RIST

Information Processing at the Digital Age

VOL22. N.2(2018) 11-19

Acknowledgment-based Approach for Coping with Node Misbehavior in Mobile Ad hoc Network

Mahdi Bounouni[a,b], Louiza Bouallouche-Medjkoune[b], Elhadi Choulak[b], Mehdi Chiker[b]*

[a] *Faculty of Law and Political Sciences, Univeversity of Setif2, Algeria,*
[b]*LaMOS Research Unit, Faculty of exact sciences, University of Bejaia, Algeria.*

submitted 03/01/2019,accepted 09/03/2019

Abstract

Abstract—A mobile ad hoc network (MANET) is a collection of nodes that are able to communicate without the help of a pre-existing infrastructure or a centralized administration. Several routing protocols have been proposed to ensure communication between nodes based on the assumption that all nodes are willing to cooperate to forward data packets from a source node to a destination node. However, such cooperation cannot be guaran-teed because some nodes may behave maliciously by dropping packets destined to be forwarded. To cope with the malicious behavior of nodes, we have proposed an acknowledgment-based approach called IAACK (Improved AACK). IAACK approach is organized around three components. The monitoring component is responsible for monitoring the correct forwarding of data packets in order to detect eventual dropping activities of nodes. The reputation component evaluates the nodes trustworthiness by computing the nodes reputation instead of the links reputation. Nodes are classified into different cooperation category according to their reputation values. Thus, the reputation value of a node is updated according to its cooperation category. The isolation component punishes nodes having the reputation values smaller than the reputation threshold. The simulation results demonstrate that our approach IAACK improves the throughput and reduces the dropping ratio of malicious nodes.

Key_words:MANET, Malicious nodes, Reputation, Security, Network simulator.

* Corresponding author.
E-mail address: bounouni@gmail.com.

1. Introduction

A mobile ad hoc network (MANET: Mobile Ad hoc Net-work) is a collection of wireless nodes that can communicate between them without relying on a centralized administration or an existing infrastructure. In a mobile ad hoc network, a node can communicate directly with any node if it is located in its transmission range. On the other hand, the communication with a node located outside of its transmission range is based on the cooperation of the intermediate nodes (multi-hop communication). Several routing protocols have been proposed to establish communication between nodes. Most of these protocols rely on the assumption that all nodes are willing to cooperate. The cooperation in a routing protocol means that a node forwards correctly all packets destined to be routed. However, such cooperation cannot be ensured due to the specific characteristics of this networks, such the lack of a central authority and the limited resources of the nodes. Nevertheless, a node may refuse to cooperate with others [1], [2]. It can drop all packets destined to be routed, either to malfunction forwarding packets activity (malicious behavior) or to preserve its resources (selfish behavior).

In order to counteract the malicious behavior of nodes, the reputation approaches have been proposed to punish nodes refusing to relay packets. A node computes the reputation values of its neighbors by monitoring their behavior in the data forwarding process. Based on the monitoring technique used, we can classify reputation approaches into two categories: promiscuous-based approaches [3]–[10] and acknowledgment-based approaches [11]–[14]. The basic idea of the promiscuous-based approaches consists on overhearing the transmission of neighboring nodes in order to check if they forward packet recently sent. Although these approaches can identify malicious nodes, they have several limitations [3] such receiver collision and Insufficient transmission power. To ad-dress these limitations, the acknowledgment-based approaches have been proposed. To monitor the behavior of neighboring nodes, these approaches rely on the transmission of new type of acknowledgment packet to verify whether the packet recently sent is forwarded. In comparison to promiscuous-based approaches, the acknowledgment-based approaches en-able nodes to identify only malicious links instead of malicious nodes.

Although acknowledgment-based approaches can address several limitations of promiscuous-based approaches, they suffer from several limitations that can influence their performance. These approaches can identify only malicious links instead of malicious nodes. This limitation gives for malicious nodes more opportunities to drop a lot of data packets by involving themselves in multiple forwarding routes. This limitation may be exploited by malicious nodes by two different behaviors:

- A malicious node can launch Black Hole attack by sending a fake RREP to force the source to route the packets through it. All packets passing through this route will be dropped. Since these approaches permit to detect only malicious links, the same malicious node may launch a multiple black hole attack without any punishment. Thus, even a malicious node is involved in a multiple malicious links, its packets are always forwarded by cooperative node which results an injustice towards nodes behaving well.
- An Ad hoc mobile network is a dynamic network, which means that the network topology changes frequently. A change of topology means that there is a change in the neighborhood of each node. Since these approaches only detect malicious links, each new neighbor of a malicious node constitutes a new chance to create a malicious link, and therefore, drop more data packets.

In order to deal with the above limitations, we have proposed an acknowledgment-based approach called

IAACK (Improved IAACK). The proposed approach aims to detect and punish malicious nodes dropping data packets. IAACK approach is an extension improvement of the AACK approach
[13]. It is structured around three components: monitoring, reputation and isolation. The monitoring component is responsible for monitoring the behavior of neighbors nodes in the data forwarding process. The reputation component computes and updates the reputation values of neighbors nodes according to their behaviors. We have proposed a new method that enables nodes to evaluate the nodes trustworthiness instead of the links trustworthiness. Thus, the isolation component permits to exclude nodes having the reputation values smaller than the reputation threshold from all networks activities.

The rest of this paper is organized as follows. In section 2, we explore briefly some related works. We introduce our proposed approach (IAACK) in section 3. In section 4, we study the performance of IAACK scheme via simulation and finally conclude the paper.

II. RELATED WORKS

Several approaches have been proposed to deal with malicious nodes refusing to relay packets. Almost of these approaches monitor the behavior of nodes in the data forwarding process, and they determine whether a node is trustworthy based on its reputation value. The reputation value is a numeric value that can be defined as the perception of a node over an-other. If a node forwards correctly a data packet, its reputation value is incremented. Otherwise, it is decremented. If a node reputation value falls below a predefined threshold, the node is considered as malicious. The reputation can be classified according to the monitoring technique employed into two categories: promiscuous-based approaches and acknowledgment-based approaches.

In the literature, the promiscuous-based approach proposed is Watchdog/Pathrater [3]. In this approach, the Watchdog and Pathrater modules were introduced with the aim of identifying malicious nodes that accept to transmit data packets but never do so. The Watchdog is used to monitor the behavior of neighboring nodes by overhearing their transmissions using the promiscuous mode. Using this mode, if a node A is within the transmission range of a neighbor B, it can overhear all the communications of its neighbor B. Each node maintains a buffer of data packets recently sent. If the overheard packet exists in the buffer, the Watchdog considers that the packet has been forwarded by neighbor. Otherwise, if the data packet is maintained in the buffer without been heard, the Watchdog.

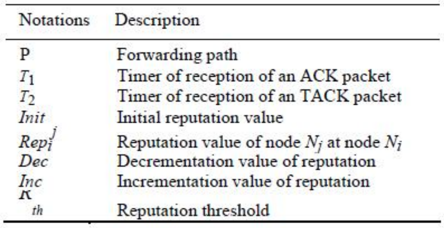
III. THE PROPOSED IAACK SCHEME

To overcome the limitations of the acknowledgment-based approaches previously described, we propose a new approach called IAACK (Improved AACK). The proposed approach is organized around three components: monitoring, reputation, isolation. The notations used in our proposed approach are described in table 1.

A. Monitoring component

This component is responsible for monitoring the behavior of neighboring nodes in data forwarding process. We employ the AACK [13] approach as monitoring technique. This approach is the result of the combinations of two modes: AACK and TACK. The AACK mode is equivalent to the end-to-end acknowledgment approach. In this mode, the destination node should return an ACK packet to the source node for each data packet received correctly.

Table1. Notations



Notations	Description
P	Forwarding path
T_1	Timer of reception of an ACK packet
T_2	Timer of reception of an TACK packet
Init	Initial reputation value
Rep_i^j	Reputation value of node N_j at node N_i
Dec	Decrementation value of reputation
Inc	Incrementation value of reputation
K_{th}	Reputation threshold

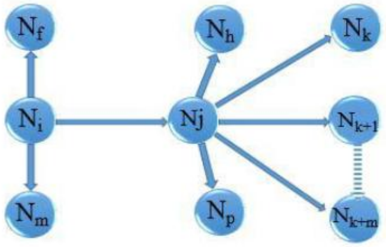


Fig1. Monitoring scenario

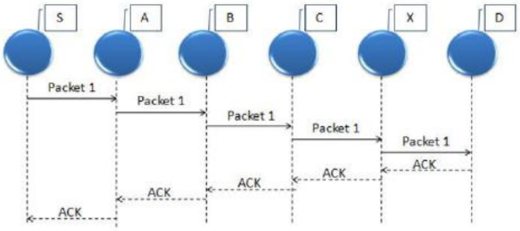


Fig. 2. AACK mode

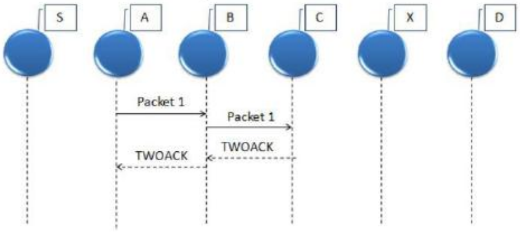


Fig. 3. TACK mode

However, if the source does not receive an ACK packet, it switches to TACK mode.

To illustrate the functioning of the monitoring process (see Fig. 1), let triplet of nodes N_i, N_j , N_k) *2 p*, where *p =fN*$_s$,
... N_i, N_j , N_k, ...N_d*g* is forwarding route, and N_s and N_d
are the source and destination nodes, respectively.

When there are data packets to be exchanged between both nodes N_s and N_d, the AACK mode is used (see Fig. 2). Then, for each data packet received, the destination node N_d should send back an ACK packet to the source node N_s. If N_s receives an ACK packet for a data packet before the expiration of the timer T_1, the monitoring process continues with ACK mode. Otherwise, if N_s has not received an ACK after T_1 has expired, N_s switches to TACK mode (see Fig. 3). In the TACK mode, the third node of the triplet N_k should returns a TACK (TWOACK) packet to the first node of the triplet N_i for each data packet received. The node N_i registers a positive event against both nodes N_j and N_k for the data packet *P acket*1 only if: the packet *P acket*1 is acknowledged by node N_k before the expiration of the timer T_2. Otherwise, if the timer T_2 is expired, the node N_i registers a negative event against both nodes n_j and N_k. For each event detected by the monitoring component, the reputation component is invoked.

B. Reputation component

The reputation component evaluates and updates the reputation values of neighboring nodes in data forwarding process. It quantifies the behavior of neighbors by a single reputation value. In comparison with existing acknowledgment-based approaches, we propose a new technique to compute the reputation values of nodes instead of forwarding links. In our approach, the reputation of a node reflects its trustworthiness in all forwarding links in which it is involved.

To illustrate the function of the reputation process, we take the Triplet of nodes ($N_i; N_j ; N_k) 2 P$ as an example, where

P is a forwarding route. Let $Rep^j{}_i$ and $Rep^k{}_i$ the reputation values of both nodes N_j and N_k as perceived by the node N_i. At start-up, the reputation value of each monitored node is initialized to *init* and it varies between 0 and *max*, where *max* 1. Following the type of event detected by the monitoring component through the link ($N_j ; N_k$), $Rep^j{}_i$ and $Rep^k{}_i$ are updated.

1) Positive event: If the monitoring component of the node N_i detects a positive event through the link ($n_j ; n_k$), the reputation values $Rep^j{}_i$ and $Rep^k{}_i$ are incremented by *Inc* as follows:

$$Rep^j_i = Rep^j_i + Inc \qquad (1)$$

$$Rep_i^k = Rep_i^k + Inc \qquad (2)$$

2) Negative event: If a negative event is detected through the link ($N_j ; N_k$) by the monitoring component of the node N_i, the reputation values $Rep^j{}_i$ and $Rep^k{}_i$ of nodes N_j and N_k) are decremented by DEC_i^j and DEC_i^k as follows:

$$Rep^j_i = Rep^j_i \quad DEC^j_i \qquad (3)$$

$$Rep_i^k = Rep_i^k \quad DEC_i^k \qquad (4)$$

In our approach, we make a distinction between incrementing and the decrementing values of the reputation. The purpose of this idea is to treat differently nodes having high reputation values and nodes having low reputation values, when they are part of the same negative event. Based on

their reputation values, nodes are classified into three cooperation categories: high cooperation, medium cooperation, less cooperation. The decrementing value DEC associated to a node depends on its cooperation category. Let a, b, and c be three constants used as a reputation decrementing values, where a < b < c. The limits in terms of reputation and the decrementing value of each cooperation category are presented in table 2 (with $R_{th} \prec$ init $\prec$ sup $\prec$ max)*:*

Table 2. Node cooperation category

Reputation value	Node cooperation category	decrementing value
[*Sup; max*]	High cooperation	a
[*init; Sup*[	Medium cooperation	b
]R_{th}; *init*[	Less cooperation	c

The rational for this idea is that: in order to achieve their goal that consists on destabilizing the data forwarding process, malicious nodes may try to involve themselves in multiple forwarding routes in order to drop a lot of data packets. This behavior causes the degradation in their reputation values because they are involved in many negative events (drop data packets). However, cooperative nodes are characterized by their high reputation values as they collect many positive events due to the correct transmission of data packets. In our approach, when a node with a high reputation value (probably cooperative) and a node with a low reputation value (probably malicious) are involved in the same negative event, they are treated according to their reputation values. The reputation value of a cooperative node is decremented with a low *DEC* value.

However, the reputation value of a low-reputed node is decremented with a high *DEC* value, which cause the degradation of its reputation value. Following this idea, we ensure equity (equality) between a cooperative node and a malicious node when they are involved in the same negative event. If the reputation value of a node is smaller than the predefined threshold R_{th}, the isolation process is invoked.

C. Isolation component

The purpose of the isolation component is to exclude malicious nodes. If the reputation of a $Rep^{j}{}_{i}$ node is smaller than the predefined threshold R_{th}, the node N_j is considered as malicious. For its isolation, the N_i node performs the following actions:

1) Informs the source node of data packet about the detected node by sending a report (similar to RERR packet).
2) Adds the detected malicious node to its black list of nodes.
3) Invalidates all forwarding routes involving the detected node.
4) Refuses to route all the RREQ initiated by this node for its punishment.

TABLE III

SIMULATION PARAMETERS

Parameter	Value
Number of node	40
Routing protocol	DSR [15]
Simulation area	670 m 670 m
Transmission range	250 m
Node speed	10 m/s and 20 m/s
Pause time	0 s
init 40	
Number of malicious nodes	2; 4; 6; 8; 10; 12
Mobility model	Random Way Point
Number of CBR	10 connections
Simulation time	600 s

Each node, including the source receiving the malicious report in the promiscuous mode or as a receiver proceeds to the same isolation process described in the previous actions.

IV. PERFORMANCE EVALUATION

Using the network simulator NS-2.34, we study the performance of the IAACK approach in comparison to the AACK approach [13] by performing series of simulation.

A. Simulation environment

We simulated 40 nodes deployed randomly over an area of 670*m* * 670m. The UDP traffic with CBR (constant bit rate) is used. The IEEE 802.11 MAC standard is used. The transmission range of each node is set to 250 m. The simulation time is fixed to 600 s. The initial reputation value assigned to a node in start-up *init* is set to 40 and it varies between 1 and 80. The rest of the simulation parameters are shown in Table 3.

The following two metrics were used to examine the performance of the IAACK approach:

Average throughput (Kbps): reflects the total size of data packets that successfully reached their destination over the simulation times.

Dropping ratio: represents the ratio of the number of data packets dropped by malicious nodes to the number of data packets sent.

B. Simulation Results

Fig. 4 plots the average throughput of the IAACK and AACK approaches as a function of the number of malicious nodes. In this case of study, the speed of the nodes is fixed to 10 m/s. We observe that the increase in the number of malicious node causes the deterioration of the average through-put of IAACK and AACK approaches. However, the average throughput of the IAACK approach is greater than the average throughput of the AACK approach. This is because IAACK approach is able to detect and isolate malicious nodes in the data forwarding process instead of malicious links compared to the AACK approach.

Fig. 5 shows the dropping ratio of the IAACK and AACK approaches as a function of the variation in the number of malicious nodes.

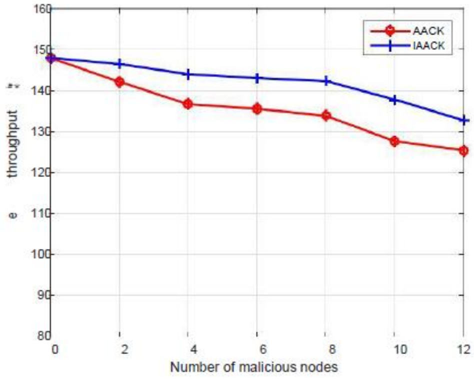


Fig. 4. Average throughput Vs Number of malicious nodes (Node Speed = 10 m/s)

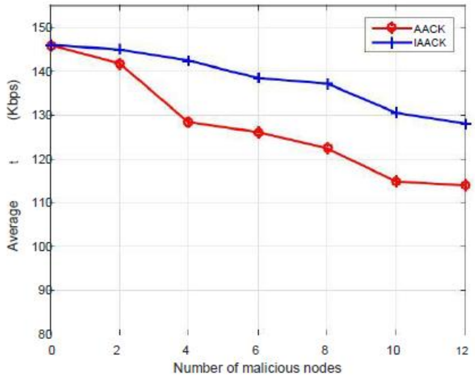


Fig. 6. Average throughput Vs Number of malicious nodes (Node Speed = 20 m/s)

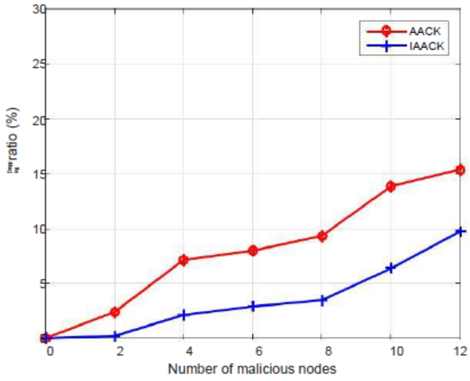


Fig. 5. Dropping ratio Vs Number of malicious nodes (Node Speed = 10 m/s)

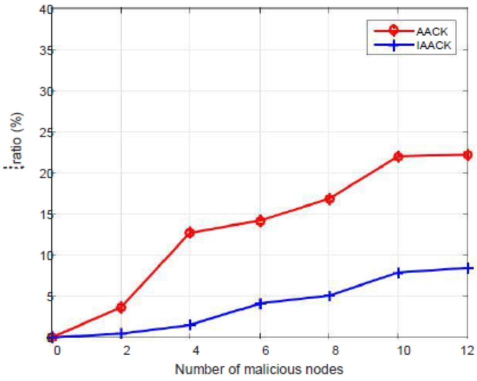


Fig. 7. Dropping ratio Vs Number of malicious nodes (Node Speed = 20 m/s)

We observe that the dropping ratio increases by increasing the number of malicious nodes. But, we can remark that the dropping ratio of the IAACK approach is significantly lower compared to the AACK approach. This can be explained by the fact that the IAACK approach detects malicious nodes and avoids to forward data packets through them. On the other hand, AACK approach is able to detect and avoid only malicious links, which gives for malicious nodes more chance to drop more data packets by involving themselves in multiple forwarding routes.

To illustrate the impact of node speed on the performance of both IAACK and AACK approaches. Fig. 6 and Fig. 7 show the average throughput and dropping ratio as function of the number of malicious nodes, respectively. The speed of nodes is fixed to 20 m/s. In accordance with the results presented in Fig. 4 and Fig. 5, the obtained results demonstrate that the IAACK approach improves the average throughput and reduces the dropping ratio compared to the AACK approach (the difference becomes more apparent when the speed of the nodes is fixed to 20 m/s). This is due to the fact that: when the nodes move quickly (high speed), their neighborhoods change (new neighbors). Since the AACK approach can exclude only malicious links, each new neighbor becomes a chance to form a malicious link, and therefore dropping more data packets. The IAACK approach is resistant to neighborhood change because it is able to avoid malicious nodes in the route discovery process.

V. Conclusion

In this paper, we have proposed IAACK, an acknowledgment-based approach which integrates three components: monitoring, reputation and isolation. IAACK approach aims to punish malicious nodes more severely in comparison to existing acknowledgment-based approaches by detecting malicious nodes instead of malicious links. To achieve this purpose, we have proposed a method to quantify the behavior of node in all forwarding links in which is involved by a single reputation value. Nodes are classified into different cooperation categories according to their reputation value. Thus, the reputation values of nodes are updated according to their cooperation categories. The simulation results obtained show that the proposed approach is able to punish malicious nodes severely which permits to improve the throughput and to reduce the dropping ratio of malicious nodes.

As perspective, we plan to thwart selective dropping attacks that occurs when malicious nodes drop data packets at low rate in order to evict to be unmasked, while at the same time to continue disrupting the forwarding activity of data packets.

References

[1] D. Djenouri and N. Badache," On eliminating packet droppers in MANET: A modular solution", Ad Hoc Networks, vol. 7, no. 6, 2009, pp. 1243-1258.

[2] M. Bounouni and L. Bouallouche-Medjkoune," A Hybrid Stimulation Approach for Coping Against the Malevolence and Selfishness in Mobile Ad hoc Network", Wireless Personal Communications, vol. 88, no. 2, 2015, pp. 255-281.

[3] S. Marti, T. J. Giuli, K. Lai, M. Baker," Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, pp. 255-265.

[4] S. Bansal, M. Baker," observation-based cooperation enforcement in ad hoc networks", arXiv preprint cs/0307012, 2003.

[5] S. Buchegger and J. Le Boudec," Performance analysis of the CONFI-DANT protocol", Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking computing, 2002, pp. 226-236.

[6] P. Michiardi, R. Molva," Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", Advanced Communications and Multimedia Security, 2002, pp. 107-121.

[7] N. Nasser and Y. Chen,” Enhanced intrusion detection system for discov-ering malicious nodes in mobile ad hoc networks”, In IEEE international conference on communications, 2007, pp. 11541159.

[8] E. Hernndez-Orallo, M. D. S. Olmos, J. C. Cano, C. T. Calafate and P. Manzoni,” A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs”, Wireless personal communications, 2014, vol. 74, no. 3, 1099-1116.

[9] Hernandez-Orallo, E., Olmos, M. D. S., Cano, J. C., Calafate, C. T., Manzoni, P,” CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes”, IEEE transactions on Mobile Computing, 2015, vol. 14, no. 6, 1162-1175.

[10] B. Jedari, F. Xia, H. Chen, S. K. Das, A. Tolba and A. M. Zafer,” A social-based watchdog system to detect selfish nodes in opportunistic mobile networks”, Future Generation Computer Systems, 2017.

[11] K. Balakrishnan, J. Deng, P. K. Varshney,” TWOACK: preventing selfishness in mobile ad hoc networks”, Wireless Communications and Networking, 2005, pp. 2137-2142.

[12] K. Liu, J. Deng, PK. Varshney and K. Balakrishnan,” An acknowledgment-based approach for the detection of routing misbehavior in MANETs”, IEEE Trans Mob Comput, pp. 536550

[13] T. Sheltami, A. Al-Roubaiey, E. Shakshuki and A. Mahmoud,” Video transmission enhancement in presence of misbehaving nodes in MANETs”, Multimedia Systems, vol. 15, no. 5, 2009, pp. 273-282.

[14] E. Shakshuki, N. Kang and T. Sheltami,” EAACKA Secure Intrusion-Detection System for MANETs”, IEEE Transactions on Industrial Elec-tronics, vol. 60, no. 3, 2013, pp. 1089-1098.

[15] D. B. Johnson, D. A. Maltz, and J. Broch,” DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks”. Ad hoc networking, vol. 5, 2001, pp. 139-172.