Hybrid Acknowledgment Punishment Scheme Based on Dempster-Shafer Theory for MANET

Mahdi Bounouni[1,2](✉) and Louiza Bouallouche-Medjkoune[1]

[1] LaMOS Research Unit, Faculty of Exact Sciences,
University of Bejaia, 06000 Bejaia, Algeria
Bounouni@gmail.com, louiza_medjkoune@yahoo.fr

[2] Faculty of Law and Political Sciences, University of Setif 2, Setif, Algeria

Abstract. In this paper, we cope with malicious nodes dropping packets to disrupt the well-functioning of mobiles ad hoc networks tasks. We propose a new hybrid acknowledgment punishment scheme based on Dempster Shafer theory, called HAPS. The proposed scheme incorporates three interactive modules. The monitor module monitors the behaviour of one-hop nodes in the data forwarding process. The reputation module assesses the direct and the indirect reputation of nodes using Dempster Shafer theory, which is a mathematical method, that can aggregate multiple recommendations shared by independent sources, while some of these recommendations might be unreliable. Since recommendations exchange between nodes consumes resources, a novel recommendation algorithm has been incorporated to deal with false dissemination attack and to minimize the recommendation traffic. The exclusion module punishes nodes regarded as malicious. The simulation results show that HAPS improves the throughput and reduces the malicious dropping ratio in comparison to existing acknowledgment scheme.

Keywords: Mobile ad hoc network · Security · Cooperation
Dempster Shafer theory · Uncertainty

1 Introduction

Mobile ad hoc network (MANET) is a collection of wireless mobile nodes that are able to perform the network tasks without requiring a fixed infrastructure or centralized administration. The communication between nodes follows a multi-hop approach. This approach depends on the assumption that all mobile nodes cooperate. Nevertheless, this assumption cannot be ensured due to the MANET features including the distributed nature, resource constraint of nodes [1]. These features make MANET vulnerable to selfish and malicious nodes. Selfish nodes

A. Amine et al. (Eds.): CIIA 2018, IFIP AICT 522, pp. 436–447, 2018.
https://doi.org/10.1007/978-3-319-89743-1_38

may refuse to relay packets for other nodes to preserve their resources. On the other hand, malicious nodes may drop all packets passing through them in order to disrupt the functioning of the network's activities. Therefore, to improve the network performance, it is critical to cope against the selfish and malicious behavior.

In the literature, one can categorize two types of related works dealing with selfish and malicious nodes dropping packets: credit-based schemes [3–7] and reputation-based schemes [2, 5, 8–10, 12, 13, 18–21, 24]. The goal of incentive-based schemes consists of encouraging nodes to relay packets for the benefits of other nodes by using credit. Node earns credits by relaying packets for other nodes and loses credits to send their packets. In the reputation-based schemes, each node monitors its one-hop nodes and computes their reputation values according to their behaviour. Almost of the reputation-based schemes use the watchdog technique [2] for the monitoring. However, this technique presents several feebleness as reported in [2, 11]. To deal with this feebleness, the acknowledgment technique is proposed in [12]. This technique permits to expand the range of neighbours monitoring to the two-hop by introducing a new kind of packet called TWOACK packet.

One of the recent scheme employing the acknowledgment technique is EAACK scheme [13]. EAACK can detect and punish malicious links. EAACK can effectively resolve some feebleness of the watchdog technique. However, EAACK is still vulnerable to other threats. (1) When nodes move faster, their neighbourhoods change often and therefore, malicious nodes have a several chances to drop more packets. Because, each new neighbour for malicious node forms a potential malicious link. This threat is inherited from TWOACK scheme [12], since TWOACK scheme can detect only malicious links and EAACK is based on TWOACK. (2) All requests initiated by malicious nodes are still relayed because the purpose is to relive malicious nodes from relaying data packets instead of punishing them.

To address the above threats, we propose a hybrid acknowledgment punishment scheme based on Dempster Shafer theory [14, 15, 23], called HAPS. HAPS scheme aims to enhance the performance of EAACK [13] by punishing malicious nodes more severely. HAPS is structured around three interactive modules: monitor, reputation, exclusion. The monitor module monitors the behavior of one-hop nodes in the data forwarding process. The reputation module computes the direct and indirect reputation values of neighbour nodes based on the information provided by the monitor module and the recommendations shared between nodes. We propose a new combination algorithm based on Demspter Shafer theory [14, 15] to compute the direct reputation value of the node. Thus, HAPS enables nodes to share their recommendations about other nodes, but only when it is necessary, and the combination of different recommendations is done based on Dempster Shafer Theory. The exclusion module punishes all nodes having reputation values smaller than the reputation threshold.

The remainder of this paper is organized as follows. In the Sect. 2, We present some preliminaries on Dempster Shafer Theory. Section 3 is devoted to the adversarial model. In Sect. 4, we present our proposed scheme (HAPS). In Sect. 5, we examine the performance of HAPS via simulation and finally conclude the paper.

2 Preliminaries on Dempster-Shafer Theory

Dempster Shafer theory of evidence [14,15] is a mathematical method, handling the uncertainty and the subjective judgment. This method is especially efficient in situation when there is a need to aggregate multiple evidences shared by independent sources while some shared evidences might be unreliable, imprecise or incomplete/ambiguous. Let $\varphi = \{A_1, .., A_n\}$ be a finite set of mutually exclusive and exhaustive hypotheses denoted as the frame of discernment, where A_i are the individual hypotheses [22]. 2^φ denotes the possible subsets (or power set) of φ. In this section, we outline some basic concepts of Dempster Shafer theory.

Definition 1 [15]**:** A basic probability assignment function (BPA) or a mass function m is a function that assigns to each subset of ϕ a quantity of belief which is a number between 0 and 1. m is defined from $2^\varphi \rightarrow [0, 1]$ and satisfying the following two constraints:

$$m(\emptyset) = 0 \; et \; \sum_{A \in \varphi} m(A) = 1 \tag{1}$$

Definition 2 [15]**:** Let $m : 2^\varphi \rightarrow [0, 1]$ be a mass function. The belief function $bel : 2^\varphi \rightarrow [0, 1]$ related to the mass function m over φ is defined as follows

$$bel(A) = \sum_{B \in A} m(B) \tag{2}$$

$bel(A)$ corresponds to the total of belief given to the hypotheses A.

Definition 3 [15]**:** Dempster's rule of combination permits to combine independent evidences issued from independent sources by applying the orthogonal sum $\bigoplus$. Given two mass functions m_1 and m_2 over the same frame of discernment φ. According to the Dempster's rule of combination, m_1 and m_2 can be combined into a new mass function $m : 2^\varphi \rightarrow [0, 1]$ as follows:

$$m(C) = m_1(A) \bigoplus m_2(B) = \frac{\sum_{A_i \cap B_j = C} m_1(A_i) m_2(B_j)}{1 - K_{12}} \tag{3}$$

Where $K_{12} = \sum_{A_i \cap B_j = \emptyset} m_1(A_i) \, m_2(B_j)$. $m(c)$ represents the mass function of the combined evidence and K_{12} reflects the amount of conflicts between m_1 and m_2.

According to the Dempster's rule of combination, we can combine n evidences as follows:

$$m_1 \bigoplus m_2 \cdots \bigoplus m_n(C) = \frac{\sum_{C_1 \cap \cdots \cap C_n = C} m_1(C_1) m_2(C_2) \ldots m_n(C_n)}{1 - K_{1 \ldots n}} \tag{4}$$

Where $K = \sum_{C_1 \cap \cdots \cap C_n = \emptyset} m_1(C_1) \, m_2(C_2) \ldots m_n(C_n) < 1$.

3 Adversarial Model

According to their purposes, nodes may behave maliciously in order to degrade the network performance. In our paper, we suppose that malicious nodes may launch: (1) Black hole attack by dropping all data packets passing through them. (2) False dissemination attack by sharing fake recommendation to falsely improve or degrade the reputation value of the malicious or honest node, respectively.

4 The Proposed HAPS Scheme

HAPS scheme is structured around three interactive modules: monitor, reputation, exclusion.

4.1 Monitor Module

This module monitors the behaviour of one-hop nodes in the data forwarding process. HAPS employ the monitoring technique proposed in the EAACK scheme [13]. EAACK scheme is the result of the combination of three modes: ACK, S-ACK and MRA. In this paper, we implement only ACK and S-ACK modes. In the ACK mode, the destination node should send back an ACK packet to the source node for every data packet received. The S-ACK mode is similar to the TWOACK scheme. In the S-ACK mode, a new kind of packet called S-ACK is used. Each node forwarding data packets should send an S-ACK packet to the two-hop node in the opposite direction of the forwarding path.

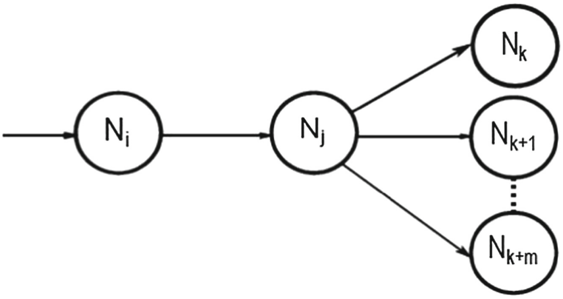

Fig. 1. Monitoring scenario

To illustrate the functioning of this technique, let $p = \{N_s, ..., N_i, N_j, N_k, ..., N_d\}$ the selected forwarding path, $<N_i, N_j, N_k> \in p$ a triplet of nodes taken as an example (see Fig. 1). $List_{ID}$ denotes the list of ID of data packets sent or forwarded waiting to be acknowledged. The source N_s sends data packets to the destination N_d through the path p. In the startup, the ACK mode is employed. In this mode, N_s adds the ID of each data packet sent D to $List_{ID}$.

Each ID is maintained for θ second. Upon reception of D at N_d, it should send back an ACK packet to N_s. For each ACK packet relayed by all nodes $N_i \in p$, the monitor module of N_i registers a good action through the link (N_j, N_k). If N_s receives an ACK packet before θ expires, which means that there are no malicious actions along the path p, it removes the ID of D from $List_{ID}$. Otherwise, N_s switches to the S-ACK mode. N_i adds the ID of each data packet forwarded D to $List_{ID}$. Each ID is maintained for ϑ second. N_j Will forward D to N_k if it behaves cooperatively. Once the packet D reaches N_k , it should send back an S-ACK packet N_i if it does not behave maliciously. If N_i receives S-ACK packet before ϑ expire, it deletes the ID of D from $List_{ID}$ and registers a good action against the link (N_j, N_k). Otherwise, if N_i does not receive S-ACK packet after ϑ expires, N_i removes the ID of D from $List_{ID}$ and registers a bad action against the link (N_j, N_k). The same process is repeated for each triplet of nodes along p. This process is repeated until N_s receives a switch packet from N_d, which means that p is a safer path. Therefore, N_s switches to the ACK mode.

4.2 Reputation Module

This module assesses and manages the reputation values of one-hop nodes. The reputation is classified into three types: direct, indirect and final. This module maintains four parameters ranging from 0 and 1: the reputation value of each monitored link $(N_j, N_k) \in FL_i^j$ denoted by $R_i\,(j,k)$ where FL_i^j denotes the set of forwarding links in which N_j is involved, The direct, indirect and final reputation values denoted by $DR_i^j(t)$, $IR_i^j(t)$ and $FR_i^j(t)$, respectively, where denotes the time of the computation of the reputation value.

Direct Reputation

A reputation is considered type direct, if it is computed based only on the recommendation of the monitor module. The reputation module of N_i evaluates the trustworthiness of N_j in all forwarding links $(N_j, N_k) \in FL_i^j$ in which is involved (see Fig. 1). If the monitor module detects a good action, $R_i\,(j,k)$ is increased. Otherwise, $R_i\,(j,k)$ is decreased. To compute the direct reputation value $DR_i^j(t)$ of N_j at time slot t, we propose a combination algorithm based on Demspter Shafer theory [14,15,23]. This algorithm combines and aggregates the reputation values of all links $R_i\,(j,k)\,,(N_j, N_k) \in FL_i^j$ to come up to a single reputation value of N_j. The proposed algorithm functions as follows. In the startup, $R_i\,(j,k)$ of each link $(N_j, N_k) \in FL_i^j$ is initialized to $neutral_v$ and it is updated according to the action detected by the monitor module. We consider two exclusive and exhaustive hypothesis that construct the frame of discernment $\varphi = \{C, \overline{C}\}$ where C means that the node N_j is cooperative and $\overline{C}$ means that the node N_j is uncooperative. The power set 2^{φ} consists of four elements: $\emptyset$, $C = \mathit{cooperative}$, $\overline{C} = \mathit{uncooperative}$ and hypothesis $U = \varphi$ (N_j is either cooperative or uncooperative which represents the uncertainty). In this scenario, the reputation module of N_i perceives the reputation of each link $(N_j, N_k) \in FL_i^j$ as recommendation provided by N_k. The reputation module determines the state of the node N_j in the link (j, k) according to $R_i(j, k)$. If reputation module states that N_j is cooperative through the link (j, k), which means that $R_i(j, k) \geq neutral_v$, The BPA of N_k is:

$$\begin{aligned} m_k(C) &= R_i(j,k) \\ m_k\left(\overline{C}\right) &= 0 \\ m_k(U) &= 1 - R_i(j,k) \end{aligned} \tag{5}$$

If reputation module states that N_j is uncooperative through the link (j, l), which means that $R_i(j, k) < neutral_v$, the BPA of N_l is

$$\begin{aligned} m_l(C) &= R_i(j,l) \\ m_l\left(\overline{C}\right) &= neutral_v - R_i(j,l) \\ m_l(U) &= 1 - neutral_v \end{aligned} \tag{6}$$

The direct reputation value $DR_i^j(t)$ is computed by combining all recommendations collected from all links $(N_j, N_k) \in FL_i^j$ by applying the Dempster rule of combination. $neutral_v - R_i(j, l)$ value reflects the degree of maliciousness of the link (j, l). The rational of this algorithm is that: a malicious node should compromise multiple forwarding links (multiple forwarding paths) to achieve its purpose that consists on disrupting the data forwarding process. Therefore, it is involved in multiple bad actions that cause the degradation of its direct reputation value. On the other hand, an honest node is involved in more good actions than bad actions; therefore, it can improve its direct reputation value.

Indirect Reputation

A reputation is considered indirect, if it is computed based only on the recommendations shared between neighbours. In HAPS, this reputation is calculated and used only when there is need. The exchange method is done only when it is necessary, especially when a particular neighbour needs to send its packets. The goal is to improve the accuracy of the computation of nodes reputation and to minimize the recommendations traffics. When a node termed requestor needs to relay its packets through neighbours, all neighbours exchange their computed direct reputation values about this requestor. After that, they compute its indirect reputation value by aggregating all received recommendations using Dempster Shafer theory. Note that recommendations from nodes regarded as malicious are ignored.

When N_i receives a RREQ packet, it checks whether the requestor N_j is a neighbour ($N_j \in NG_i$). If the requestor N_j is not neighbour, N_i simply forwards the RREQ packet. Else, N_i shares its recommendation about N_j in the neighbourhood and set the timer T_r. To prevent malicious nodes from colluding with other nodes or from manipulating the reputation values of some nodes, node N_i accepts only recommendation received before T_r expire. In order to compute the indirect reputation value of N_j, N_i aggregates all received recommendations using Dempster Shafer Theory. The recommendation of N_i about N_j is one among the set {cooperative-uncooperative}. Therefore, the frame of discernment is $\varphi = \{cooperative, uncooperative\}$. For instance, the reputation value of N_k at N_i is $DR_i^k(t)$. If N_k states that N_j is cooperative, the BPA of N_k is [16]:

$$\begin{aligned} m_k(C) &= DR_i^k(t) \\ m_k(\overline{C}) &= 0 \\ m_k(U) &= 1 - DR_i^k(t) \end{aligned} \tag{7}$$

If N_k claims that N_j is uncooperative, the BPA of N_k is:

$$\begin{aligned} m_k(C) &= 0 \\ m_k(\overline{C}) &= DR_i^k(t) \\ m_k(U) &= 1 - DR_i^k(t) \end{aligned} \tag{8}$$

The indirect reputation value of N_j is obtained after combining all recommendations using the Dempster's rule of combination. According to Dempster Shafer Theory features, the relevance of a recommendation depends on the reputation value of the recommender, which permit to get a reliable reputation value. This feature make our approach resilient to false recommendation dissemination. Thus, our approach can cope with collusion attack that occurs when a group of malicious nodes provides fake recommendations about an honest node. Because, the time T_rec between the diffusion and the combination of recommendations is very low. Then, these nodes have not sufficient times to collude.

Illustration Example:

Let assume three nodes $N_k, N_l \ and \ N_f$ with reputation values 0.4, 0.45 and 0.9 at N_i, respectively. They share their recommendations about N_j. N_k claims that N_j is cooperative, $N_l \ and \ N_f$ claims that N_j is uncooperative. Hence, the mass function are:

$$\begin{aligned} m_k(C) &= 0.9,\ m_k(\overline{C}) = 0,\ m_k(U) = 0.1 \\ m_l(C) &= 0,\ m_l(\overline{C}) = 0.3,\ m_l(U) = 0.7 \\ m_f(C) &= 0,\ m_f(\overline{C}) = 0.3,\ m_f(U) = 0.7 \end{aligned}$$

The reputation module of N_i combines $m_k \ and \ m_l$ as follows:

$$\begin{aligned} K_{kl} &= m_k(C)\, m_l(\overline{C}) + m_k(\overline{C})\, m_l(C) = 0.27 \\ m_{kl}(C) &= m_k \bigoplus m_l(C) = \frac{m_k(C)\, m_l(C) + m_k(C)\, m_l(U) + m_k(U) m_l(C)}{1 - K_{kl}} = 0.863 \\ m_{kl}(\overline{C}) &= m_k \bigoplus m_l(\overline{C}) = \frac{m_k(\overline{C})\, m_l(\overline{C}) + m_k(\overline{C})\, m_l(U) + m_k(U) m_l(\overline{C})}{1 - K_{kl}} = 0.041 \\ m_{kl}(U) &== m_k \bigoplus m_l(U) = \frac{m_k(U)\, m_l(U)}{1 - K_{klf}} = 0.0958 \end{aligned}$$

The obtained m_{kl} is combined with m_f as:

$$\begin{aligned}
K_{klf} &= m_{kl}\left(C\right) m_f\left(\overline{C}\right) + m_{kl}\left(\overline{C}\right) m_f\left(C\right) = 0.258\\
m_{klf}\left(C\right) &= m_{kl} \bigoplus m_f(C) = \frac{m_{kl}\left(C\right) m_f\left(C\right) + m_{kl}\left(C\right) m_f\left(U\right) + m_{kl}(U) m_f(C)}{1-K_{klf}} = 0.815\\
m_{klf}\left(\overline{C}\right) &= m_{kl} \bigoplus m_f(\overline{C}) = \frac{m_{kl}\left(\overline{C}\right) m_f\left(\overline{C}\right) + m_{kl}\left(\overline{C}\right) m_f\left(U\right) + m_{kl}(U) m_f(\overline{C})}{1-K_{kl}} = 0.094\\
m_{klf}\left(U\right) &== m_{kl} \bigoplus m_f(U) = \frac{m_{kl}\left(U\right) m_f\left(U\right)}{1-K_{klf}} = 0.0905
\end{aligned}$$

From this result, the indirect reputation value $IR_i^j(t)$ of node N_j is 0.81.

Final reputation

After obtaining $DR_i^j\left(t\right)$ and $IR_i^j\left(t\right)$, the final reputation value $FR_i^j\left(t\right)$ is computed by combining $DR_i^j\left(t\right)$ and $IR_i^j\left(t\right)$ with the following equation:

$$FR_i^j(t) = \delta * DR_i^j(t) + (1-\delta) * IR_i^j(t). \tag{9}$$

Where $\delta (0 < \delta < 1)$ determines the relevance of direct reputation compared to the indirect reputation.

4.3 Exclusion Module

The exclusion module is responsible for punishing malicious nodes. It considers a node having final reputation value smaller than the threshold as malicious. This module puts the detected node in its black list $Black_{list}$, and it sends a misbehaving report to the source node of data packets to proceed to its punishment. All nodes forwarding, receiving or overhearing the misbehaving report put the detected node in their $Black_{list}$ and proceed to its punishment. The punishment consists on: (1) invalidating all forwarding paths involving this node and evicting to route their data packets through this node. (2) Refusing to forward packets initiated from this node by discarding all its RREQ packets generated.

5 Performance Evaluation

In this section, we conduct a series of simulation experiments to examine the performance efficiency of the HAPS scheme using the network simulator NS-2.34. We evaluate the effectiveness of the HAPS scheme on the exclusion of malicious nodes dropping data packets in comparison to EAACK [13]. We simulate 40 mobile nodes deployed within an area of $700 * 700$ m. The number of malicious nodes varies from 2 to 12. The rest of simulation parameters are shown in Table 1. The following two metrics are used to examine the efficiency of HAPS:

Table 1. Malicious scenario parameters

Parameter	Value
Number of node	40
Routing protocol	DSR [17]
Simulation area	700 m × 700 m
Transmission range	250 m
Node speed	2 m/s, 4 m/s, 6 m/s, 8 m/s and 10 m/s
Pause time	0 s
Number of malicious nodes	2, 4, 6, 8, 10, 12
Number of CBR	20 connections
Simulation time	600 s

- **Average throughput (Kbps)** represents the total size of data packets that successfully reached their destination over the simulation times.
- **Malicious dropping ratio** refers to the ratio between the total numbers of data packets dropped by malicious nodes to the total numbers of data packets sent.

All plotted results are obtained after averaging the result of 20 simulation runs.

5.1 Average Throughput (Kbps)

Figure 2 shows the average throughput of HAPS and EAACK under varying the number of malicious nodes. We can observe that as the number of malicious nodes increases, the average throughput of two schemes decreases. However,

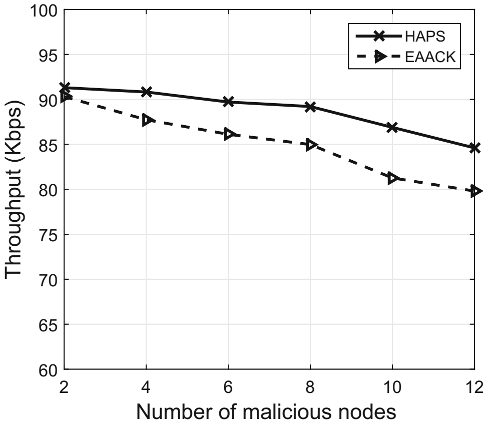

Fig. 2. Average throughput vs Number of malicious nodes

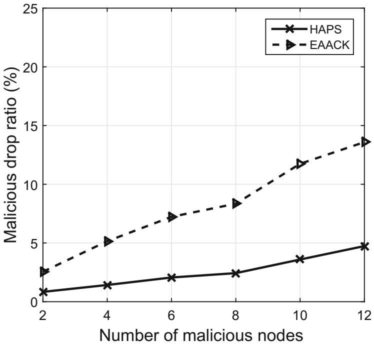

Fig. 3. Malicious dropping ratio vs Number of malicious nodes

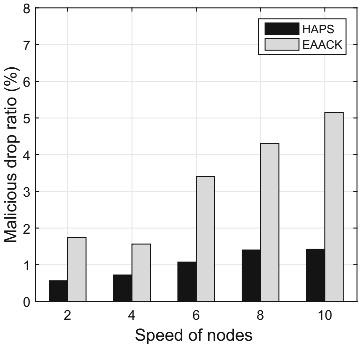

Fig. 4. Malicious dropping ratio vs Nodes speeds

the obtained results indicate that HAPS improves the average throughput much more than EAACK. This improvement is due to the fact that HAPS can identify and isolate malicious nodes instead of malicious links. Therefore, using HAPS scheme, the established paths between each pair of nodes is more reliable.

5.2 Malicious Dropping Ratio

Figure 3 depicts the malicious dropping ratio of HAPS and EAACK as a function of the number malicious nodes. The results show that the malicious dropping ratio increases as the number of malicious nodes increases. But, the malicious dropping ratio with HAPS increases more gently than with EAACK. This is because AASC penalizes malicious nodes more effectively and severely compared EAACK that is able to isolate only malicious links.

Figure 4 plots the malicious dropping ratio across varying the node speed. In this scenario, the network contains 4 malicious nodes. From this figure, we can observe that HAPS has a lower malicious dropping ratio in all cases compared to EAACK. This gap is more apparent when the nodes move faster. Because, when the nodes move faster, their neighbourhoods change frequently. As EAACK isolates only malicious links, each new neighbour for malicious nodes forms a new opportunity (malicious link) to drop more packets. Therefore, HAPS is more resilient to topology changes.

6 Conclusion and Future Work

In this paper, we have proposed HAPS, which is a novel acknowledgment Punishment Scheme aiming to detect and punish malicious nodes dropping data packets. In HAPS scheme, the reputation values of all links in which node is involved, are perceived as recommendations. Using Dempster Shafer Theory, these recommendations are combined to compute the reputation value of the node. HAPS incorporates a novel manner to exchange recommendations between nodes following the nature of on-demand routing protocol. The recommendations exchange is performed only when it is necessary and the aggregation is done based on Dempster Shafer Theory. HAPS punishes malicious nodes, whose the reputation values are smaller than the threshold by refusing to forward their packets, and isolating them from all network activities. The simulation results demonstrate that HAPS improves the throughput and reduces the malicious dropping ratio. As future work, We plan to evaluate mathematically the complexity of HAPS approach, and by simulation the effect of other network parameters in the effectiveness of HAPS approach (such Node density). We also plan to extend the HAPS scheme with an incentive mechanism aiming to cope against the selective packet dropping attack, while to motivate the cooperation of selfish nodes.

References

1. Peng, S.C., Wang, G.J., Hu, Z.W., Chen, J.P.: Survivability modeling and analysis on 3D mobile ad-hoc networks. J. Cent. South Univ. Technol. **18**(4), 1144–1152 (2011)
2. Marti, S., Giuli, T.J., Lai, K., Baker, M.: 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)
3. Buttyan, L., Hubaux, J.P.: Stimulating cooperation in self-organizing mobile ad hoc networks. Mob. Netw. Appl. **8**(5), 579–592 (2003)
4. Zong, C., Yang, S.: Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM), pp. 1987–1997 (2003)
5. Bansal, S., Baker, M.: Observation-based cooperation enforcement in ad hoc networks. arXiv preprint cs/0307012 (2003)
6. Zhu, H., Lin, X., Lu, R., Fan, Y., Shen, X.: Smart: a secure multilayer credit-based incentive scheme for delay-tolerant networks. J. IEEE Trans. Veh. Technol. **58**(8), 4628–4639 (2009)
7. Mahmoud, M.E., Shen, X.: FESCIM: fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks. J. IEEE Trans. Mob. Comput. **11**(5), 753–766 (2012)
8. Buchegger, S., Le Boudec, J.Y.: Performance analysis of the CONFIDANT protocol. In: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 226–236 (2002)
9. Michiardi, P., Molva, R.: Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Jerman-Blažič, B., Klobučar, T. (eds.) Advanced Communications and Multimedia Security. IFIP AICT, vol. 100, pp. 107–121. Springer, Boston (2002). https://doi.org/10.1007/978-0-387-35612-9_9
10. He, Q., Wu, D., Khosla, P.: SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks. In: Wireless Communications and Networking Conference (WCNC), pp. 825–830 (2004)

11. Yau, P.W., Mitchell, C.J.: Reputation methods for routing security for mobile ad hoc networks. In: Proceedings of the Mobile Future and Symposium on Trends in Communications, pp. 130–137 (2003)
12. Balakrishnan, K., Deng, J., Varshney, P.K.: TWOACK: preventing selfishness in mobile ad hoc networks. In: Wireless Communications and Networking, pp. 2137–2142 (2005)
13. Shakshuki, E.M., Kang, N., Sheltami, T.R.: EAACK—a secure intrusion-detection system for MANETs. IEEE Trans. Industr. Electron. **60**(3), 1089–1098 (2013)
14. Shafer, G.A.: Mathematical Theory of Evidence. Princeton University Press, Princeton (1976)
15. Sudkamp, T.: The consistency of Dempster-Shafer updating. Int. J. Approx. Reason. **7**(1), 19–44 (1992)
16. Chen, T.M., Venkataramanan, V.: Dempster-Shafer theory for intrusion detection in ad hoc networks. IEEE Internet Comput. **9**(6), 35–41 (2005)
17. Johnson, D.B., Maltz, D.A.: Dynamic source routing in ad hoc wireless networks. In: Imielinski, T., Korth, H.F. (eds.) Mobile Computing. The Kluwer International Series in Engineering and Computer Science, vol. 353, pp. 153–181. Springer, Boston (1996). https://doi.org/10.1007/978-0-585-29603-6_5
18. Liu, K., Deng, J., Varshney, P.K., Balakrishnan, K.: An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Trans. Mob. Comput. **6**(5), 536–550 (2007)
19. Sheltami, T., Al-Roubaiey, A., Shakshuki, E., Mahmoud, A.: Video transmission enhancement in presence of misbehaving nodes in MANETs. Multimedia Syst. **15**(5), 273–282 (2009)
20. Sun, H.M., Chen, C.H., Ku, Y.F.: A novel acknowledgment-based approach against collude attacks in MANET. Expert Syst. Appl. **39**(9), 7968–7975 (2012)
21. Djahel, S., NaïtAbdesselam, F., Zhang, Z., Khokhar, A.: Defending against packet dropping attack in vehicular ad hoc networks. Secur. Commun. Netw. **1**(3), 245–258 (2008)
22. Campos, F., Cavalcante, S.: An extended approach for Dempster-Shafer theory. In: Information Reuse and Integration, pp. 338–344 (2003)
23. Bloch, I.: Some aspects of Dempster-Shafer evidence theory for classification of multi-modality medical images considering partial volume effect. Pattern Recogn. Lett. **17**(8), 905–919 (1996)
24. Bounouni, M., Bouallouche-Medjkoune, L.: A hybrid stimulation approach for coping against the malevolence and selfishness in mobile ad hoc network. Wirel. Pers. Commun. **88**(2), 255–281 (2016)