Towards an efficient monitoring in multi-hop mobile ad hoc networks

NADIA BATTAT[1]*, ABDALLAH MAKHOUL[2]†, HAMAMACHE KHEDDOUCI[3]‡

[1] *LIMED Laboratory, University of Bejaia, Algeria*

[2] *FEMTO-ST Institute, Univ. Bourgogne Franche-Comté, CNRS, Belfort, France*

[3] *LIRIS Laboratory, University of Lyon 1, Villeurbanne France*

Mobile ad-hoc networks (MANET) are vulnerable to many types of attacks. Monitoring MANET is then important to ensure high level performance. This monitoring can be achieved by two operations: first by observing the operational states of the connected mobile nodes in relation with the existing links; and second by controlling the application quality of service. Many challenges arise in the MANET self-monitoring. Hence, the non-cooperation behavior of mobile nodes can decrease the monitoring performance and may cause damages. Moreover, some malicious participants may disrupt the monitoring system through

* email: nadiabattat@yahoo.fr
† email: abdallah.makhoul@univ-fcomte.fr
‡ email: hamamache.kheddouci@univ-lyon1.fr

altering the collected data, reporting false measurements, defining new management policies or flooding false alarms. Therefore, in this paper we propose a new self monitoring scheme that comprises a new multi-criteria monitors' election method while integrating a new trust based cooperation technique based on game theory. This scheme does, not only, elect the trustworthy monitors having a large capacity, but it also can guarantee the continuous participants' control.The conducted experimental results indicate that the proposed scheme outperforms the cluster-based and CDS-based architectures in terms of the number of exchanged messages, excluded regular monitors and that of detected irregular monitors.

Key words: Mobile ad hoc network; monitoring; trust; evolutionary game theory; topologies;

1 INTRODUCTION

Mobile Ad hoc NETwork (MANET) is defined as an autonomous system of mobile devices (PDA, laptop, and others) [16] that can be connected anywhere without any infrastructure [1] [9] [15] [21] [29]. These devices can cooperate to maintain this temporary network and to provide services such as routing and service discovery. The ability to create this kind of network without any extra cost or centralized administration allows it to operate under difficult conditions as in battlefields, emergency search, and rescue missions or under normal conditions as in classroom meetings and data acquisition in remote areas. However, MANET has specific requirements in terms of limited resources (battery power, bandwidth, CPU and storage space), communication overhead, lifetime, security, mobility, scalability, etc. [27, 25]. Considering these specific constraints, a monitoring mechanism must be implemented to control the state of the network.

Self monitoring of MANET consists in evaluating the operational state of its mobile devices, the links between them as well as its quality of service. This is achieved by a subset of mobile nodes (called monitors) which are elected according to several predefined parameters [7]. Each monitor performs its assigned tasks and in the same time is responsible for controlling a subset of mobile nodes in its area called the monitored nodes. In addition, it can create or update the policies and delegate part of its monitoring tasks to some mobile nodes and collaborate other monitors to exchange data or to ensure a global monitoring. In their turn, the monitored nodes are responsible for enforcing the policies they receive from their monitors, collecting the requested information and delivering them to their corresponding monitors. They can also achieve local monitoring, filtering and aggregating [24][5]. Then, the monitoring evaluation can be performed by analyzing and processing the local collected data by the nodes as well as the information received from their neighbors. This evaluation aims to guarantee fault monitoring, configuration, performance monitoring and/or accounting

To realise high level monitoring, it is vital that each participant (monitored node or monitor) contributes correctly to the election of monitors and the monitoring process. However, this leads to consume more computational and energy resources. Actually, not all nodes participate in this process. Selfish nodes can use the resources of the others without participating in the monitoring functions. Malicious nodes can falsify the collected data, modify the distributed policies and make illegal and inappropriate decisions. Furthermore, some MANET applications need to have real time monitoring data. Nevertheless, the latter are not often available from a single monitor, but are distributed on network. The set of nodes that store monitoring data can either exchange periodically or provide an unreal or outdated data

In order to force mobile nodes to obey the monitoring approach and cooperate with each other in a legal way, we propose in this paper a new monitor electing method. It is based on two main factors: truthfulness and capability. In this case, trust is a belief level that a monitored node (resp. a monitor) can put on a monitor (resp. a monitored node). A malicious (or selfish) node can behave like a regular node and it can return to its malicious behavior after the election of monitors. In fact, we propose a new monitoring scheme in which participants must be controlled by their regular neighbors. Thus, each node estimates the trust values of its neighbors which are calculated according to the number of the positive realized monitoring tasks. These values can be increased or decreased according to the behaviors of the participants. If an estimated trust value of a participant is less than a given threshold, then this node can be considered as an irregular one. Consequently, it will be denied or penalized.

In this paper we propose a new monitoring scheme in which participants must be controlled by their regular neighbours. Thus, each node estimates its neighbors' trust values, which are calculated according to the number of positive monitoring tasks performed. Depending on participants' behaviors, these values can be increased or decreased. If the estimated trust value of a participant is lower than a given threshold, then this node can be considered as irregular and will be denied or penalized. It is possible to determine the decision to contribute or not in the monitoring process while observing the behavior of the neighbors of the nodes. This encourages us to use evolutionary game theory to model the contribution of the nodes as strategic interactions between two players (regular and irregular nodes). The regular player tries to maximize its payoff by increasing its likelihood of successful contribution to the monitoring process while the irregular (either malicious or selfish node) tries to maximize its likelihood of using monitoring services while at the same time minimizing its contribution to the monitoring process implemented by formulating a non-cooperative zero-sum game.

The contributions of this paper can be summarized as follows:

- We review and classify the existing monitoring approaches according to the monitors election algorithms. We present the proposed election algorithms and each maintenance process.

- We define the set of rules to detect the malicious and selfish behavior of all nodes involved in the monitoring process and we provide a formulation of an evolutionary game theory based model to analyze the cooperation behavior of mobile nodes.

- We propose a new scheme that ensures effective monitoring in multi-hop MANETs.

- We analyze the proposed scheme regarding some of the MANET monitoring requirements as mentioned in [7] that can minimize vulnerability in the presence of malicious and selfish nodes.

- We analyze the proposed architecture through MATLAB simulations to show that the proposed scheme can significantly reduce overhead and maintain a high level of detection compared to cluster-based architecture and CDS-based architecture.

- We evaluate the dynamic performance of the replicator through simulations to prove its validity.

The rest of this paper is organized as follows: the second section describes previous works in the field of monitoring of mobile ad hoc networks. The basic concepts of efficient monitoring are defined in section 3. Section 4 is dedicated to presenting our proposed improvement to ensure efficient monitoring, whereas section 5 includes the evolutionary model based on game theory. In section 6, we define new security policies to detect participants' abnormal behaviors. In section 7, we evaluate the replicator dynamic performance and analyze the performance of our scheme compared to cluster-based architecture and CDS-based performance. Section 8 contains the proposed approach analysis regarding both survivability and safety requirements. Finally, section 9 concludes our paper and suggests future work.

2 RELATED WORKS

In literature, several monitoring approaches were proposed for mobile ad hoc networks [7]. Among the majority of monitoring approaches, the researchers explained their algorithms for electing monitors. In this paper, we propose to classify the existing monitoring approaches according to their electing algorithms as follows:

1. ***Unique criterion based election approaches:*** These approaches ([10] [4] [23] [22] [24]) use only one criterion such as Lowest-ID or Highest-Degree to elect monitors in that they are easily achievable. However,

these algorithms do not take into account all MANET characteristics and the resources level of the elected nodes. This can lead to reapply the election process which reduces the lifetime of monitoring cycle and increases the network overhead in addition to the consumed energy. Moreover, they do not balance the monitoring tasks uniformly among all the nodes. This can result in electing the same node as monitor frequently.

2. ***Multi criteria based election approaches:*** These ones ([26] [8] [31] [19]) use a diversity of criteria to elect monitors. They aim to increase the lifetime of the monitoring cycle by electing the most cost-efficient nodes as monitors and at, the same time, balancing the resource consumption among the nodes and their neighbors. Each algorithm has its advantages and disadvantages.

The proposed algorithms can either perform in accordance with the occurrence of an event (mobility, insufficient battery power, etc.), or periodically. As we may note, several approaches of both classes allow to elect monitors regardless of the mobile nodes' sincerity and honesty. These two criteria are needed from the monitored nodes and their monitors to establish trust relationships. The latter can guarantee that the performance of their network will not be affected.

In [4], the authors propose a probabilistic scheme in order to enhance the reliability of monitoring by excluding the dishonest managed nodes that provide unreal data management from the data collection. Nevertheless, the scheme effectiveness depends on the exchanged measurements correctness [5]. First, it will not be efficient, if the network mobility is unpredictable.

Second, the abnormal nodes are selected according to one metric which is not always sufficient to determine if the given data management is trustworthy or not. Third, the authors do not take into account the managers malicious behavior. Finally, coherence mechanism must be considered in the presence of more than one manager in the connected component [4], which is expensive.

In [3], the authors propose a survivable monitoring that allows a set of nodes called domain nodes to monitor the behavior of visitors when they join their domains. The authors assume that the supervisor is reliable and trusted and that the domain nodes are too. Nevertheless, a malevolent visitor can share its key with other unauthorized nodes [3]. Moreover, using cryptography mechanisms can be computationally expensive for resource use.

In [18], the authors propose to assess the selfish behaviors of each monitored node regarding its cooperations in forwarding others packets. However, it is a passive monitoring. In addition, they do not take into account the monitoring units malicious and selfish behaviors.

In [11], the authors propose to use a set of predefined network security policies to ensure access control, a sequence number to prevent replay attacks and an Intrusion Detection Systems (IDSs) to detect the nodes malicious behaviors. However, EDRAMA allows the network administrator to manually change the node status from a malicious to a trusted one. It also has the limits of the IDS.

In [23], the authors propose to authenticate mobile nodes in order to detect intrusion. Thus, they use a non-interactive zero knowledge technique to determine a set of nodes having access to specific applications or services in MANET. From among these authorized nodes, only those with the highest battery can play the role of monitors. The latter analyze all the transmitted packets in their areas to identify any intrusion. Once an intrusion is detected, a monitor informs its neighbors about this malicious behaviors by forwarding warning message. However, the authors do not take into account the monitors malicious or selfish behaviors. Moreover, they are exclusively based on the analysis of exchanged packets for detecting intrusion.

In [14], the authors aim to detect the inappropriate behaviors of mobile nodes for ensuring efficient routing. In fact, they propose to add three components: a monitor, a reputation system and a path manager, to the DSR (Dynamic Source Routing) routing protocol functionality. Nevertheless, this approach relies on passive monitoring. Moreover, it is based on the direct observation of a neighbor regardless its malicious behavior.

In [17], the authors propose a novel algorithm to prevent sybil attacks in WSN using mobile observers nodes. They first detect areas suspicious to Sybil attack and then record information about these areas in their memories. Using stored information, they will be able to detect Sybil nodes. However, they do not precise how to choose the mobile nodes and if these nodes can be ordinary nodes or not.

All these limits in the related works provide us with the motivation to propose a new monitoring scheme which is based on active and passive monitoring and integrates trust system dedicated to monitoring.

We can mainly notice that only some of the existing approaches take into consideration the participants behavior in either monitors election ([23] [18] [3]) or monitoring process ([10] [3] [11] [18] [14] [4]). Some of these approaches [18], [4], [20] and [3] assume that the monitors are trusted and they do not detail how to detect their normal behaviors.

To detect the abnormal behaviors of participants, these approaches rely on different mechanisms: [10], [3], [11], and [23] allow access control by checking the identity of each node that participates in the monitoring tasks. While, [18], [23], [11], and [14] monitor the incoming and outcoming traffic, whereas [4] monitors the connectivity variations of the controlled nodes. Nevertheless, these mechanisms might not be enough to detect the irregular nodes behaviors. Moreover, one of these approaches (EDRAMA [11]) is part of management solution that is applicable only in specific application (military field).

Unlike the majority of these approaches, we use a penalization technique and we indicate how an irregular node behaves and participates legally in monitoring process at the end of the penalty period. Our approach is also distinguished from the trust system developed for routing mentioned in [14]. We evaluate the normal behaviors of participants while observing the success of realized monitoring tasks. Moreover, we calculate the trust values based on the combination of direct and indirect estimations. However, besides the main security services, our monitoring approach satisfies specifically integrity and availability.

3 EFFICIENT MANET MONITORING

In order to ensure an efficient monitoring for MANET several tasks must respected and done by mobile nodes:

- Policies announcement: the network administrator (or network/subnetwork monitors) may define a set of rules/policies (**If** condition **then** action), in order to simplify the monitoring process. These rules will be diffused to all/some participants [7].

- Data collection: a large list of data can be collected from each node (latitude, longitude, energy level, storage capacity, bandwidth, etc.) according to the network applications. Depending on the type of data requested (time dependent data like energy left on the device or time independent data on the example of packet logs), the collection can be active (by exchanging data message or introducing new fields in the routing messages) or passive (by analyzing network traffic).

- Data analysis: the collected data can be locally analyzed before being sent to the corresponding monitors. Local analysis allows a node to extract some information such as the use of resources and disconnections. The received data and local reports will be processed in order to detect some anomalies (failures, intrusions, etc.), to determine topology or to extract some features and/or measurements as well as the network performance in terms of security, availability, and also in terms of service quality. Subsequently, alarms can be launched to announce a devices dysfunction, links failures or an irregularity in the network.

- Data storage: the collected data and/or the obtained reports can be exchanged between monitors or simply stored locally.

Ensuring effective monitoring can be assured by detecting participants with abnormal behaviors (malicious and selfish behaviors). This can lead to the achievement of goal-oriented monitoring, help monitoring to generate a suitable decision and thus guarantee the robust operation of mobile ad hoc networks and increase their performance.

4 OUR MANET SELF MONITORING SCHEME

In the following, we describe our proposed scheme. The main idea of our method is summarized in Figure 1, where each node should execute these states.

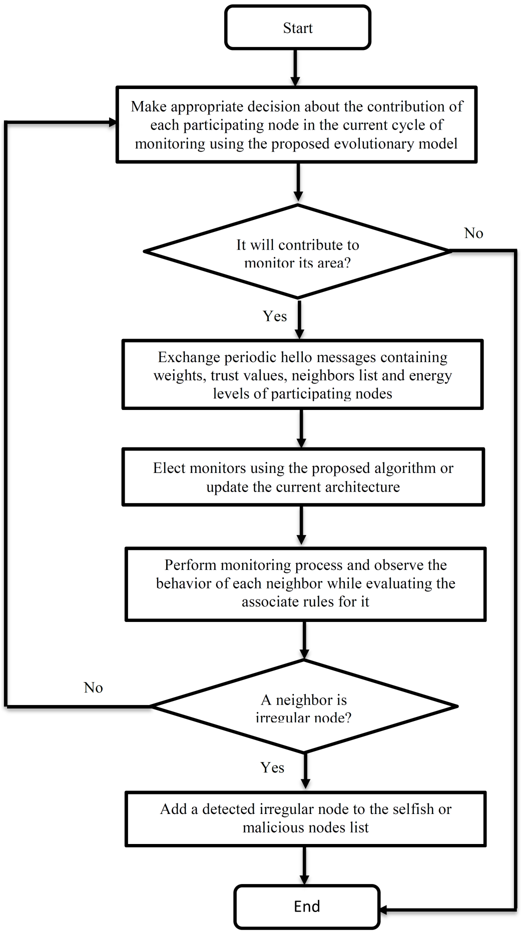

Start
Make appropriate decision about the contribution of each participating node in the current cycle of monitoring using the proposed evolutionary model
It will contribute to monitor its area?
No
Yes
Exchange periodic hello messages containing weights, trust values, neighbors list and energy levels of participating nodes
Elect monitors using the proposed algorithm or update the current architecture
Perform monitoring process and observe the behavior of each neighbor while evaluating the associate rules for it
No
A neighbor is irregular node?
Yes
Add a detected irregular node to the selfish or malicious nodes list
End

FIGURE 1
A diagram flow chart of our proposed scheme

4.1 Messages structure

Monitoring message overhead can increase the energy consumption, decrease the available bandwidth and cause network congestion. Thus, we propose some modifications on the original hello message by adding the following fields:

- *Weight* ($W(n_i) \in [0,1]$): this field contains the weight of the node n_i that is initialized to 0. Its value is estimated in section 4.3.
- *Trust value* $T(n_i) \in [0,1]$: this field represents the trust value of the node n_i that is initialized to 0.5.
- *Energy level* $E(n_i)$: this field indicates the remained energy level of the node n_i.
- *Role*: this field defines the role of the node n_i: monitor, delegated monitor or ordinary node.
- $NeighborsList$: this field contains the IDs of the node neighbors and their estimated trust values.

4.2 Trust computation method

Each node must observe the behaviors of its neighbors to detect their malicious or selfish comportments. Consequently, it can observe and trace their behaviors by the continuous updates of the trust values.

Initially, we assign to each node a trust value equal to 0.5 [⋆] . We believe that controlling the exchanged messages between monitors and their monitored nodes is not sufficient to confirm the malicious behavior or the selfish-

[⋆] to not consider a node in advance as being selfish, malicious or confident ness of either monitors or monitored nodes, since they can forward the exchanged messages without participating legally in the monitoring process. In fact, we define the following rules for identifying the selfish or the malicious behaviors of mobile nodes participating in monitoring process.

- The contribution level of each mobile node in the monitoring process (data collecting and/or data analysis) can be regarded as specific information. Consequently, it can provide falsified evaluation about its collaborations in order to raise its trust value. Therefore, a monitor can distribute the full report (or only part of this report) to its controlled node to confirm its honesty. A monitored node can either select a route containing a maximum number of its neighbors for forwarding its data and/or the local report, or divide this quantity of data into N packets (N represents the number of its neighbors). Then it sends each one through each neighbor. When one neighbor drops packets and that this behavior is observed by a sender, the latter will decrease its trust value.

- A local analysis is needed to avoid monitors to act maliciously and to detect their selfish behaviors. Misbehaved or selfish nodes will be penalized by decreasing their trust values.

- As mobile nodes use limited storage capacities, they can discard not only their collected data but also other nodes collected ones, in order to exploit its resources for further interesting uses. Therefore, the monitored node (resp. the monitor) can periodically ask its monitors (resp. the data holder) to send a randomly selected piece of its collected data at a specific time. Once receiving this requested data, the monitored node (resp. the monitor) compares it to its stored data hunk and then increases or decreases the corresponding node trust value. However, this checking may cause extra communication and computational cost.

- The participants' contributions of mobile nodes can indicate the existence of malicious or selfish nodes. For instance, if a node exchanges its opinions on neighbors periodically and performs a local analysis while it does not participate in forwarding data or data storage, it will be considered as malicious.

- A monitor can compare the received data within its radio range to detect the malicious or selfish behaviors of its neighbors. For instance, if more than one neighbor indicate that two nodes X and Y are two neighbors and the neighbors' list of X does not contain any information about Y, a monitor can conclude that X is either selfish or malicious.

For updating this value of confidence, we use the activity rate (AR), which is calculated according to the number of positive realized tasks including the packet forwarding rate and the realized monitoring tasks (creating and updating of policies, distribution of policies, data collection, data analysis and/or data storage). If we consider two nodes i and j, the node i calculates the $AR(j)$ as follows: the node i should record the number of positive interactions ($pos(i, j)$) with the node j, and the total number of interactions ($total(i, j)$), over a given interval of time, and then it calculates the activity rate as follows:

$$AR = pos(i, j)/total(i, j) \tag{1}$$

The trust value is estimated over time to reflect changes in the activity rate.

Nevertheless, local estimation on each mobile node might not be enough to detect any node bad behavior. It should have information from other nodes. Moreover, in some cases, a mobile node can monitor only the behavior of its direct neighbors. As a result, not all neighbors at $n-hops$ will honestly share the real values. Consequently, we propose that each node calculates the trust values based on the combination of direct and indirect estimations that derive from neighbors. Therefore, we consider also the two following cases:

- A neighbor does not report his accurate trust value about the corresponding monitor (resp. monitored node) in case of hardware or software failures held by this node.
- A neighbor can provide a false trust value about the corresponding monitor (resp. monitored node). It may provide a negative (or positive) value to misbehaved/trusted monitor (resp. monitored node): *false accusation attack* [6] [28] (or *false praise attack* [2] [12]).

These trust values will be exchanged between each node with its neighbors. After receiving the indirect estimations, a node i calculates the trust values $T(c)$ (its and that of its neighbors) using the following formula:

$$T(n_j) = (\sum_{k=1}^{n}(T(k,j)) + T(i,j))/(n+1) \tag{2}$$

n is the nodes number having sent their trust values about the node j to the node i. $T(k,j)$ is node k trust value about node j.

When a node does not receive any trust value, it can rely either on its trust values or on the previously gathered ones. The trust value can be increased or decreased by a chosen changing step Stp, according to nodes' behaviors. We assume that the chosen changing step Stp equal to 0.1. The choice of this value refers to the existing works in the literature [30].

Mobile node can behave selfishly or maliciously following to its features (to save its energy or to realize its malicious goals) or according to the mobile environment characteristics (Nodes' mobility, involuntary disconnection due to low energy, insufficient energy level to forward packets, network congestion, malicious nodes presence, etc.). Nevertheless, environmental conditions can lead to intensively deteriorate trust values. Therefore, we propose to use the maximum authorized faults number $MaxNbrF$ to avoid the inexactitude of trust value estimation. If a node does not participate in $three$ successive activities while it has sufficient energy level to perform them and its trust value is equal or less than a predefined threshold $Bt = 0.3$, it will be irregular. A detected node will be added to the selfish or malicious nodes list (see algorithm 1) according to its last behavioras mentionned in table 1).

4.3 Monitors election

Our approach is a multi criteria based election method. The election process targets to increase the monitoring system lifetime through distributing the monitoring tasks and sharing the resource consumption among all (or some) nodes. Thus, the network is logically divided into clusters with a single monitor (cluster-head). We assume that only regular nodes can participate in monitors election. As a result, every regular node n_i, aware of its neighbors, performs the following steps:

1. it calculates its weight $W(n_i)$ which indicates its ability to serve as

Algorithm 1 Locally detection of regular, irregular and normal nodes

```
Constant $MaxNbrF = 3$ ;
$T(n_i)$: Trust value of the node $n_i$;
$NbrF$: number of node' faults ;
$A$: Last activity that must be realized by the node $n_i$;
$The function K$: $K(A) = 1$, if $A$ is correctly realized by $n_i$, otherwise $K(A) = 0$;
$The function B$: $B(n_i) = M$, if $n_i$ acts maliciously $or$ $B(n_i) = S$ if $n_i$ acts selfishly;
$SL$: List of detected selfish nodes;
$ML$: List of detected malicious nodes;
$E(n_i)$: Energy level of the node $n_i$;
$Et$: Necessary energy level for realizing $A$ ;
$The function S$: $S(n_i) \in${Irregular, Regular, Normal};
$Dt$: Penalty period;

Begin
if $(((n_i \notin SL) and (n_i \notin ML)) or (S(n_i) = Normal))$ then
  if $(K(n_i) = 1)$ then
    if $(T(n_i) \prec 1)$ then
      Recompute $T(n_i)$;
      if $(T(n_i) \succ 0.5) and (S(n_i) = Normal))$ then
        $S(n_i)$ = Regular;
      end if
    end if
  else
    if $(T(n_i) \succ 0)$ then
      Recompute $T(n_i)$;
      $NbrF = NbrF + 1$ ;
    end if
  end if
  if $(T(n_i) \leq Bt)$ then
    if $(((n_i \notin SL) and (n_i \notin ML)))$ then
      if $(E(n_i) \succ Et)$ then
        if $(NbrF \geq MaxNbrF)$ then
          $S(n_i)$= Irregular;
          $Dt$ = CurrentTime + $Tb$ ;
          if $(B(n_i) = S)$ then
            add $n_i$ to $SL$;
          else
            add $n_i$ to $ML$;
          end if
        end if
      end if
    end if
  end if
end if
End
```

Malicious behaviors	**Selfish behaviors**
Mobile node will be considered as malicious if it: • falsifies the monitoring policies. • Generate unnecessary traffic. • Advertises non-existing monitors. • Modifies the monitoring system. • Provides fake data • Broadcasts a false alarm • Contributes in some monitoring tasks only.	Mobile node will be considered as selfish if it: • refuses to participate in monitoring process. • Discards the collected data. • Drops the exchanged monitoring messages

TABLE 1
Participants malicious and selfish behaviors

monitor as follows:

$$W(n_i) = COF1 * T(n_i) + RS(n_i) \tag{3}$$

- $COF1 \in [0, 1]$ is the metric trust value coefficient.
- A monitor can consume more resources than a monitored node because of the monitoring tasks that must be performed. In fact, we also use the weighted parameter $RS(n_i)$ to elect monitors. This weighted parameter can be computed according to some/all of the node hardware and software capabilities such as:
  - the processing power: node with little processing power can slow the forwarding or analyzing of collected data.
  - The energy level: node with sufficient energy level can per-

form the monitoring tasks.

  - The storage capacity: node with sufficient storage capacity can ensure collected data and monitoring reports storage as well.

  The choice of these performance related attributes is related to MANET features and the network applications' needed.

2. it forwards a hello message, containing its weight, its trust value, its neighbors and their estimated trust values list and its energy level, to its neighbors.

3. it waits a time period for receiving the same kind of message from its neighbors

4. it compares its weight with those of its neighbors. It becomes monitor, if it has the maximum weight. We assume that if a mobile node is the only node in the network or it does not have any neighbors, then it becomes monitor.

A monitor informs its neighbors about its presence by sending hello message, while initializing the field $Role$ to 1. Each neighbor selects the nearest monitor based on hop count.

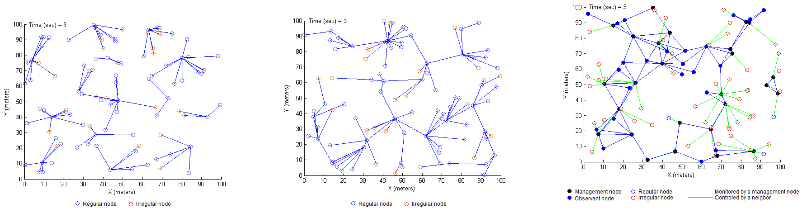
4.4 Maintenance of the monitoring architecture

To detect any mobile node neighbors, periodic hello messages are exchanged. Once these messages are received, each mobile node can update the list of its neighbors, their weights, their trust values and their roles with minimum transmission overhead.

When mobile nodes voluntarily/involuntarily disconnect or move, our approach faces these topological changes by applying the following policies:

- When a new regular node joins a network, it exchanges with its neighbors its data, and then chooses the nearest monitor.
- When a mobile node loses connectivity with its monitor, two cases can be considered:
    - *Voluntary disconnection of regular monitor*: the regular monitor can select one of its regular neighbors having the maximum weight to replace it. Then, it informs its neighboring nodes and the other monitors about the new one.
    - *Involuntary disconnection of monitor*: when a mobile node detects the sudden death of its monitor, it launches the election of new monitor.

In order to reduce the number of monitors election and consequently to maximize the lifetime of the monitoring process, a monitor can integrate a delegation strategy. It checks the list of its neighbors, their energies and their trust values to select the set of candidates. Each candidate must have a trust value ≥ 0.5. The selection of the delegated monitors can be randomly or must satisfy some criteria (those having maximum/minimum energies). The number of the delegated monitors is determined by the monitor, according to its area density and the cluster's diameter. Nevertheless, in our case, the delegated monitors are authorized only to collect and analyze independent time data that do not have any influence on the network performance such as monitor ID and the used routing protocol.



(a) Cluster-based

(b) CDS-based

(c) Our scheme

FIGURE 2
The network architecture.

The monitor sends a *delegation-message* to the considered nodes for obtaining their confirmations. If these nodes confirm their participations, the corresponding monitor sends a message including its ID, the list of the delegated monitors and the delegation period. At the end of the considered period, other nodes can be delegated to control their areas.

4.5 Architecture

The proposed topologies for the monitoring approaches are usually based on the construction of cluster or CDS (Connected Dominating Set) [7] as shown in figure 2. Our proposed approach is also cluster-based where each participant (monitor or monitored node) is controlled by its regular neighbors (see figure 2 [c]).

The architecture of our scheme is shown in Figure 3. When a participant locally detects an irregular neighbor, it sends a hello message containing the new estimated trust value to all the members of its cluster. Once receiving this message, each member updates the trust values of its neighbors. According to the new calculated trust value, the mentioned node can be considered as irregular one or not.

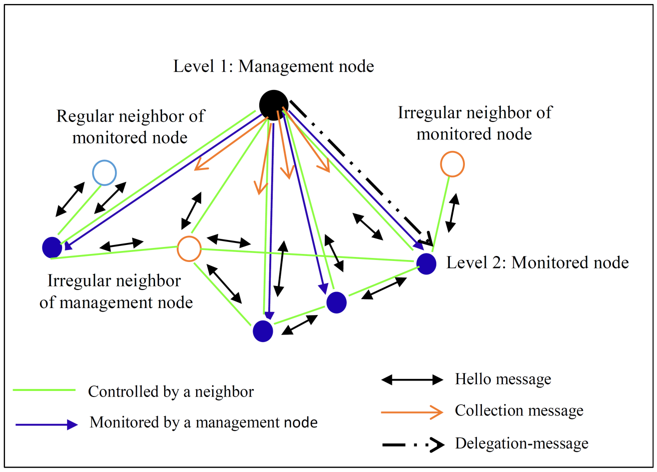

Level 1: Management node
Regular neighbor of monitored node
Irregular neighbor of monitored node
Level 2: Monitored node
Irregular neighbor of management node
Controlled by a neighbor
Monitored by a management node
Hello message
Collection message
Delegation-message

FIGURE 3
The architecture of our proposed scheme

To urge the irregular nodes to behave normally and participate legally in monitoring process, a penalization technique must be considered. In this paper, a detected irregular will be penalized by excluding it from the monitoring services. In addition, selfish node's neighbors can refuse to perform its requests or forward its packets.

We assume that an irregular node will be considered as a normal node at the end of a predefined timeout period Tb which can be fixed to $100s$ according to [14]. This is justified by the following reasons:

- A mobile node might be false defendant due to the congestion, the interference, the collisions, or the noise.
- Selfish or malicious node may change its irregular behavior and acts honestly. So, it realizes its legally tasks in order to beneficiate from monitoring services.

- The monitoring system success depends highly on the participants cooperation.

We assign to each normal node a trust value equal to 0. When a neighbor finds that the trust value of a normal node exceed 0.5, it considers it as a regular one, then removes it from the malicious or selfish list. Consequently, this node is authorized to participate in monitoring process.

4.6 Monitoring process

With our approach, all the collection of monitoring data acquisition from the monitored nodes will be done periodically. When a monitor decides to begin a collection of data, it sends a *collection* message, consisting of two fields to its monitored nodes. These fields correspond respectively to the identifier of the appropriate monitor and the parameters of collection. The latter may indicate the node features (the remaining energy level, the available storage space, the percentage of CPU utilization, the available bandwidth, the location (longitude and latitude), the speed and direction, the link quality, etc.) and relate to the network data (latency, packets logs, neighbors list, etc.). Nevertheless, we notice that data analysis and data storage are not addressed in this paper.

5 EVOLUTIONARY GAME THEORY BASED MODEL FOR MONITORING

The evolutionary game theory (EGT) [13], which originated as an application of Game Theory to model animal evolution in biology, treats the behavior of individuals set over a period of time. It aims to formulate a model to help evaluate the dynamic evolution of their selected strategies [13]. We propose using an evolutionary model based on game theory to study the interaction between regular and irregular modes in order to obtain the proportion of mobile nodes that contribute to MANET monitoring. This model allows a participant node to analyze the contradictory situations about how much and when to participate in the monitoring process. Consequently, as the game runs, the regular (resp. irregular) node may change its normal (resp. abnormal) behavior. The decision to participate (i.e. illegally) in the monitoring process correctly and legally does not depend on any regular (i.e. irregular) node current beliefs, but rather on the behavior of irregular (i.e. regular) neighbors.

5.1 Players

In our model of game, during the monitoring process, the MANET architecture is a monitoring game and a player could be of two types:

- Regular node: that assumes correctly its task according to its role (monitor or monitored node).
- Irregular node: selfish node that is defined as an economically reasonable node or malicious one that aims to increase as much as possible its benefits.

5.2 Strategies

The game is modeled to analyze two pure nodes strategies in the network: *Correct Contribute (CC)* and *Incorrect Contribute (IC)* (as shown in table 2). A participant node may select the strategy CC based on :

- Global interest: mobile node can cooperate to help others and enhance the network performance.
- Behavior of the other nodes: mobile node may cooperate in monitoring

process if the other nodes (for instance, the majority of its neighbors) behaved correctly the last time.

- Private interests: mobile node can participate to achieve its own interests (e.g. gain a trust).

The nodes that choose IC strategy can be further classified into two categories, as described below. To distinguish between these two categories, we use a parameter H as follows:

- A node exploiting the network to achieve its own reward noted by OR (it uses the network to transmit its own data, to increase its trust value, to provide a wrong data or to perform an attack). This node has $H = 1$.
- The second type can be described as a node which when following honest selfish strategy refuses to cooperate with the other to perform the network services and does not care about the reward of the whole network. This node has $H = 0$.

An irregular node makes its decision over the participation or not in monitoring system. Let's consider the probability of an irregular node exhibiting malicious/selfish activity be s, and the same node exhibiting normal behavior one be $1 - s$.

When a node participates to monitor the network, its consumed energy level is E. A reward R can be obtained if a node profits from the monitoring services. This can be guaranteed when the network is totally monitored, i.e. all nodes choose the strategy CC. If at least one node chooses the strategy IC, the network becomes not (or partially) monitored. This fact will reduce

$R\ I$	$S_I(CC)$	$S_I(IC)$
$S_R(CC)$	$((1-s)*(R-E),$ $(1-s)*(R-E))$	$((1-s)*(R-L-E),$ $s*(R-L+H*(RO-E)))$
$S_R(IC)$	$(s*(R-L+H*(RO-E)),$ $(1-s)*(R-L-E))$	$(s*(R-L+H*(RO-E)),$ $s*(R-L+H*(RO-E)))$

TABLE 2
Strategic form of the game:CC vs IC

the overall network performance (losses of data, damages, etc.) by the value noted by L. Note that $R > L$, $R > E$ and $OR > E$.

Table 2 shows the obtained payoffs corresponding to the interaction between regular and irregular nodes.

- When the regular and irregular nodes decide to behave correctly in monitoring process, they choose the strategy CC. Consequently, they get a payoff which is their gain from the successful contribution in monitoring process minus the required energy level necessary to perform monitoring tasks ($R - E$).

- When the regular and irregular nodes decide to act maliciously or selfishly, they choose the strategy IC. Consequently, they can get a payoff equals to their gain from the offered monitoring services minus the unachieved performance ($R-L$). Also, according to their behaviors, they can gain the desired reward minus the required energy level needed to perform monitoring tasks and their activities ($RO - E$).

- When the regular node decides to cooperate in monitoring process and the irregular one chooses the strategy IC, the expected gain for the regular node is $R - L - E$, whereas the expected gain for the irregular one is $R - L + H * (RO - E)$.

- When the regular node chooses the strategy IC and the irregular one decides to contribute legally in monitoring process, the expected gain for the irregular node is $R - L - E$, whereas the expected gain for the regular one is $R - L + H * (RO - E)$.

5.3 Evolutionary Stable Strategy (ESS)

As the studied game is a symmetrical one, we consider the same matrix of the profits as follows:

$$A= \begin{matrix} (1-s)*(R-E) & (1-s)*(R-L-E) \\ s*(R-L+H*(RO-E)) & s*(R-L+H*(RO-E)) \end{matrix}$$

We noticed:

- The obtained gains when the players choose the strategy CC is higher than those obtained when one player chooses the strategy CC and the others choose the strategy IC. Consequently, (CC, CC) is Nash equilibrium and CC constitutes an ESS.

- The obtained gains when the players choose the strategy IC is higher than those obtained when one player chooses the strategy CC and the others choose the strategy IC and in this case (IC, IC) is Nash equilibrium and IC constitutes an ESS.

5.4 Game dynamics

The game dynamics are used to assess the strategies evolution of participants over time periods. Every period, a participant may change its strategy to CC or IC depending on its benefits.

Let's consider P_{CC} be the probability to change to a CC strategy and P_{IC} be the probability to change to a IC one. $Pro = (nr, nir)$ where nr is the regular nodes proportion in the network, nir is the irregular nodes proportion in the network. As, in real world, it is not always possible to determinate the regular and irregular nodes proportion in MANET. Thus, we propose that each participating node calculates the nr and nir as the proportion of its regular and irregular neighbors respectively.

The formula of the replicator dynamic is defined as follows:

$$P_{CC}^{*} = P_{CC}[(A * Pro)_{CC} - Pro^{T} A * Pro] \tag{4}$$

$$P_{IC}^{*} = P_{IC}[(A * Pro)_{IC} - Pro^{T} A * Pro] \tag{5}$$

This system describes the replication process in continuous time. It presents the percentage of both regular and irregular players which will be considered as the next population.

$$\text{A*Pro} = \begin{matrix} (1-s)*(nr*L+R-L-E) \\ s*(R-L+H*(RO-E)) \end{matrix}$$

$$Pro^{T} A * Pro = \begin{matrix} (1-s)*(nr^{2}*L+nr*(R-L-E)) \\ (1-nr)*s*(R-L+H*(RO-E)) \end{matrix}$$

$P^*_{CC} =$

$$(1-s)*(R-L-E-nr^2*L-nr*E)+s*nr*(-L+H*(RO-E)) \quad (6)$$

By replacing nr by $1 - nir$, we obtain:

$$P^*_{IC} = (1-s)*(R-L-E-(1-nir)^2*L-(1-nir)*E)+$$

$$s*(1-nir)*(-L+H*(RO-E)) \quad (7)$$

6 SECURITY ENFORCEMENT

In the following, we define new security policies that specifies the participating nodes nature (regular or irregular nodes) in order to ensure efficient monitoring.

- In the case of policy-based monitoring, the administrator must distribute policies to all nodes (not only to monitors) to avoid monitors to falsify them.

- A selfish node must ensure and confirm the forwarding of packets containing a specific kind of data (alert, policies, etc.) by sending acknowledgment message to the sender.

- Excluding malicious nodes from the monitoring process is not always possible (all paths between monitors and monitored nodes can contain malicious nodes, neighbors can be malicious, etc.). Thus, a sender must encrypt its packets containing critical data, if it has malicious neighbors.

- A monitor can treat only limited number of requests to avoid denial of service attack.
- A malicious node cannot be allowed to perform local analysis or launch alarms.

In particular situations, monitors or monitored nodes may receive an unknown node in an alert form. For example, a volunteer at a disaster site could help a police officer who loses device there. This police officer can use the smart phone of a volunteer to send alerts to the corresponding monitor. We propose to assign to each trusted participant a random number indicating the number of messages to be sent to the appropriate monitors.

7 SIMULATION RESULTS

In this section, we discuss the experimental results, including the description of the selected parameters. Two sets of experiments are presented to assess the effectiveness of our improvements. First, we show the results obtained while evaluating the dynamic replicator effectiveness. Secondly, we deliver results while evaluating the validity of the proposed scheme.

7.1 Evaluation of the replicator dynamic

The replicator dynamic is implemented in order to obtain the proportion of mobile nodes contributing to the MANET monitoring through out simulations. All those simulations are conducted in a network made up of 500 nodes. The latter are initially randomly placed in a surface of $100m * 100m$ and may also move randomly in this zone.

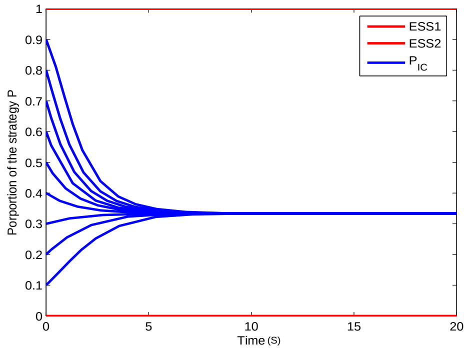


FIGURE 4
Convergence of the replicator dynamic with $R = 4$, $E = 1$ and $L = 3$

Figure 4 illustrates the convergence of the replicator dynamic of the strategy P_{IC} while varying the initial rate. The game parameters are then fixed as follows: $R = 4$, $E = 1$, $L = 3$, $H = 1$ and $RO = 2$.

Figure 5 shows the convergence of the replicator dynamic of the strategy P_{CC} while varying the initial rate and the parameters of the game. The increase of the reward R and L leads to the convergences of the replicator dynamic towards the stable strategies: $P^*_{CC} = 0$ and $P^*_{CC} = 1$.

Figure 5 [b] indicates that the convergence speed when $R = 5$ is larger compared to the case described in figure 5 [a]. In fact, the mobile nodes proportion that choose the strategy P_{CC} increases due to an important reward that incites the mobile nodes to adopt the strategy P_{CC} quickly.

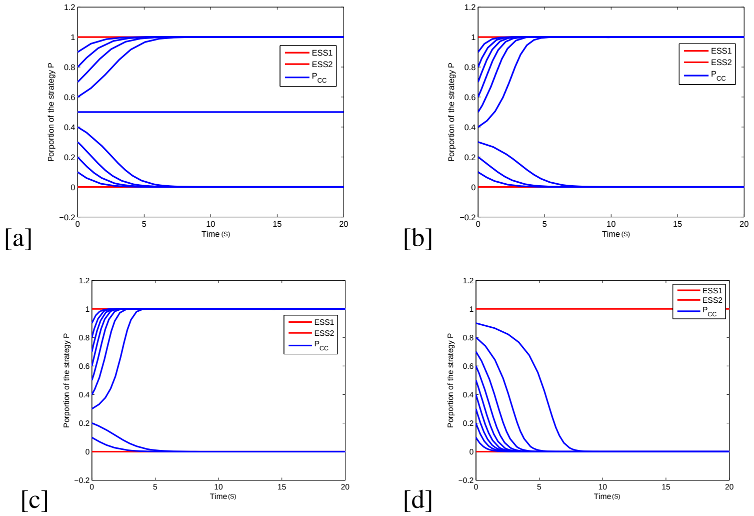


FIGURE 5
Convergence of the replicator dynamic [a] $R = 3$, $E = 1$ and $L = 2$ [b] $R = 5$, $E = 2$ and $L = 4$ [c] $R = 5$, $E = 1$ and $L = 4$ [d] $R = 5$, $E = 2$ and $L = 2$

Furthermore, when the value of L is increased (see figures 5 [b] and 5 [c]), the replicator dynamic convergences are much larger in the comparing with the instance of the reward. This is due to the fact that the mobile nodes are encouraged to participate when the risks related to the losses are important.

Figure 5 [d] demonstrates that an increase in the values of E and R leads to the convergences of the replicator dynamic towards the strategy $P^*_{CC} = 0$. Thus, all the mobile nodes end up choosing the same strategy P_{CC}.

Parameters	**Values**
Duration	5000s
Number of nodes	100
Territory scale	$100m^2$
Range of node	20
Mobility model	Random WayPoint
Pause interval	[0, 20](s)
speed interval	[0, 20](m/s)

TABLE 3
Simulation parameters

7.2 Evaluation of the proposed scheme

To study the effectiveness of our scheme, we compare it with the cluster-based and CDS-based architectures (as shown in figure 2). We use the same metric, as our approach, to elect cluster-heads and dominator nodes. We assume that $RS(n_i) = COF2 * EC(n_i)$ where $COF1 = COF2 = 0.5$ and $EC(n_i)$ indicates the remaining energy level of the node n_i. We also assume that the necessary energy for performing a given monitoring task, the mobile node trust value and remaining energy level are randomly selected from the range $[0, 1]$ following a uniform distribution.

The simulation settings and parameters are listed in table 3.

7.3 Simulation results and analysis

Figure 6 indicates the number of the exchanged messages in order to construct topologies through time. From the results, we can observe that our scheme outperforms the cluster and CDS based architectures by attaining low message overhead. This explains that only regular nodes can perform the

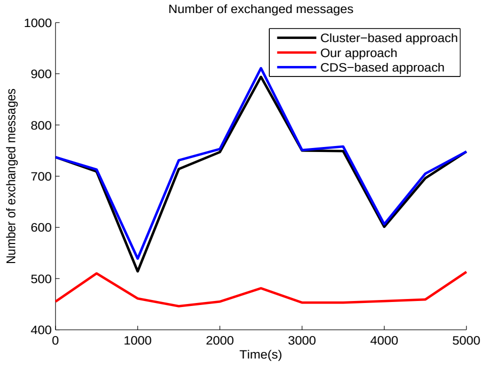


FIGURE 6
Number of exchanged message

monitoring plan.

Figure 7 illustrates the evolution of the irregular monitors detection rate through time. The results indicate that an important detection rate of our scheme. This is interpreted by the fact that in CDS-based architecture, regular monitors can be isolated and consequently, cannot detect the malicious or selfish behaviors of irregular ones.

Figure 8 shows that our scheme decreases the number of the excluded regular monitors compared to CDS-based architecture.

We also measure the maintenance time of both our scheme and CDS-based architecture through time. The obtained results (see figure 9) demonstrate that our scheme can reduce this criterion. This is interpreted by the fact that our scheme allows the replacement of any detected irregular monitor with one of

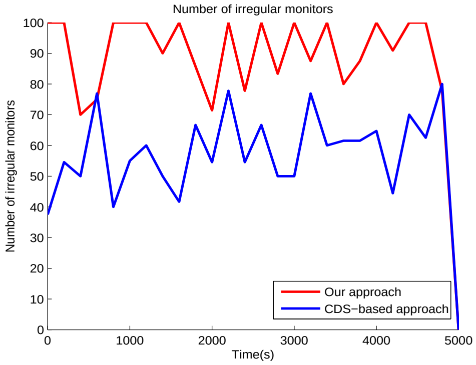


FIGURE 7
Number of detected irregular monitors

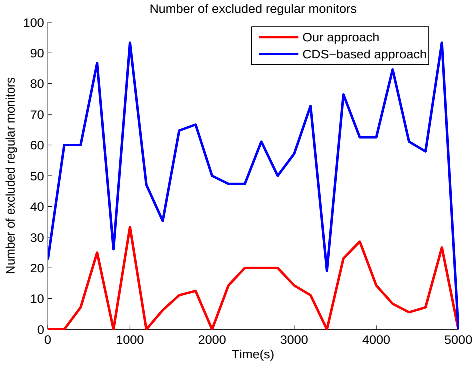


FIGURE 8
Number of excluded regular monitors

its regular neighbors.

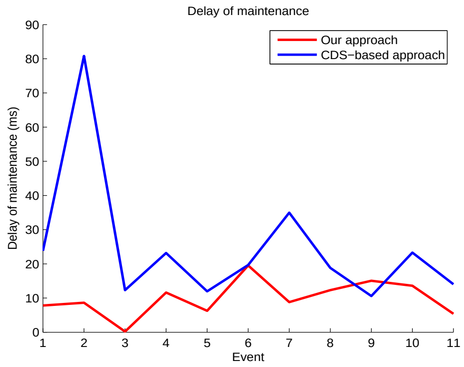


FIGURE 9
Time of maintenance

8 DISCUSSION

In the following, we analyze our approach reliability against some management requirements:

1. Our network monitoring approach is robust. This is due to the absence of a single point failure [5]. When a monitor disconnects or moves, the monitoring activity will not stop. An irregular monitor or a disconnected monitor may be replaced by one of its regular neighbors.

2. It integrates a monitoring election mechanism that selects monitors based on their behaviors and resources.

3. It balances the resource consumption and monitoring tasks among the participating nodes that can extend the overall lifetime.

4. It is scale as it allows the control of a mobile ad hoc network composed

of thousands of mobile nodes.

5. It can decrease the overhead in order to construct/reconstruct monitoring structure as only regular nodes can participate in this task.

6. In the presence of delegated monitors, the proposed scheme may neither generate any extra cost (additional complex computation) to reconstruct the monitoring architecture nor to elect new monitors. It also reduces the time between either the detection of any irregular monitor or the disconnection of any regular monitor, and the election of a new one.

Nevertheless, the robustness and the effectiveness of our approach depend on:

- the node's neighbors honesty and participation rate : a regular participant can be easily excluded if at least a half of its neighbors are irregular nodes. Consequently, the monitoring system taken decision might be incorrect, inaccurate or inappropriate.

- Nodes' resources: mobile nodes usually have limited resource capabilities that directly affect our approach performance. The regular nodes die faster when irregular ones exist in the network, as the same node may be elected as monitor repeatedly.

- Link quality: a regular node can be considered as irregular due to problems in the communication with its neighbors such as congestion.

We also note that some security services are not considered by our approach such as:

- Authentication: the absence of any authentication technique allows irregular nodes to rejoin the network as new participants with new identities. Those nodes may also replace involuntary disconnected monitors.
- Privacy and confidentiality: any malicious node may intercept and easily replay or falsify the trust values or nodes identities.

In addition, the values of the following parameters must be regarded:

- The chosen changing step: the trust value of any participant must be decreased by a value α according the generated damages.
- The timeout period Tb must be determinated considering the nodes' behaviors.

9 CONCLUSION AND FUTURE WORK

The effectiveness of monitoring in MANET depends on the correct contribution rate of the participating nodes as well as their resources. It is therefore essential that most nodes, if not all, participate in the monitoring plan. Although participating in this process enhances network performance, it affects participants' reliability and lifetime (they lose their limited critical resources such as battery power, bandwidth, storage space, etc.). Mobile nodes can, in fact, take on either regular or irregular roles. An irregular node attempts to increase its own utility while reducing the overall network utility, while a regular one ensures monitoring tasks to enhance MANET's performance and benefit from monitoring services. Monitoring the behavior of each mobile is therefore an essential requirement for developing a robust and reliable monitoring approach. In this paper, we propose to choose only good behavior and honest nodes as monitors. We select monitors based on a weighing factor that uses the trust value. The latter is measured using the contribution rate in the participants and their neighbors' monitoring process. However, irregular nodes can try to avoid being detected by hiding as regular nodes, providing a proper network functioning either for a period of time or in specific situations. Then they act maliciously or selfishly to either disrupt the measurements and decisions of the monitoring system or preserve their critical resources. We are therefore proposing a new scheme in which monitoring and monitoring nodes are controlled by their regular neighbours. Compared to cluster-based and CDS-based architectures, we evaluated the performance of this scheme. The results obtained demonstrate the effectiveness of our scheme in terms of the number of messages exchanged, the excluded regular monitors and the detected irregular monitors. The proposed scheme also reduces maintenance time. We also propose an evolutionary model based on game theory that assists a participant node to make appropriate decisions about its contribution, especially if it has limited and shared resources. We analyzed the achieved Nash equilibrium for the correct / incorrect contribution and implemented the replicator dynamic to allow a player to adapt behavior as the game runs. The reliability analysis of our approach against some management requirements shows that the proposed improvements can ensure effective monitoring by minimizing some damage caused by participants' irregular behaviors while maintaining robust monitoring without incurring high communication costs.

We believe that these improvements are necessary in particular in areas such as military, emergency and rescue domains. However, some of the concerns mentioned in section 8 have not been resolved and must be addressed in future work. For instance, in our future work we plan to take into consideration the link quality, authentication, the chosen changing step, the timeout period in funtion of nodes behaviors, etc. Furthermore, as we randomly generate some system parameters as trust value and energy, we investigate the implementation of the predefined rules while specifying the measurement of those parameters. We also plan to consider human behavior and social factors in order to calculate trust value.

REFERENCES

[1] Dharma P Agrawal and Qing-An Zeng. (2015). *Introduction to wireless and mobile systems*. Cengage learning.

[2] Hani Alzaid, Manal Alfaraj, Sebastian Ries, Audun Jøsang, Muneera Albabtain, and Alhanof Abuhaimed. (2013). Reputation-based trust systems for wireless sensor networks: A comprehensive review. In *IFIP International Conference on Trust Management*, pages 66–82. Springer.

[3] G. Ateniese, C. Riley, and C. Scheideler. (Sept. 2006). Survivable Monitoring in Dynamic Networks. *IEEE Transactions on Mobile Computing*, 5:33–47.

[4] R. Badonnel, R. State, and O. Festor. (April 2006). Probabilistic management of ad-hoc networks. In *2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006*, pages 339–350, Vancouver, Canada.

[5] R. Badonnel, R. State, and O. Festor. (2007). *Management of Ad-Hoc Networks*. Handbook of Network and System Administration.

[6] Z. Bankovic, J. C. Vallejo, D. Fraga, and J. M. Moya. (2011). Detecting bad-mouthing attacks on reputation systems using self-organizing maps. In *in: Proceedings of the* 4^{th} *International Conference on Computational Intelligence in Security for Information Systems, in:CISIS-11, Springer Verlag, Berlin, Heidelberg*, pages 9–16.

[7] N. Battat, H. Seba, and H. Kheddouci. (2014). Monitoring in mobile ad hoc networks: A survey. *Computer Networks*, 69:82–100.

[8] Nadia Battat and Hamamache Kheddouci. (2011). Hman: Hierarchical monitoring for ad hoc network. In *2011 IFIP 9th International Conference on Embedded and Ubiquitous Computing*, pages 414–419. IEEE.

[9] M. S. Bouassida, I. Chrisment, and O. Festor. (2008). Group key management in MANETs. *International Journal of Network Security*, 6(1):67–79.

[10] Wenli Chen, Nitin Jain, and Suresh Singh. (1999). Anmp: Ad hoc network management protocol. *IEEE Journal on selected areas in communications*, 17(8):1506–1531.

[11] Y.H. Cheng, A. Ghosh, R. Chadha, and G. Hadynski. (2010). Managing network security policies in tactical MANETs using DRAMA. In *MILCOM, Military Communications Conference*, pages 960–964.

[12] Véronique Cortier, Jérémie Detrey, Pierrick Gaudry, Frédéric Sur, Emmanuel Thomé, Mathieu Turuani, and Paul Zimmermann. (2011). Ballot stuffing in a postal voting system. In *2011 International Workshop on Requirements Engineering for Electronic Voting Systems*, pages 27–36. IEEE.

[13] Herbert Gintis. (2000). *Game theory evolving: A problem-centered introduction to modeling strategic behavior*. Princeton university press.

[14] K. Gopalakrishnan and V. R. Uthariaraj. (2011). Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad Hoc Networks. *European Journal of Scientific Research*, 57(3):411–425.

[15] Y. K. Hassan, M. H. A. El-Aziz, and A. S. A. El-Radi. (2010). Performance evaluation of mobility speed over MANET routing protocols. *International Journal of Network Security*, 11(3):120–138.

[16] Jean-Pierre Hubaux, Levente Buttyán, and Srdan Capkun. (2001). The quest for security in mobile ad hoc networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 146–155. ACM.

[17] Mojtaba Jamshidi, Milad Ranjbari, Mehdi Esnaashari, Aso Mohammad Darwesh, and Mohammad Reza Meybodi. (2019). A new algorithm to defend against sybil attack in static wireless sensor networks using mobile observer sensor nodes. *Ad Hoc & Sensor Wireless Networks*, 43(3-4):213–238.

[18] Hanif Kazemi, George Hadjichristofi, and Luiz A DaSilva. (2008). Mman-a monitor for mobile ad hoc networks: design, implementation, and experimental evaluation. In *Proceedings of the third ACM international workshop on Wireless network testbeds, experimental evaluation and characterization*, pages 57–64. ACM.

[19] A. Malatras, A. M. Hadjiantonis, and G. Pavlou. (March 2007). Exploiting Context-Awareness for the Autonomic Management of Mobile Ad Hoc Networks. *Journal of Network and Systems Management*, 15:29–55.

[20] Ola Malawi and Mohammad Obaidat. (2018). Mitigating the effect of blackhole attack on manets using aodv protocol under transmission control protocol. *Adhoc & Sensor Wireless Networks*, 42.

[21] C. Murthy and B. Manoj. (2004). Ad Hoc Wireless Networks: Architecture and Protocols. *Prentice Hall*.

[22] Cristian Popi and Olivier Festor. (2008). A scheme for dynamic monitoring and logging of topology information in wireless mesh networks. In *NOMS 2008-2008 IEEE Network Operations and Management Symposium*, pages 759–762. IEEE.

[23] Marjan Kuchaki Rafsanjani and Ali Movaghar. (2008). Identifying monitoring nodes with selection of authorized nodes in mobile ad hoc networks. *World Applied Sciences Journal*, 4(3):444–449.

[24] Krishna N Ramachandran, Elizabeth M Belding-Royer, and KC AImeroth. (2004). Damon: A distributed architecture for monitoring multi-hop mobile networks. In *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.*, pages 601–609. IEEE.

[25] Malihe Saghian and Reza Ravanmehr. (04 2019). Efficient qos-aware middleware for resource discovery in mobile ad hoc networks. *Ad Hoc & Sensor Wireless Networks*, 43:283–312.

[26] Chien-Chung Shen, Chaiporn Jaikaeo, Chavalit Srisathapornphat, and Zhuochuan Huang. (2002). The guerrilla management architecture for ad hoc networks. In *MILCOM 2002. Proceedings*, volume 1, pages 467–472. IEEE.

[27] W. Stallings. (2003). *Cryptography and Network Security*. Prentice-Hall, 4^{th} Edition.

[28] Yan Lindsay Sun, Zhu Han, Wei Yu, and KJ Ray Liu. (2006). Attacks on trust evaluation in distributed networks. In *2006 40th Annual Conference on Information Sciences and Systems*, pages 1461–1466. IEEE.

[29] C. Toh. (2002). Ad Hoc Mobile Wireless Networks: Protocols and Systems. *rentice-Hall, New York*.

[30] X. Xu, X. Gao, J. Wan, and N. Xiong. (27 June 2011). Trust Index Based Fault Tolerant Multiple Event Localization Algorithm for WSNs. *Sensors*, 11:6555–6574.

[31] Zhou Yanping, Jin Yuehui, Cui Yidong, and Que Xirong. (2009). The reasearch of hierarchy model for ad hoc network monitoring based on clustering. In *2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology*, pages 276–280. IEEE.