node is malicious or legitimate. In the proposed approach, the result is the combination of three modes: ACK, 1HAck and 2HAck. The ACK mode is equivalent to the end-to-end acknowledgment mode. In the latter, the destination should return the packet ACK to the source using the reverse route when the transfer process proceeds correctly. However, if the source does not receive the packet ACK, it is necessary to use the 2HAck mode, in which each node involved in the message transfer sends the packet 2HAck to the node that is two-hop predecessor in the path that the message footprints. If a node does not receive the packet 2HAck, in this case, 1HAck mode will be used. The packet 1HAck will be sent by a node to its one-hop predecessor to make the indictment of a node more precise. We made the assumption that a certification service is implemented in the network, the messages will be encrypted to ensure their integrity and authenticity to avoid the malicious node falsified the acknowledge packets so that its predecessors will believe that the message is successfully received.

4.2.2. Reputation management

Let's consider a source node S, which needs to send a message to the node destination D. By using any protocol, the source node S builds-up a routing path $P = \langle n_1, n_2, \cdots, n_{|P|} \rangle$,

Table 4: Used notations

Notation	Significance
2HAck	Packet to send by a node to its two-hop predecessor in the path that the message footprints
1HAck	Packet to send by a node to its one-hop predecessor if the message 2HAck is not received
α	Positive value to add to the reputation of a node where a message is correctly transmitted
β	Positive value to subtract from the reputation of a node for failing to transmit a message
γ	Positive value to subtract from the reputation of a suspected black hole attacker
ρ	Positive value to add to the reputation of a node for having sent 2HAck and 1HAck packets
Ω	Time that a node waits for the acknowledgment of a message that it has routed
$\widetilde{\Omega}$	Time that a node waits for 2HAck packet coming from its two-hop successor
$\widehat{\Omega}$	Time that a node waits for 1HAck packet coming from its successor
Θ_0	Initial reputation value of the network nodes
$\Theta_{\mathsf{i}}(\mathsf{j})$	Returns the reputation value of the node j in the i's eye
$\widehat{\Theta}_{\mathsf{i}}(\mathsf{j})$	Last reputation value being diffused by the node i about the node j
$\widetilde{\Theta}_{\mathsf{k}}(\mathsf{i},\mathsf{j})$	Executed by k, and returns 1 if the reputation of j is more than i, and returns 0 otherwise
φ	Factor that one gives to the reputation that it was have been previously calculated
$\Delta\Theta$	Shift threshold time that a node waits before diffusing the new reputation of a node
$\overline{\Theta}$	Threshold from which a node will be considered as a black hole attacker
η	Node accusation rate
Blackhole_Alert	Packet to send by a node to the source alerting a black hole attacker
Previous_Alert	2HAck and 1HAck packets

where n_1 and $n_{|P|}$ represent respectively S and D. During the transfer process, each intermediate node i waits for the destination acknowledgment during the time Ω. When the acknowledgment arrives, each intermediate node i increases the reputation of its successor nodes in the routing path such as

$$\Theta_i(j) = \Theta_i(j) + \alpha \tag{3}$$

for $j = i + 1, \cdots, |P| - 1$, and

$$\Theta_i(D) = \Theta_i(D) + \rho \tag{4}$$

for the destination node D.

After that, if the acknowledgment is not received, each node $i+2$ involved in the message transfer sends the packet 2HAck to the node i. Upon receiving, the node i increases the node $i+1$'s reputation such as

$$\Theta_i(i+1) = \Theta_i(i+1) + \alpha, \tag{5}$$

and the node $i+2$'s reputation such as

$$\Theta_i(i+2) = \Theta_i(i+2) + \rho. \tag{6}$$

When a node $i+1$ observes during the time $\widetilde{\Omega}$ that the node $i+2$ does not send the 2HAck packet to the node i, it decreases its reputation such as

$$\Theta_{i+1}(i+2) = \Theta_{i+1}(i+2) - \beta, \tag{7}$$

and sends the packet 1HAck to the node i. After that, if the packet 1HAck is received by the node i, then the latter node increases the node $i+1$'s reputation by ρ, and decreases the node $i+2$'s reputation such as

$$\Theta_i(i+2) = \Theta_i(i+2) - \beta \cdot \Big(1 - \Theta_i(i+2)\Big) - \gamma \cdot \widetilde{\Theta}_i(i+2, i+1). \tag{8}$$

If the node i does not receive the packet 1HAck during the time $\widehat{\Omega}$, then it punishes the node $i+1$ such as

$$\Theta_i(i+1) = \Theta_i(i+1) - \beta \cdot \Big(1 - \Theta_i(i+1)\Big) - \gamma \cdot \widetilde{\Theta}_i(i+1, i). \tag{9}$$

In this situation, the node k ($k = i+1$ or $k = i+2$) will be considered responsible for the message transmission failure, and the node i alerts the source node S through a Blackhole_Alert packet. This packet contains its identity and the identity of the accused node. All the nodes

in the path, upon receiving the alert, reduce the node k's reputation by β, and increase the reputation of the other intermediate nodes by α. Nevertheless, in certain situations, the Blackhole_Alert packets are not taken into consideration. A Blackhole_Alert packet is considered as false alert when the alerter has not acknowledged the last 1HAck and 2HAck packets.

If the reputation of a node passes below the threshold $\overline{\Theta}$ and if one receives a certain number of accusations for a given node during a certain time, then this node will be suspected as black hole attacker. This operation speeds up the detection process of the black hole nodes. Indeed, a high rate of η would reduce the false accusations to be generated by defamation from the black hole nodes. A smaller rate of η ensures that the black hole nodes detection is faster, but unfortunately, the false positive rate could considerably grow if the black hole nodes start diffusing false accusations.

At each time a node receives a packet from its neighbor, it checks the node chain getting to the message before arriving to it, and increases their reputations by α for $j = 1, \cdots, i-1$. In order to detect more quickly the black hole nodes, it is necessary that the network nodes collaborate together by exchanging their knowledges about the behavior of the other nodes. To avoid encumbering the network by the messages superfluous, a node i transmits the reputation values of a node j if it changes by the threshold $\Delta\Theta$, i.e., if $|\Theta_i(j) - \widehat{\Theta}_i(j)| > \Delta\Theta$. A smaller value of the threshold will make the cooperation stronger and therefore more effective. However, it will increase the network load and will be a waste of the nodes energy. Similarly, having a large value of the threshold value will reduce the network load and will decrease the nodes cooperation, making the black hole attack detection slower.

When receiving the reputation value of a node, one calculates the new reputation for this node by taking into account this value and the owned one. To avoid distorting of nodes reputation, it takes into consideration a low impact factor received values. The calculation of the new reputation value by taking into account the received values is done such as

$$\Theta_i(j) = \frac{\varphi \cdot \Theta_i(j) + \sum_{l=1}^{N} \Theta_l(j)}{\varphi + N}, \tag{10}$$

where N represents the number of received values.

The reputation is directly related to the cooperative behavior of nodes. If the reputation of a node passes below $\overline{\Theta}$, then it will be classified as black hole attacker. However, if the reputation value is high, then the node is considered as a trusted node. The cooperative behavior allows the network nodes to increase their reputation values. Algorithm 1 and 2 present the detailed operations of the proposed approach. The asymptotic time complexity of these algorithms are of order $O(n)$ and $O(1)$, respectively.

4.3. Cooperative black hole attack

Let's consider $\{n_1, n_2, \cdots, n_{|P|}\}$ be the path P intermediate nodes set from a source to a destination node. A node n_i, $i = 2, \cdots, |P| - 1$, leads to a successful cooperative black hole

Algorithm 1 Routing process under the proposed approach

Establish a routing path $\mathsf{P} = \langle n_1, n_2, \cdots, n_{|\mathsf{P}|} \rangle$;
Send a message over P;
Upon receiving the message by the node i:
for $j = 1$ to $i - 1$ **do**
  $\Theta_i(j) \leftarrow \Theta_i(j) + \alpha$;
end for
if the message reaches $n_{|\mathsf{P}|}$ **then**
  Send an acknowledgment;
  else
  Save the message's ID and P in PostTable;
  Wait for an acknowledgment during Ω;
  if the acknowledgment is received **then**
    for $j = i + 1$ to $|\mathsf{P}| - 1$ **do**
      $\Theta_i(j) \leftarrow \Theta_i(j) + \alpha$;
    end for
    $\Theta_i(d) \leftarrow \Theta_i(d) + \rho$;
    Remove the line corresponding to the message's ID from PostTable;
    else
    Each node of P sends the 2HAck packet to its two-hop predecessor;
    Wait for 2HAck during $\widetilde{\Omega}$;
    if 2HAck received **then**
      $\Theta_i(i+1) \leftarrow \Theta_i(i+1) + \alpha$;
      $\Theta_i(i+2) \leftarrow \Theta_i(i+2) + \rho$;
      else
      $\Theta_i(i+1) \leftarrow \Theta_i(i+1) - \beta$;
      n_{i+1} sends the 1HAck packet to n_i;
    end if
    Wait for 1HAck during $\widehat{\Omega}$;
    if 1HAck received **then**
      $\Theta_i(i+1) \leftarrow \Theta_i(i+1) + \rho$;
      $\Theta_i(i+2) \leftarrow \Theta_i(i+2) - \beta \cdot (1 - \Theta_i(i+2)) - \gamma \cdot \widetilde{\Theta}_i(i+2, i+1)$;
      Send the Blackhole_Alert packet containing the node $i+2$'s ID to n_1
      else
      $\Theta_i(i+1) \leftarrow \Theta_i(i+1) - \beta \cdot (1 - \Theta_i(i+1)) - \gamma \cdot \widetilde{\Theta}_i(i+1, i)$;
      Send the Blackhole_Alert packet containing the node $i+1$'s to n_1;
    end if
    if n_i receives the Blackhole_Alert packet **then**
      if n_i has not received the Previous_Alert packet **then**
        Drop the Blackhole_Alert packet;
      end if
      else
      Accept the Blackhole_Alert packet;
    end if
    if n_1 receives the Blackhole_Alert packet **then**
      Extract the suspected node k'ID;
      for $j = 1$ to $k - 1$ **do**
        $\Theta_i(j) \leftarrow \Theta_i(j) + \alpha$;
      end for
      $\Theta_i(k) \leftarrow \Theta_i(k) - \beta$;
    end if
  end if
end if
end if

Algorithm 2 Reputation diffusion process

if $|\Theta_i(j) - \widehat{\Theta}_i(j)| > \Delta\Theta$ **then**
  Broadcast $\Theta_i(j)$;
  $\widehat{\Theta}_i(j) \leftarrow \Theta_i(j)$;
end if

attack if all the nodes n_j, $i < j < |P|$, cooperate with it. Following the proposed approach, a cooperative black hole attack cannot be conducted without being detected. We proceed by recurrence to prove this supposition. We consider the predicate $\mathsf{Blackhole\_Attack}(i) = 0$, for $i = 2, \cdots, |P| - 1$, if an acknowledgment is received, and $\mathsf{Blackhole\_Attack}(i) = 1$ otherwise. By induction, we suppose $\mathsf{Blackhole\_Attack}(i) = 0$ for $i = 2, \cdots, |P| - 1$. We consider the worst case in which the black hole node $n_i \in \{n_2, \cdots, n_{|P|}\}$. In case of one or two nodes, the launching of cooperative black hole attack is impossible. In case of three nodes, namely n_1, n_2 and n_3, the cooperative black hole attack occurs when n_2 and n_3 cooperate. This means that n_2 can send an acknowledgment message to n_1 instead of n_3. The nodes n_2 and n_3 cooperate for launching a successful black hole attack (i.e., n_3 discloses its private key to n_2) means that $\mathsf{Blackhole\_Attack}(2) = 1$ and an acknowledgment is received. This is impossible because the black hole node n_2 cannot acknowledge the messages instead of the destination node n_3. By assumption, n_1 (source node) and n_3 (destination node) are in confidence to each other and the public key certification service is set for encrypting the circulating messages in the network. Moreover, each node maintains in $\mathsf{PostTable}$, the messages identifier that it transmits, and the path that it footprints. The network nodes collaborate together by exchanging their knowledges about the behavior of the other nodes. Hence, the reputation is directly related to the cooperative behavior of nodes. If the reputation of a node passes below the threshold, then it will be classified as black hole attacker. However, if the reputation value is high, then the node is considered as a trusted node. Therefore, $\mathsf{Blackhole\_Attack}(2) = 0$.

In case of $i = |P| - 1$, the cooperative black hole attack occurs when n_i and n_j cooperate, such as $i = 2, \cdots, |P|$. This means that n_i acknowledges the received message from n_1 instead of n_j. The node n_i and n_j cooperate for launching a successful black hole attack means that $\mathsf{Blackhole\_Attack}(i) = 1$ and an acknowledgment is received. Again, this is impossible for the same reasons in case of three nodes. Consequently, $\mathsf{Blackhole\_Attack}(i) = 0$ for $i = 2, \cdots, |P| - 1$, i.e., the cooperative black hole attack cannot be launched.

5. Simulation results

In this section, we present the simulation parameters, the metrics of evaluation and the obtained results.

5.1. Simulation parameters

We have developed the simulations using Java programming language. In our simulator, the mobile nodes are considered as any equipment can communicate and send signals. We have simulated an ad hoc network including 20 mobile nodes in which the black hole nodes are randomly designated with a percentage ranging from 0 to 40% in steps 5%. The black hole nodes drop packets going through them in random manner and their positions depend to the random way point mobility model. The evaluation is made about both simple and cooperative black hole attacks. The nodes move randomly according to random way point model, i.e., a node randomly chooses a destination position and a moving speed. Once arrived at the chosen destination, it marks a random pause time and restarts the same process again. We set the maximum speed of a node with 15m/s and the maximum pause time with 3s. Network nodes move on a surface of $1km^2$ and have the same communication range, which is equal to 150m. Message sending follows a Poisson distribution with $\lambda = 10$ and the simulation duration is 500 seconds. We repeat the execution 20 times for each increase of the black hole nodes rate in the network.

TrustTable of each node is initialized with a reputation $\Theta_0 = 0.75$ and the $\overline{\Theta} = 0.25$. We reward a node with $\alpha = 0.1$, $\rho = 0.05$ and we punish it with $\beta = 0.15$. The additional value is subtracted from node seems the most probably black hole is $\gamma = 0.05$ and the shift threshold is $\Delta\Theta = 0.2$. The accused node rate to be considered black hole is $\eta = 5\%$. We have assumed that the network is reliable, i.e., a sent packet is a received packet, in which there is no loss due to the collisions or any other problems except the malicious behavior. In order to avoid encumbering the network in the messages superfluous, the values to add or to subtract must be studied well depending on the shift threshold that we must wait before diffusing a new reputation of node $\Delta\Theta$. In Table 5, we summarize the simulation parameters.

5.2. Metrics of evaluation

In order to evaluate the efficiency and performance of the proposed approach, we have considered three important metrics, namely the overhead, packet delivery rate and the detection rate. The overhead: indicates the traffic quantity generated. The packet delivery rate is the total number of received packets to the total number of the generated ones. It describes the effectiveness of the protocol enjoys in forwarding the data packets from their sources to their destinations. The detection rate is the number of the detected dropped packets to the number of all the dropped ones. A detected dropped packet means a packet which have been dropped by a black hole node, and detected by the source node. The congestion rate is the number of lost packets to the total transmitted ones. The false positive is calculated as a total number of good performing nodes which are detected as malicious regarding the total number of the honest nodes. The false negative is calculated as a total number of undetected malicious nodes regarding the total number of malicious nodes. These metrics describe the detection efficiency.

Table 5: Simulation parameters

Parameter	**Value**
Number of nodes	20
Rate of black hole nodes	0–40% (step 5%)
Mobility model	Random way point
Maximal speed	15m/s
Maximal pause time	3s
Nominal range	150m
Surface	$1km^2$
Time of simulation	500s
Θ_0	0.75
$\overline{\Theta}$	0.25
α	0.1
β	0.15
γ	0.05
ρ	0.05
$\Delta\Theta$	0.2
η	5

We compare the proposed approach to the Merkle tree approach proposed in [13]. We have considered the two versions of this approach, namely the Merkle tree under AODV and the Merkle tree under OLSR. In this protocol, all the intermediate nodes need to acknowledge the reception of packets. Using acknowledgments, the source node constructs a Merkle tree and compares the value of the tree root with a pre-calculated one. If both values are equal then the end-to-end path is secure against the packet droppers. As comparison metrics, we measured the overhead, the packet delivery rate, the detection rate and the congestion rate.

5.3. Obtained results and discussions

Figure 3 plots the size of TrustTable and PostTable per node in function of the network size. For instance, with a network size of 1000 nodes, we notice that the maximum storage requirement for TrustTable is about 6 KBytes, and for PostTable is about 125 KBytes for 100 messages sent simultaneously. Therefore, we note that our approach presents no constraints in terms of storage capacity requirements.

Figure 4 plots the overhead of the proposed approach with comparison to the Merkle tree approach in both cases OLSR and AODV in function of time. At the beginning of simulation, the overhead starts rising constantly. During this process, the proposed approach generates the control packets, such as 2HAck and 1HAck, until the black hole nodes are detected. As result, the overhead begins turning less important in the time. By comparison, the overhead generated by the proposed approach is less important than the other approaches. Indeed, the proposed approach is quite faster in black hole detection, hence generating less messages. The proposed approach generates one Ack packet for a $\mathfrak{m}$ hop path in absence of attacks, and a

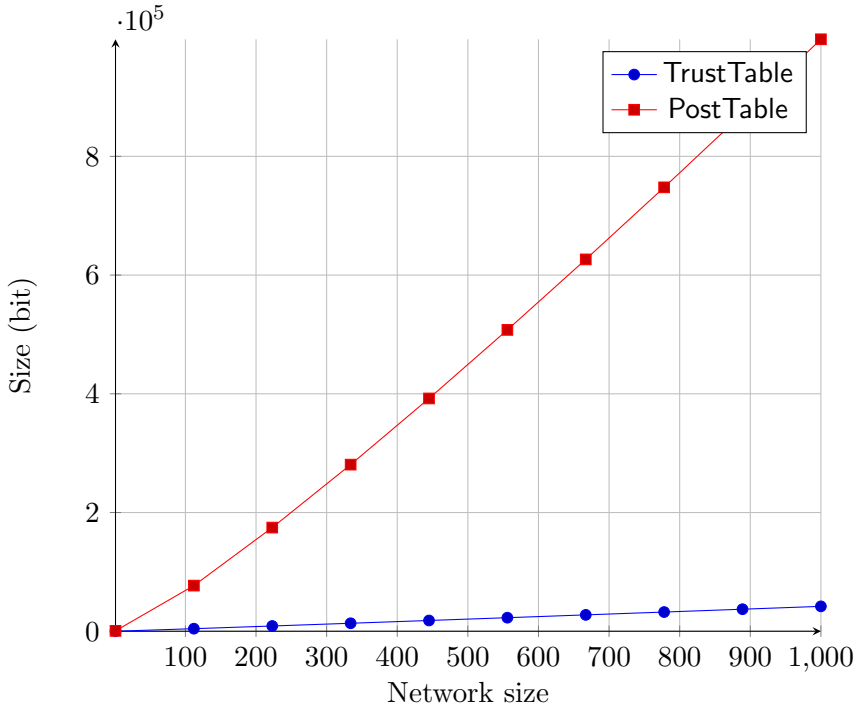

Figure 3: Size of TrustTable and PostTable for N = 100

$\mathfrak{m} - 1$ Ack packets in case of attacks. However, the Merkle tree approach generates $\mathfrak{m}$ Ack packets in both cases.

Figure 5 plots the packet delivery rate in function of time. The packet delivery rate is approximatively 100% due to the success forwarding of the generated packets, i.e, the total received packet number is approximatively the same to the generated ones. By comparison, we notice that the packet delivery rate is almost similar for both approaches despite that the overhead level of the proposed approach is less important than the Merkle tree approach.

Figure 6 plots the detection rate in function of time. The packet detection rate is approximatively 100%. This is interpreted by the dropped packets detection. We can see, the packet detection rate is almost similar for both approaches despite that the overhead in the proposed approach is less important than in the Merkle tree approach.

Figure 7 plots the congestion rate in function of time. The congestion rate is approximatively less than 2%. This is interpreted by the black hole nodes detection, in which the source avoids the suspected nodes when forwarding the packets using another trusted alternative route. We notice that the congestion rate is almost similar for both approaches despite that the overhead in the proposed approach is less important than in the case of Merkle tree approach.

Figure 8 plots the false positive and negative in function of the black hole nodes rate in the network. The obtained results are the average of the false positives and negatives at every

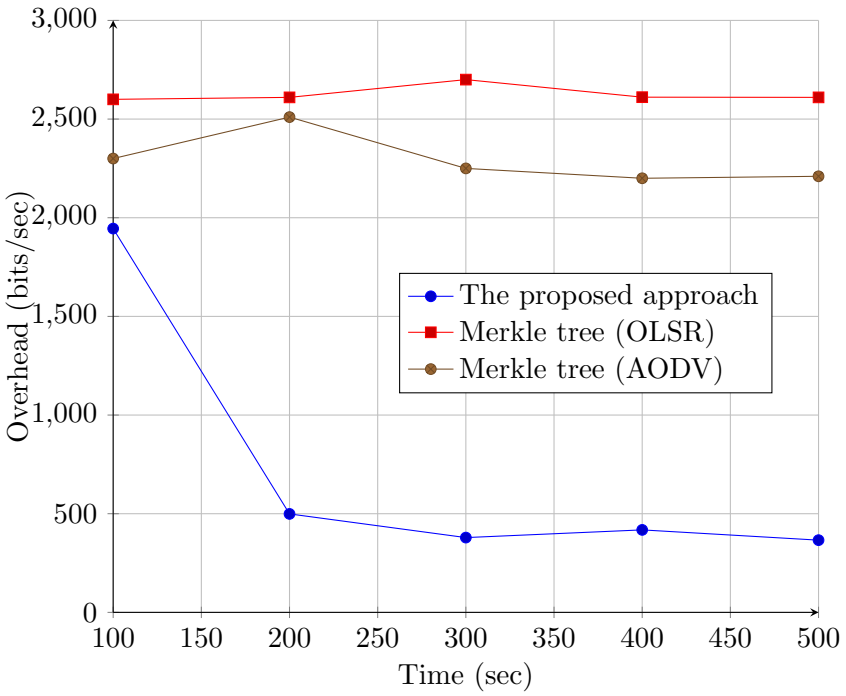

Figure 4: Overhead

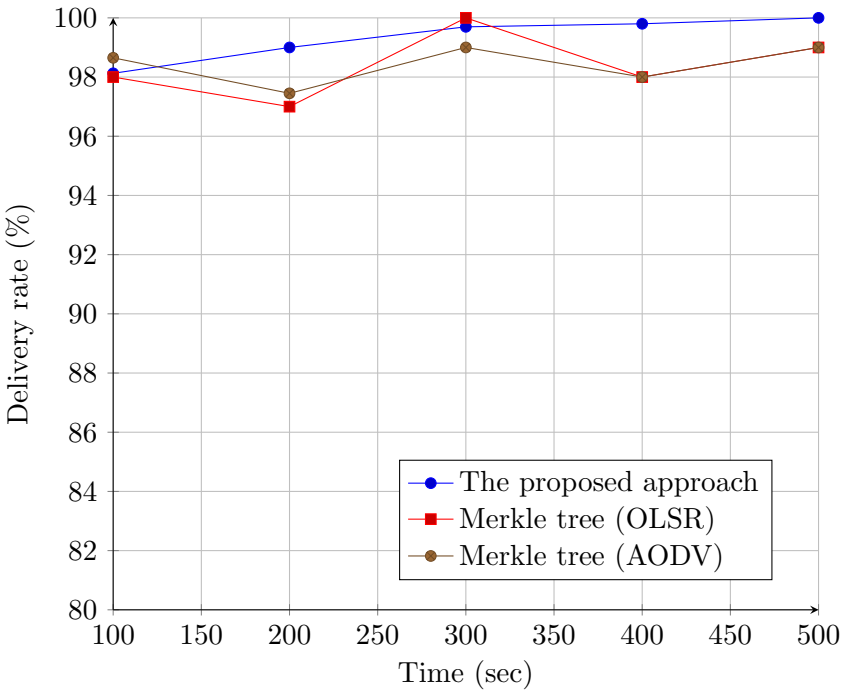

Figure 5: Packet delivery rate

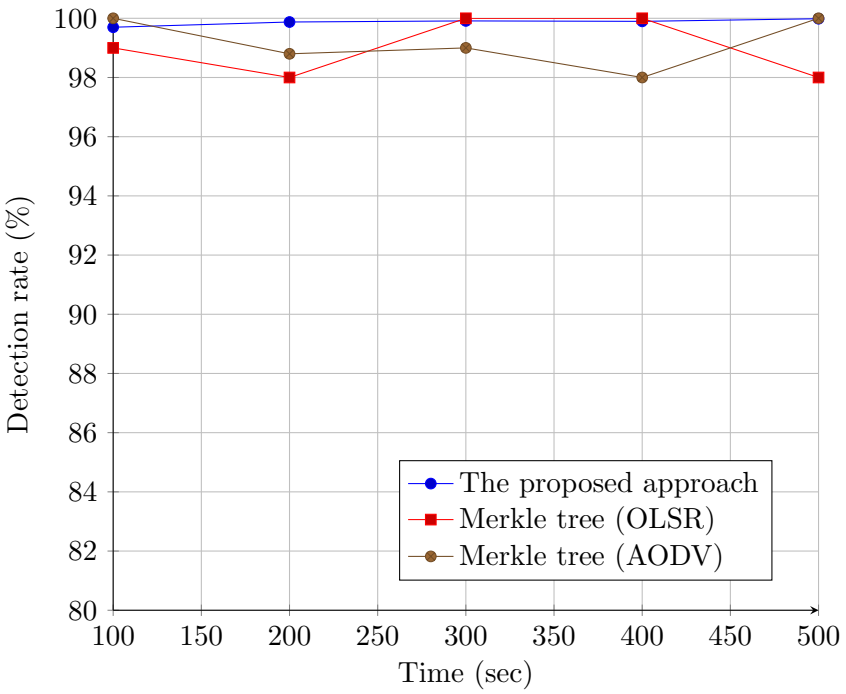

Figure 6: Detection rate

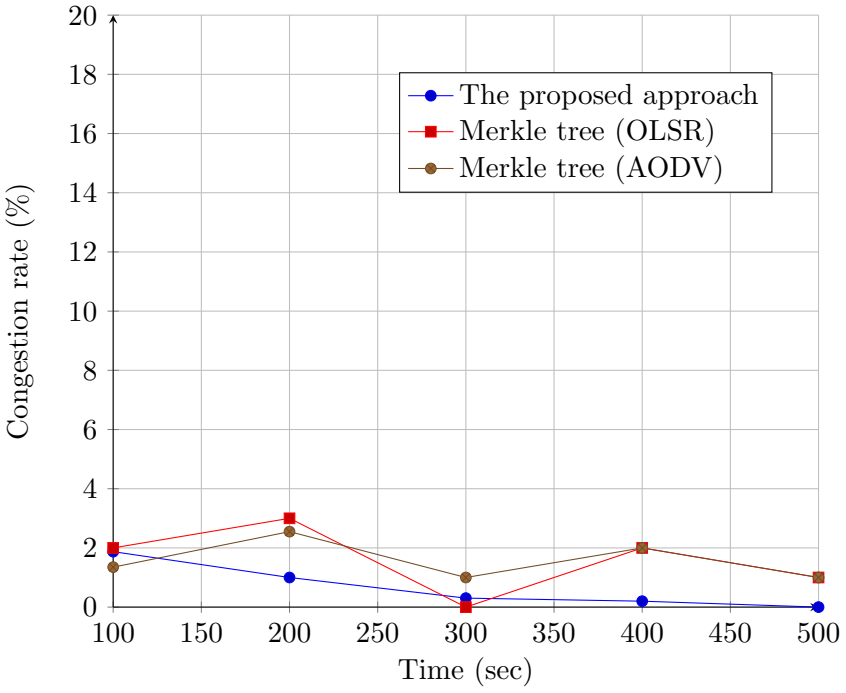

Figure 7: Congestion rate

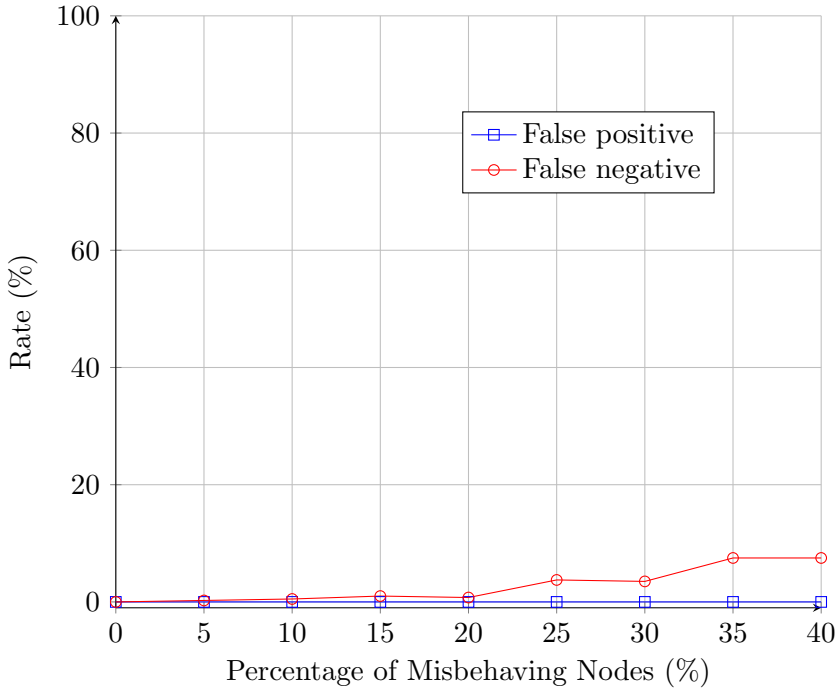

Figure 8: False positive and negative

5%. Regarding the false positive, we notice that the curve is regular and fixed at 0%, i.e., no node is accused wrongly, which confirmes the effectiveness of the proposed approach. This is due to the mechanism of declaration of black hole nodes. We have fixed a rate of 5% of the nodes which must acknowledge a given node, so that the latter is declared as a black hole attacker. Regarding the false negative, we notice that the curve does not exceed 7.5% when the rate of black hole nodes in the network increases, i.e., almost all the black hole nodes in the network have been detected. If the reputation of a node passes below the threshold, then this node will be detected as black hole attacker. The obtained results illustrated in Figure 9 confirm the accuracy of the proposed approach, where the sent and received traffic are approximately close.

Figure 10 plots the average of the reputation values in function of time and number of nodes in the network. The obtained results are the average of the reputation values of each node every 10s. In the figure, we present a reputation variation sampling of 10 nodes. We notice that the reputation values change every time because of the control packets exchanging in the system, namely ACK, 1HAck, 2HAck, and Blackhole_Alert. We notice that the nodes n_3, n_4, n_7 and n_9 are black hole nodes because their reputation values do not exceed 0.25. Regarding the other nodes, their reputation values change. If the 2HAck is not received, the reputation of this node will be penalized. Otherwise, all the nodes that are involved in the end-to-end routing path will be rewarded. Furthermore, we notice that the reputation values

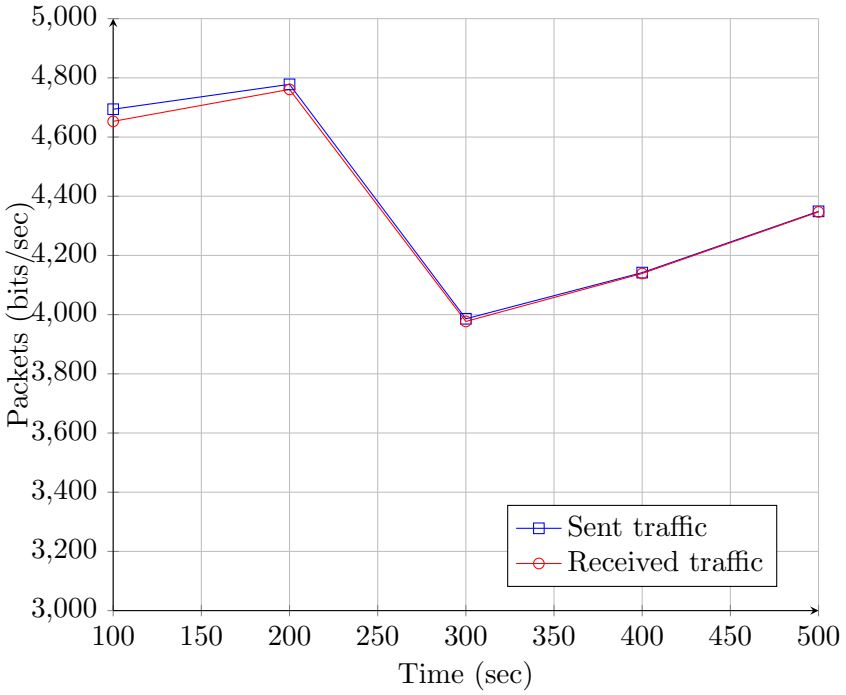

Figure 9: Accuracy of the proposed approach

vary in the same period and in every packet sending. However, the node is considered trusted.

6. Conclusion

Mobile ad-hoc network is a collection of nodes that are dynamically and arbitrarily located in such a manner that the interconnections among nodes are capable of changing on continual basis. Due to the vulnerabilities of the routing protocols, this kind of networks is unprotected against attacks. Against the black hole attack, we have proposed an efficient approach to deal with simple and cooperative forms. The proposed solution is able to detect, exclude black hole nodes and enforcing the cooperation among the network nodes. The simulations clearly demonstrate its advantages. Compared to the Merkle tree AODV and the Merkle tree OLSR, we note that the delivery and the detection rates of packets are almost similar for the compared approaches despite that the results are very interesting in terms of communication overhead in favor of the proposed approach.

Acknowledgments

This work was carried out in the framework of research activities of the laboratory LIMED, which is affiliated to the Faculty of Exact Sciences of the University of Bejaia.

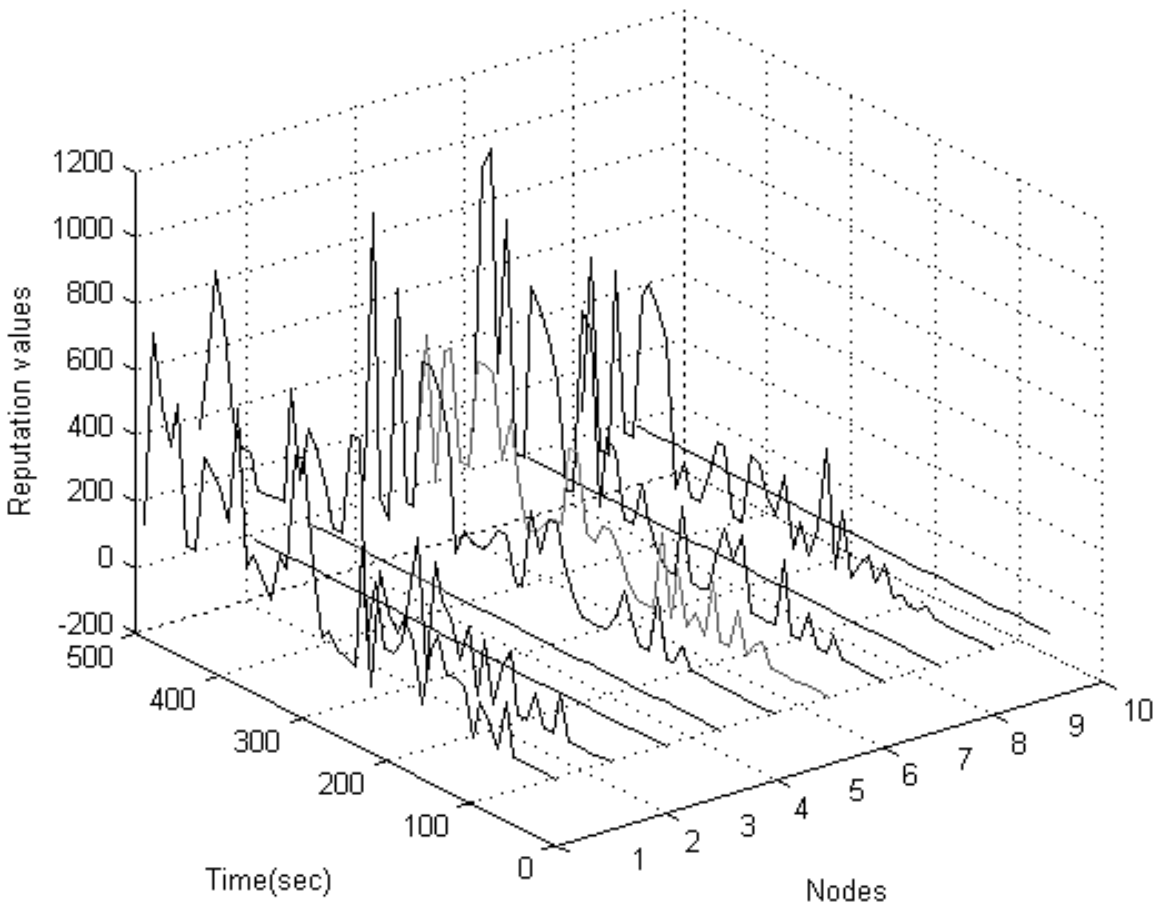

Figure 10: Average of the reputation values

7. Bibliography

[1] Sharmaa, B., Bhatiab, R-S., & Singhb, A-K. (2017). A logical structure based fault tolerant approach to handle leader election in mobile ad hoc networks. Journal of King Saud University – Computer and Information Sciences, 29(3), 378–398

[2] Omar, M., Boufaghes, H., Mammeri, L., Taalba, A., & Tari, A. (2016). Secure and reliable certificate chains recovery protocol for mobile ad hoc networks. Journal of Network and Computer Applications, 62, 153–162

[3] Khamayseh, Y., Bader, A., Mardini, W., & Baniyasein, M. (2011). A new protocol for detecting black hole nodes in ad hoc networks. International Journal of Communication Networks and Information Security, 3(1), 36–47

[4] Biswas, K., & Ali, M-L. (2007). Security threats in mobile ad hoc network. Department of Interaction and System Design School of Engineering

[5] Pegueno, G-A., & Rivera, J-R. (2006). Extension to MAC 802.11 for performance improvement in MANET. Sweden: Karlstads University

[6] Deng, H., Li, W., & Agrawal, D-P. (2002). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40(10), 70–75

[7] Shivaramu, K-N., Prasobh, P-S., & Poti, N. (2016). Security Issues in Mobile Ad Hoc Networks. Procedia Computer Science, 92, 329–335

[8] Shivaramu, K-N., Prasobh, P-S., & Poti, N. (2016). A Survey on Security Vulnerabilities in Wireless Ad Hoc High Performance Clusters. Procedia Technology, 25, 489–496

[9] Pietro, R-D., Guarino, S., Verde, N-V., & Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks: A survey. Computer Communications, 51, 1–20

[10] Marti, S., Giuli, T-J., Kevin, L., & Mary, B. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp. 255–265, 2000

[11] Djenouri, D., & Badache, N. (2006). Cross-layer approach to detect data packet droppers in mobile ad-hoc networks. In Proceedings of IWSOS/EuroNGI, pp. 163–176, 2006

[12] Djenouri, D., & Badache, N. (2008). Struggling against selfishness and black hole attacks in MANETs. Wireless Communications and Mobile Computing, 8(6), 689–704

[13] Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. Journal of Network and Computer Applications, 35(3), 1130–1139

[14] Tamilselvan, L., & Sankaranarayanan, V. (2007). Prevention of black hole attack in MANETs. In Proceedings of the International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 27–30, 2007

[15] Gurung, S., & Chauhan, S. (2017). A dynamic threshold based approach for mitigating black-hole attack in MANET. Wireless Networks, DOI: https://doi.org/10.1007/s1127

[16] Sathish, M., Arumugam, K., Neelavathy, P., & Harikrishnan, V-S. (2016). Detection of Single and Collaborative Black Hole Attack in MANET. IEEE WiSPNET 2016 conference

[17] Alem, Y-F., & Xuan, Z-C. (2010). Preventing black hole attack in mobile ad-hoc networks using anomaly detection. In Proceedings of the International Conference on Future Computer and Communication, pp. 672–676, 2010

[18] Su, M-Y., Chiang, K-L., & Liao, W-C. (2010). Mitigation of black-hole nodes in mobile ad hoc networks. In Proceedings of the International Symposium on Parallel and Distributed Processing with Applications, pp. 162–167, 2010

[19] Michiardi, P., & Molva, R. (2002). CORE : A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security : Advanced Communications and Multimedia Security, pp.107–121, 2002

[20] Buchegger, S., & Le-Boudec, J-Y. (2005). Self-policing mobile ad hoc networks by reputation systems. IEEE Communications Magazine, 43(7), 101–107

[21] Li, J-S., & Lee, C-T. (2006). Improve routing trust with promiscuous listening routing security algorithm in mobile ad hoc networks. Computer Communications, 29(8), 1121–1132

[22] Sreedhar, C., Verma, S-M., & Kasiviswanath, N. (2010). A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols. International Journal on Computer Science and Engineering, 2(2), 224–232

[23] Zaouche, L., Ait-Arab, S., Khireddine, A., Omar, M., Natalizio, E., & Bouabdallah, A. (2014). A reputation-based approach using collaborative indictment/exculpation for detecting and isolating selfish nodes in MANETs. In Proceedings of the International Conference of Networking, Distributed Systems and Applications

[24] Dorri, A. (2017). An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Wireless Networks, Vol. 23, No. 6, pp. 1767–1778

[25] Khan,S., Usman, F., Matiullah, & Khan Khalil, F. (2018). Enhanced Detection and Elimination Mechanism from Cooperative Black Hole Threats in MANETs, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3

[26] Panda, N. & Pattanayak, B. K. (2018). Energy aware detection and prevention of Black Hole attack in Manet. International Journal of Engineering & Technology, 7 (2.6), 135–140