Journal of Computer and Communications, **2014, 2, 1-10**
Published Online February 2014 (http://www.scirp.org/journal/jcc)
http://dx.doi.org/10.4236/jcc.2014.23001

Distributed and Cooperative Anomaly Detection Scheme for Mobile Ad Hoc Networks

Hisham Mustafa[1,2], Yan Xiong[2], Khalid Elaalim[1,2]

[1]Department of Statistic and Computer Sciences, Faculty of Applied Sciences, Red Sea University, Port Sudan, Sudan; [2]School of Computer Science and Technology, University of Science and Technology of China, Hefei, China.
Email: hisham@mail.ustc.edu.cn, yxiong@ustc.edu.cn, osman64@mail.ustc.edu.cn

Received December 31st, 2013; revised January 25th, 2014; accepted February 3rd, 2014

ABSTRACT

Due to their unique characteristics, such as the dynamic changing topology, the absence of central management, the cooperative routing mechanisms, and the resources constraints, Mobile ad hoc networks (MANETs) are relatively vulnerable to both active and passive attacks. In MANET, routing attacks try to disrupt the functions of routing protocol by intentionally or unintentionally dropping packets or propagating faked routing messages. However, due to their computation requirements, the prevention mechanisms are not powerful enough to secure MANET. In this paper, we propose a distributed and cooperative scheme using statistical methods to detect routing attacks in MANETs. Our scheme uses both direct and indirect observations to characterize the behaviors of both neighboring and remote nodes. Simple threshold and *Grubb's Test* are utilized to propose our new detection methods. The scheme includes innovative methods to compute our proposed measures, Maximum Accusation Number (MAN) and Accusation Number (AN), which are used to make decision about node's behavior. Experimental results show that our scheme performs well in detecting anomalous events in routing functions.

KEYWORDS

MANET; Routing Protocol; Routing Attacks; Anomaly Detection; Trust and Availability; Statistical Test

1. Introduction

Mobile Ad hoc Network (MANET) consists of a group of mobile nodes communicating over shared wireless links with no central management point. However, the nodes in MANET are mobile, so the topology may change rapidly over time, which as a result, may add more burdens to the node and whole network. The nature of mobility creates new vulnerabilities that do not exist in a fixed wired network, and yet many of the proven security measures turn out to be ineffective [1]. In addition, mobile nodes are usually limited-resource devices, such as energy, storage, bandwidth, and computational power, and therefore, the expensive security solution is no longer appropriate for MANETs.

Generally, wireless networks are highly susceptible to passive attacks, such as the eavesdropping of secure information, and active attacks, such as impersonation, message delay, message distortion, and denial of service (DoS) [2]. MANET, as a particular type of wireless networks, is relatively vulnerable for attacks that threaten its basic functions (*i.e.*, routing and packets forwarding). Because of its unique characteristics, such as wireless open medium, dynamic changing topology, absence of central management, cooperative routing mechanisms, and resource constraints, MANET protocols could be threatened by both passive and active attacks [3]. In passive attack (the attacker referred as selfish), the node does not intentionally harm the network, but in order to save its battery life, it does not cooperate with others in carrying out basic functions, such as routing and packets forwarding, which as a result, could endanger the correct execution of routing functions or even segment the MANET. In active attack (the attacker referred as malicious), the attacker intentionally misbehaves to sabotage the network operation by performing harmful operations such as dropping packets, modifying or fabricating routing information, and/or impersonating other's identities, which as a result, could disrupt the node's operation, and hence, degrade the performance of the whole MANET.

The prevention mechanisms that rely on cryptographic methods were used to protect the basic functions of MANETs. However, studies such as [1] have proved that the intrusion prevention mechanism is not powerful enough to secure MANET, because of its limitations such as the computation requirements that cause considerable resources consumptions (e.g. energy and storage resource). However, to secure MANET, two security approaches are used: an approach to design secure protocol and an approach to design an intrusion detection system (IDS). In recent years, IDSs are used in MANET to cope with the limitations of intrusion preventive mechanisms, in addition, to serve as a detection and reaction mechanism against both passive and active attacks. IDSs can be classified based on the detection method into two basic types: misuse-based detection method and anomaly-based detection method [4]. The misuse detection system uses known attack patterns (signatures) to recognize the known attacks, and therefore, it fails to identify the unknown attacks. The anomaly detection system learns from the normal data and builds a model to describe the normal behavior, and thus, an event is considered to be anomalous if the difference between audit data and the model of normal behavior exceed a certain threshold.

In this paper, we propose a fully distributed and cooperative scheme using statistical methods to detect routing attacks in MANETs. In order to characterize the behaviors of both neighboring and remote nodes, our proposed scheme uses both direct observations and the indirect observations that are provided by other nodes. Simple threshold and *Grubb's Test* are utilized to propose our new methods that are to analyze audit data and hence to detect anomalous events. The rest of the paper is organized as follows. Section 2 discusses the related works briefly, and then we present detailed descriptions of our proposed scheme in Sections 3 and 4. Section 5 discusses the experiments setups and results. Last, conclusion and future work are presented in Section 6.

2. Related Work

In recent years, a lot of work has been done in anomaly detection. However, the main challenge of IDS researches in MANET is that, with the absence of central trust management, the basic functions rely on cooperation between neighbor nodes. Thus, Zhang *et al*. proposed in [1] that intrusion detection systems in MANETs should be both distributed and cooperative, due to the fact that MANET's nature is distributed and its basic functions require the cooperation of all participated nodes. In this architecture, the node has IDS agent collects and analyzes data to detect intrusions and then initiates the proper response. The distributed and collaborative architecture of IDS based on mobile agents is also used in [5] by implementing a Local Intrusion Detection System (LIDS) on every node for local concerns, which can cooperate with other's LIDS for global concerns.

However, statistical-based approaches have been widely used to detect anomalous. The approach presented in [6] uses various features and captures the basic view of network topology and routing operations to detect anomaly by using statistical method. Also, the system uses several identification rules to identify the type of attack and attacker node. Meanwhile, Kruus *et al*. [7] used the path delay data to detect wormhole attack, where the path is considered as a subject of attack if its delay time exceeds a pre-defined threshold. The path delay feature is also utilized in [8] to detect an in-band wormhole attack by using the Sequential Probability Ratio Test (SPRT) and the non-parametric methods.

To detect misbehaved nodes, Marti *et al*. in [9] proposed two techniques, Watchdog and Pathrater. Watchdog is a simple agent to identify the misbehaving nodes by eavesdropping on the transmission of the next hop. Pathrater helps node to find the routes that do not contain misbehaviors. Generally, the two techniques are quite effective for choosing secure paths that can improve MANET's throughput. CONFIDANT [10] is proposed as an extension to DSR protocol to detect misbehaviors and enforce cooperation among nodes. In this approach, misbehaved nodes are punished, and moreover, warning messages are sent to all trusted nodes, but, without any encouragement for the well-behaved nodes. Michiardi *et al*. proposed CORE [11], based on both direct and indirect reputation information, to detect misbehaviors and enforce cooperation among nodes. Where, the misbehaved nodes are prevented from the network services. The node in CORE has Watchdog component to monitor its neighbor's activities. In this mechanism, a reputation table is established and updated based on the information generated by Watchdog component.

Overall, most of the proposed approaches share some critical concerns that still need to be solved. That is, some of the proposed approaches do not propose any deterrent or punishment that can enforce or encourage the misbehaved node to behave well. However, some of them provide the same level of services for all well-behaved nodes. Therefore, with no rewarding; the well-behaved nodes might tend to behave selfishly. Moreover, malicious node by propagating faked security information might disrupt the correctness of anomaly detection (*i.e.*, increase the false rate). In this paper, we aim to address those critical concerns by introducing new statistical-based methods to detect anomalous events in routing functions that utilizing both direct and indirect observations. Although the response of attacks has not been considered much in the literature for MANETs, but we delay it to our future works.

3. The Proposed Scheme

In our proposed solution, the deviation in path delay is utilized to detect suspected nodes, because of the fact that, the existence of misbehaviors on a path causes a noticeable deviation in some of the path characteristics, which can easily be detected by using statistic methods. Based on the findings of path delay analysis, the monitored nodes will preliminarily be classified. However, the behavior of suspected nodes will further be verified based on direct and indirect observations.

For each neighbor, behavior metrics are evaluated based on direct observations and further verified based on indirect observations. Meanwhile, the behavior metrics of the remote nodes (*i.e.*, non-neighbor nodes) are evaluated by utilizing the indirect information that provided by their neighboring monitors. However, the indirect information from different monitor nodes are filtered and evaluated based on its source behavior. For each monitored node, the behavior metrics will be used to compute and update the Maximum Accusation Number (MAN) and the Accusation Number (AN), which are compared to characterize nodes' behaviors.

In order to achieve fully distributive and cooperative anomaly detection, the concept of IDS-agent in [1] is developed and utilized in our proposed scheme (see **Figure 1**). The node in our scheme has an IDS-agent that is responsible for specific tasks. The agents of different nodes cooperate and exchange monitoring information in a way that reduces the consumption of computational and energy power that required by each node. Each agent performs the following basic tasks:

- collects audit data (path delay time, packets counts and statistics, and behavior metrics)
- analyzes data and detects any anomalous event
- establishes *Monitoring Table* to maintain the security related information
- shares behavior metrics of all 1-hop neighbors
- make decision of node behavior

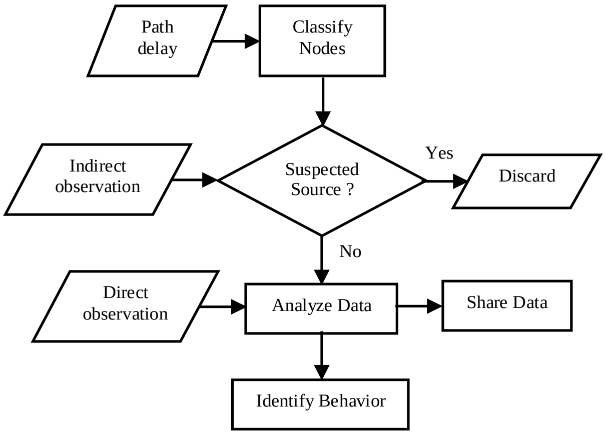


Figure 1. Diagram of our proposed scheme.

The proposed scheme makes use of path delay data, direct and indirect observations. The path delay data is used to decide whether a monitored node is located on an abnormal path or no. Then, based on the path classification, the node is classified as normal or suspected. However, the direct and indirect observations are aggregated and used to evaluate the behavior metrics of all monitored nodes (*i.e.*, characterize node's behavior). To obtain path delay data, each monitor node periodically broadcasts ping and collects the delay time *d* of each path that reply within *t* seconds. However, the direct observations are obtained by monitoring 1-hop nodes and gathering counts and statistics of packets traffic (*i.e.*, the received and forwarded packets). Meanwhile, the indirect observations are gathered from the security information that computed and provided by other trusted monitors.

The findings of data analysis are used to update existing records in the *Monitoring Table* (see **Table 1**) or to create a new record for the unforeseen node. However, our proposed scheme assumes that each node in MANET has a unique and distinct identifier (ID). The reasons behind this assumption are; in the normal situations none of the nodes have ability to distinguish true and fake identities. In addition to, the only perfect method that can protect MANET from the threats of identity spoofing is the cryptographic-based mechanism, which is not of interest in this paper. We expect that, maintaining the information of nodes behavior uses up some storage at the monitor node.

However, by gathering indirect observations from different source nodes, the anomaly detector might faced by inconsistent information about the behavior of one monitored node. In addition to, due to the indirect observa-

Table 1. Monitoring Table Fields.

Field	Description
Node_ID	node identifier
tr_ratio	trust ratio of node
av_ratio	availability ratio of node
Node_CHR	node characteristic based on trust and availability
MAN	maximum accusation number of node
AN	accusation number of node
Node_BHR	node behavior based on accusation number

tions are more vulnerable than direct observations, the malicious nodes might degrade the anomaly detection rate by propagating faked behavior information, moreover, the message that routed by a malicious node might be modified or deleted. In order to address the concerns mentioned above and hence to decrease their negative effects, our scheme introduces procedures that are to filter and evaluate the indirect observations.

4. Anomaly Detection and Behavior Identification

4.1. Detecting Anomalies in Path Delay

Our proposed scheme makes use of threshold to determine whether the path delay is outside the range of normal values. According to the *Central Limit Theorem*, we suppose that the path delay, which is a sum of large number of node delays, have a distribution much like a Normal. Then, based on the statistical 3σ*_rule* [12], more than 99.7% of the normal path delays should be in the range $[0, \mu_D + 3\sigma_D]$, where μ_D and σ_D are the mean and the standard deviation of path delay data set D, respectively. Thus, according to this rule, our threshold (*THD*) is defined as the upper limit of range $[0, \mu_D + 3\sigma_D]$ (*i.e.*, the delay that exceed $\mu_D + 3\sigma_D$ is considered anomalous).

The delay data are tested using *THD* to detect anomalous delays. The findings of this test are used to classify the monitored path as either normal or abnormal, and accordingly, the nodes located on this path will classify as normal or suspected. We believe that, the preliminary classification of remote nodes would reduce the possibility of false accusation for node that located on a path considered normal. Table 2 illustrates our proposed procedure to detect anomalous delays and to classify nodes, based on the following steps:

Step (1): the threshold is computed as:

$$THD = \mu_D + 3\sigma_D \tag{1}$$

where, μ_D and σ_D are calculated using the delay set $\{d_p\}$; $p \in \{path\}$, of size N as:

$$\mu_D = \frac{1}{N} \sum_{p\in\{path\}} d_p \tag{2}$$

$$\sigma_D = \sqrt{\frac{1}{N} \sum_{p\in\{path\}} \left(d_p - \mu_D\right)^2} \tag{3}$$

then, d_p (*i.e.*, the delay of path p) is declared to be anomalous if d_p is greater than *THD*, otherwise normal.

Step (2): path with normal delay is classified as normal (*i.e.*, *Path_CLS*: = "*normal*"), otherwise is classified as abnormal (*i.e.*, *Path_CLS*: = "*abnormal*"). However, node that fails to reply ping within *t* seconds (without any link failure notification) is classified as suspected. Where *t* is defined, based on the delay data in the last time period, as the mean of path delay data set (μ_D) plus its standard deviation (σ_D).

Table 2. Node Classification.

```
Procedure Node_Classification ()

Input   $d_p$ : path delay;
Output   normal or suspected;

Begin

Broadcasts ping;
if (no ping reply within t seconds)
        Path_CLS$_p$ := "abnormal";

*/ compute threshold (THD) using all available $d_p$ as /*
THD = $\mu_D + 3\sigma_D$;

for p∈{path}
{
        if ($d_p$ > THD)          */ $d_p$ is anomalous /*
                Path_CLS$_p$ := "abnormal"
        else
.               Path_CLS$_p$ := "normal";
} */ end for p /*

for i∈{monitored}
{
            for p∈{path}
            {
                        Node_CLS$_i$ := "normal";
                        if (Path_CLS$_{ip}$ = "abnormal ")
                        {
                                    Node_CLS$_i$ := "suspected";
                                    goto end for p;
                        }
            } */ end for p /*
 } */ end for i /*

End.
```

Step (3): node i is classified as a suspected node (*i.e.*, *Node_CLS$_i$*: = "*suspected*") if it is located at least on one abnormal path, where, *Path_CLS*$_{ip}$ is the classification of path *p* that includes node i. Note that, the new node is assumed to behave well (*i.e.*, *Node_CLS* is initiated as "normal"), unless it is located on an abnormal path.

4.2. Detecting Anomalies in Direct and Indirect Observations

According to the assumption of anomaly detection approaches that, the anomalous activity usually causes significant changes in the traffic features that can be detected by using statistical tests. However, our proposed scheme makes use of the counts of both forwarded and received packets to compute the behavior metrics, *tr_ratio* and *av_ratio*, for each monitored node. *tr_ratio* is used to evaluate node's trustworthiness, meanwhile, *av_ratio* is used to represent node's availability for both routing and packet forwarding purposes. However, the direct and indirect observations are aggregated and evaluated to produce two weighted average vectors. In statistic, there are many techniques to detect anomalous. For our proposed method, we make use of the statistical *Grubbs*' *Test* to detect anomalous of *tr_ratio* and *av_ratio*. Grubbs' Test is a statistical test used to detect anomalies in a univariate data set under the assumption that the data are generated by a normal distribution [13]. According to the *Central Limit Theorem* we suppose that, *tr_ratio* and *av_ratio* have a distribution much like a Normal. Due to, *tr_ratio* and *av_ratio* of each node is defined as a sum of large number of *tr_ratio* and *av_ratio*, respectively. **Table 3** illustrates our proposed procedure to characterize node's behavior, based on the following steps:

Table 3. Behavior Characterization.

```
Procedure Behavior_Characterization ()

Input  tr_ratio$_{ij}$ : trust rate of node i in the view of node j;
       av_ratio$_{ij}$ : availability  rate of node i in the view of node j;
Output  suspected and normal;

Begin

*/filter data and update the weighted-average vectors/*
for i$\in${monitored}
{
    sum_tr_monitored := 0;  sum_av_monitored := 0;
    sum_tr_monitor := 0;  sum_av_monitor := 0;
    for j$\in${monitor}
    {
        if  (Node_CLS$_j$ $\neq$ "suspected")   */ trusted source/*
        {
            tr_ratio[i,j] := tr_ratio$_{ij}$;  */ accepted /*
            av_ratio[i,j] := av_ratio$_{ij}$;  */ accepted  /*
            sum_tr_monitored = + tr_ratio[i,j]*tr_ratio$_j$;
            sum_av_monitored = + av_ratio[i,j]*av_ratio$_j$;
            sum_tr_monitor = + tr_ratio$_j$;
            sum_av_monitor = + av_ratio$_j$;
        }
        else
            discard tr_ratio$_{ij}$ and av_ratio$_{ij}$;
    }  */ end for j /*
    tr_ratio[i] :=  sum_tr_monitored / sum_tr_monitor;
    av_ratio[i] :=  sum_av_monitored / sum_av_monitor;
} */ end for i /*

*/ compute the test statistics s$_{tr}$ and s$_{av}$ /*
$s_{tr} = \left( \left( N_{tr} - 1 \right) \big/ \sqrt{N_{tr}} \right) \sqrt{ t^2_{\alpha/(2N_{tr}), N_{tr}-2} \Big/ \left( N_{tr} - 2 + t^2_{\alpha/(2N_{tr}), N_{tr}-2} \right) }$ ;
$s_{av} = \left( \left( N_{av} - 1 \right) \big/ \sqrt{N_{av}} \right) \sqrt{ t^2_{\alpha/(2N_{av}), N_{av}-2} \Big/ \left( N_{av} - 2 + t^2_{\alpha/(2N_{av}), N_{av}-2} \right) }$ ;

*/characterize node's behavior/*
for i$\in${monitored}
{
    */ compute the test standards ztr$_i$ and zav$_i$ /*
    ztr$_i$ = ( |tr_ratio$_i$ – µ$_{tr}$| ) / σ$_{tr}$ ;
    zav$_i$ = ( |av_ratio$_i$ – µ$_{av}$| ) / σ$_{av}$ ;
    */ characterize the node behavior /*
    if  ( (ztr$_i$ > s$_{tr}$) AND ( zav$_i$ > s$_{av}$) )
        Node_CHR$_i$ := "suspected"
    else
        Node_CHR$_i$:= "normal";
} */ end for i /*

End.
```

Step (1): *tr_ratio*$_i$, as in (4), is calculated as the ratio of all packets forwarded by node i to all packets received by node i, whereas, *av_ratio*$_i$ is calculated as the ratio of all packets forwarded by node i to the average of packets forwarded by all neighbor nodes, as in (5).

$$tr\_ratio_i = \frac{Num.\ packets\ forwarded\ by\ node\ i}{Num.\ packets\ received\ by\ node\ i} \quad (4)$$

$$av\_ratio_i = \frac{Num.\ packets\ forwarded\ by\ node\ i}{Av.\ packets\ forwarded\ by\ all\ neighbors} \quad (5)$$

Step (2): if the difference between the current and previous value exceeds its average in the last time period (*i.e.*, $\left|\Delta tr\_ratio_i\right| > \mu_{tr}$ OR $\left|\Delta av\_ratio_i\right| > \mu_{av}$), then the current values of *tr_ratio*$_i$ and *av_ratio*$_i$ are propagated via the Route Replay (RREP) packets, which are uni-casted packets. However, by using this simple mechanism to share information, our proposed solution may introduce low communication overhead.

Step (3): the behavior information, *tr_ratio*$_{ij}$ and *av_ratio*$_{ij}$; $i \in \{monitored\}$, $j \in \{monitor\}$, and $i \neq j$, are evaluated based on the behavior of node j's (*i.e.*, the source nodes). Sometimes, due to a selfish behavior of node j or that node i and node j are not neighbors, *tr_ratio*$_{ij}$ and *av_ratio*$_{ij}$ might be missed. However, *tr_ratio*$_{ij}$ and *av_ratio*$_{ij}$ are accepted if and only if node j is not classified as suspected. The accepted information {*tr_ratio*$_{ij}$} and {*av_ratio*$_{ij}$} are weighted, using (6) and (7), to update the vectors {*tr_ratio*$_i$} and {*av_ratio*$_i$}; i$\in${monitor}, respectively. Note that, if node j is the IDS-host itself, then *tr_ratio*$_j$ = *av_ratio*$_j$ = 1 (*i.e.*, the direct observations are weighted by 1).

$$tr\_ratio_i = \sum_{j \in \{monitor\}} \left(tr\_ratio_{ij} * tr\_ratio_j \right) \Big/ \sum_{j \in \{monitor\}} tr\_ratio_j \quad (6)$$

$$av\_ratio_i = \sum_{j \in \{monitor\}} \left(av\_ratio_{ij} * av\_ratio_j \right) \Big/ \sum_{j \in \{monitor\}} av\_ratio_j \quad (7)$$

Step (4): the anomalous activity of node i is detected as following:

First, for each monitored node, the test standards *ztr*$_i$ and *zav*$_i$ of *tr_ratio*$_i$ and *av_ratio*$_i$, respectively, are computed as:

$$ztr_i = \left| tr\_ratio_i - \mu_{tr} \right| \big/ \sigma_{tr} \quad (8)$$

$$zar_i = \left| av\_ratio_i - \mu_{av} \right| \big/ \sigma_{av} \quad (9)$$

where, μ_{tr} and σ_{tr} are the mean and the standard deviation of {*tr_ratio*$_i$}, respectively, and, μ_{av} and σ_{av} are the mean and the standard deviation of {*av_ratio*$_i$}, respectively.

Second, for each {*tr_ratio*$_i$} and {*av_ratio*$_i$}, a test statistic s_{tr} and s_{av}, respectively, is computed as:

$$s_{tr} = \frac{N_{tr}-1}{\sqrt{N_{tr}}}\sqrt{\frac{t^2_{\alpha/(2N_{tr}),N_{tr}-2}}{N_{tr}-2+t^2_{\alpha/(2N_{tr}),N_{tr}-2}}} \quad (10)$$

$$s_{av} = \frac{N_{av}-1}{\sqrt{N_{av}}}\sqrt{\frac{t^2_{\alpha/(2N_{av}),N_{av}-2}}{N_{av}-2+t^2_{\alpha/(2N_{av}),N_{av}-2}}} \quad (11)$$

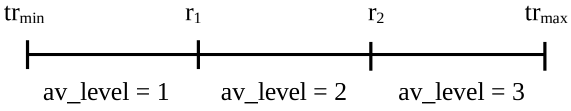
where, N_{tr} and N_{av} are the sizes of vectors {*tr_ratio*$_{\mathrm{i}}$} and {*av_ratio*$_{\mathrm{i}}$}, respectively, $t_{\alpha/(2N_{tr}),N_{tr}-2}$ and $t_{\alpha/(2N_{av}),N_{av}-2}$ are the *t*-distribution at significance levels $\alpha/(2N_{tr})$ and $\alpha/(2N_{av})$, respectively.

Last, for each data point, if its test standard *z* is greater than the test statistic *s*, the data point is declared anomalous. Based on this test, node i is characterized as a suspected (*i.e.*, *Node_CHR$_i$*: = "*suspected*") if both *tr_ratio*$_{\mathrm{i}}$ and *av_ratio*$_{\mathrm{i}}$ are anomalies, otherwise it is characterized as normal (*i.e.*, *Node_CHR$_i$*: = "*normal*").

4.3. Identifying Node Behavior

Once the vectors {*tr_ratio*$_{\mathrm{i}}$} and {*av_ratio*$_{\mathrm{i}}$} are updated, the Maximum Accusation Number (MAN) of each node i is updated, where, MAN is used to determine the maximum allowed number of which node i can be characterized as a suspected (*i.e. Node_CHR$_i$*: = "*suspected*"). As the behaviors of monitored nodes are characterized, the Accusation Number (AN) of each node i is updated accordingly. For our proposed scheme, *MAN*$_{\mathrm{i}}$ is evaluated based on the levels of *tr_ratio*$_{\mathrm{i}}$ and *av_ratio*$_{\mathrm{i}}$. Therefore, MANs of different nodes are varying as *tr_ratio* and *av_ratio* are varying. However, *AN*$_{\mathrm{i}}$ is used as a counter of times in which node i have been characterized as a suspected node (*i.e.*, *Node_CHR$_i$* = "*suspected*"). Note that, due to new-joined node is assumed to behave well, AN is initiated as zero. The behavior of node i is identified by comparing *MAN*$_{\mathrm{i}}$ and *AN*$_{\mathrm{i}}$. Table 4 illustrates our procedure to update MAN and AN, and hence, to identify node behavior, based on the following steps:

Step (1): relative to all known nodes, three discrete values of each context are calculated to identify three trust levels (*tr_level*) and three availability levels (*av_level*) of the vectors {*tr_ratio*$_{\mathrm{i}}$} and {*av_ratio*$_{\mathrm{i}}$}, resp ectively, such as follows:



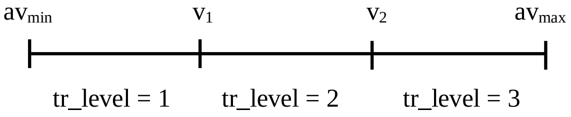
where, r_1 and r_2 are given as:

$$r_1 = tr_{\max} + (tr_{\max} - tr_{\min})/3$$

$$r_2 = tr_{\max} - (tr_{\max} - tr_{\min})/3$$

Table 4. **Node Behavior Identifying.**

```
Procedure Behavior_Identification ()

Input     {tr_ratio_i}: the weighted average vector of tr_ratio;
              {av_ratio_i}: the weighted average vector of av_ratio;
Output    well-behaved, misbehaved, and accused;

Begin

*/represent each of {tr_ratio_i} and {av_ratio_i} as three-equal sets /*
Calculate three discrete values for {tr_ratio_i} and {av_ratio_i};

for i∈{monitored}
{
        */compare tr_ratio_i and av_ratio_i with the three values/*
        Identify tr_level_i and av_level_i;

        */compute the maximum accusation number (MAN) /*
        MAN_i = ( tr_level_i + av_level_i ) / 2;

         */ update the accusation number (AN) /*
     if (Node_CHR_i= "suspected")
             AN_i := AN_i + 1
    else
             AN_i := AN_i − (Δtr_ratio_i +Δav_ratio_i)*AN_i;

    */ identify the node behavior /*
    if (AN_i ≤ 0)
            Node_BHR_i := "well-behaved"
    else
    {
          if (AN_i > MAN_i)
                      Node_BHR_i := "misbehaved"
          else
                      Node_BHR_i := "accused";
    }
} */ end for i /*

End.
```



where, v_1 and v_2 are given as:

$$v_1 = av_{\min} + (av_{\max} - av_{\min})/3$$

$$v_2 = av_{\max} - (av_{\max} - av_{\min})/3$$

Then, based on the trust and availability levels, *MAN*$_{\mathrm{i}}$ is evaluated as:

$$MAN_i = (tr\_leve_i + av\_level_i)/2 \quad (12)$$

Step (2): AN is updated based on the node's characteristic (*Node_CHR*) as follows:

if node i is suspected
increase AN$_i$ by 1
else
decrease AN$_i$ by
$(\Delta tr\_ratio_i + \Delta av\_ratio_i) * AN_i$ *;*

Where, Δ*tr_ratio$_i$* and Δ*av_ratio$_i$* are the differences between the current and previous values of *tr_ratio*$_{\mathrm{i}}$ and *av_ratio*$_i$, respectively.

Step (3): the findings of **step (1)** and **(2)** are used to identify the behavior of node i (*i.e.*, to update *Node_BHR*$_i$) as follows:

$$Node\_BHR_i = \begin{cases} \text{"}well-behaved\text{"};\ AN_i \le 0 \\ \text{"}misbehaved\text{"};\ AN_i > MAN_i \\ \text{"}accused\text{"};\ otherwise \end{cases} \qquad (13)$$

Therefore, by using this approach to identify node behavior, our proposed scheme gives the accused node a fair chance to avoid the BLACK-LIST (*i.e.*, to be declared as misbehaved node). That is, the more the values of *tr_ratio* and/or *av_ratio*, the more the value of *MAN* and the less the value of *AN*.

5. Simulation Study

5.1. Simulation Setup

Simulation experiments, by using Global Mobile Information System Simulator (GloMoSim 2.03), have been conducted so as to evaluate the performance of our proposed scheme. In order to watch the different performances of our proposed scheme, the experiments are repeated with different setups and scenarios. We used different network sizes, namely, 60, 70, 80, 90, and 100 nodes, with different attacker ratios, namely, 5%, 10%, 15%, 20%, and 25%, runs under different pause times, namely, 30, 90, 150, 300, and 600 seconds, to represent five mobility scenarios. However, for each scenario we run the simulation experiment 1200 seconds. The parameters and settings of simulation experiments are summarized in **Table 5**.

To show the effectiveness of our proposed scheme, two types of attacks, flooding and black-hole, have been simulated. Those two attacks are selected to evaluate our proposed scheme, due to their significant impacts on network performance. That is, the observable increase or decrease of packet rates that caused by those two attacks could be detected soon after the attack. In our simulation experiments, the flooding attack is implemented by pumping a great volume of forged RREQ packets (over 20 packet/second). However, in the black-hole attack, which is a type of denial of services, attacker drops all the received packets. When we simulate the attacks, less than or equal 25% of all nodes are chosen as misbehaved nodes (attackers). Therefore, in our simulated network, the number of attackers (*i.e.*, 25% of all nodes) guarantees that the fair nodes are the majority. Both of the attacks are tested under the mobility scenarios mentioned above. Due to its publicity in MANET researches, the Dynamic Source Routing (DSR) protocol is used as our routing protocol for those experiments.

Table 5. Parameters and Settings.

Parameter	Setting
Area size	1000 m × 1000 m
Number of nodes	60, 70, 80, 90, and 100 nodes
Mobility model	Random way-point model
Node speed	uniformly 3 - 10 m/s
Pause time	30, 90, 150, 300, and 600 seconds
Routing protocol	DSR protocol
Channel capacity	2 Mbps
Radio range	150 m
MAC layer protocol	IEEE 802.11
Background traffic	Constant Bit Rate (CBR)
Packet size	512 bytes

5.2. Evaluation Metrics and Results

The classic evaluation metrics Detection Rate (*DR*) and False Positive Rate (*FPR*), which are the most usual evaluation metrics for measuring the anomaly detection performance, are used as our main evaluation metrics. The detection rate is computed, as in (14), as the ratio of the attacks detected correctly to the total of all attacks. However, the false positive rate is computed, as in (15), as the ratio of the attacks detected incorrectly to the total of all normal behaviors.

$$DR = \frac{the\ correctly\ detected\ attacks}{total\ of\ the\ actual\ attacks} \qquad (14)$$

$$FPR = \frac{the\ incorrectly\ detected\ attacks}{total\ of\ all\ normal\ behaviors} \qquad (15)$$

Our proposed scheme has been tested, under different setups and scenarios, with the two attacks mentioned above. **Figures 2** and **3** show the detection rates of our scheme under different network sizes and attacker numbers, respectively. From **Figure 2** we observe that, with the increase of network size (*i.e.*, increase of node number), the detection rates of both attacks decrease, however, a notable decrease of detecting the black-hole attack is observed. **Figure 3** shows similar results for both flooding and black-hole attacks. That is, the increase of attackers number (*i.e.*, the increase of misbehaved ratio) results in similar decreasing of detecting both attacks. The reason may be that, as the ratio of attacker increase, the number of untrusted node also increases. Therefore, according to our proposed filtering procedure in which only the security related information from trusted nodes is utilized, a high volume of indirect information will be rejected due to their suspected source nodes. As a result, the lack of monitoring information causes that some of

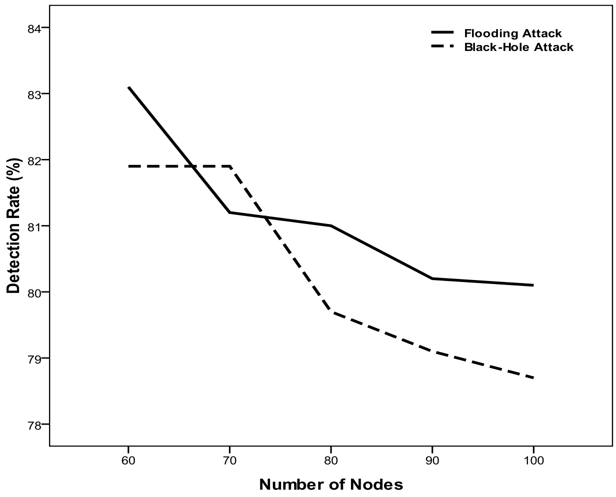


Figure 2. Detection rate and network size.

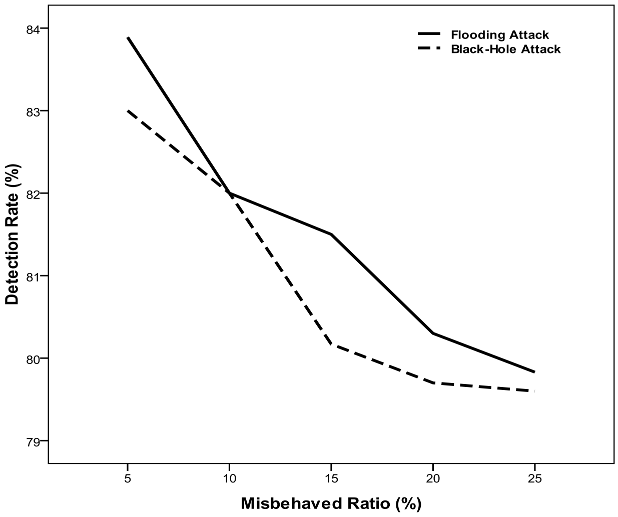


Figure 3. Detection rate and attackers' number.

the anomalous events might not be detected.

Figures 4, 5, and 6 show the false positive rates of our proposed scheme under different network sizes, attacker numbers, and mobility scenarios, respectively. In Figure 4 as the network size increases; we can see slight increase of the false positive rate of detecting both flooding and black-hole attacks. Similar relation between the misbehaved ratio and the false positive rate is shown in Figure 5. The results in this figure indicates that, the false positive rate of both attacks increases as the attacker number increases, with a difference that, the detecting of flooding attack results in a relatively high false positive rate when the attackers number is greater than 15%. The reason behind these results may be that, as the misbehaved ratio increases, more untrusted information are discarded by the monitor, however, this situation results in the detector can not characterize the behavior more accurately (*i.e.*, lead to high false positive rate). Beside

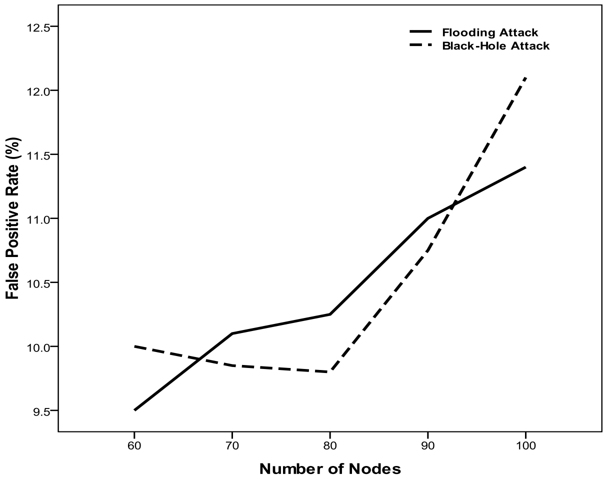


Figure 4. False positive rate and network size.

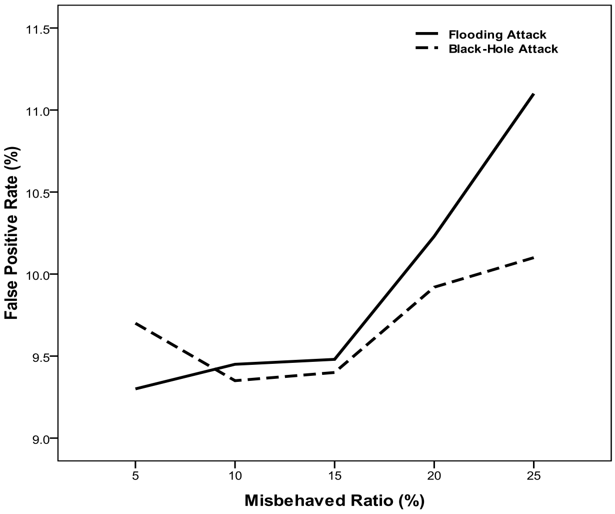


Figure 5. False positive rate and attackers' number.

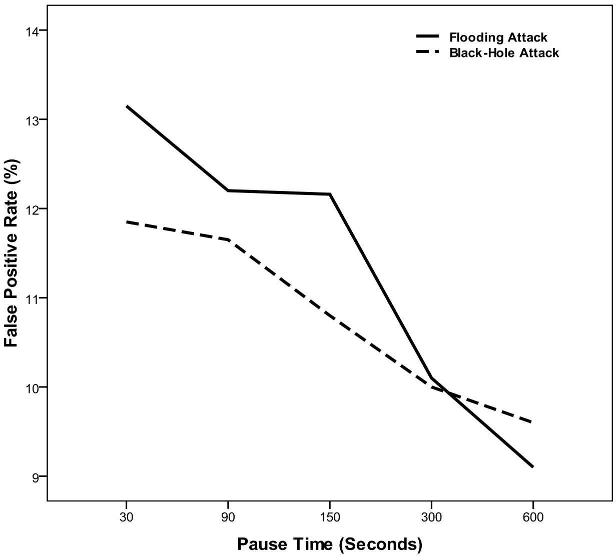


Figure 6. False positive rate and mobility.

that, some normal nodes may temporarily suffer a high request volume that cause some of them are mistakenly declared as misbehaved.

Figure 6 shows the false positive rates of both attacks under different mobility scenarios. The results shown in this figure indicate that, with the increase of pause time (*i.e.*, the decrease of mobility) the false positive rates of detecting both attacks decrease, which are predictable results. Because the data of lower mobility is more regular, and therefore, the detector could detect the anomalous events more accurately than in higher mobility environment. This implies that, in terms of false positive rate, the performance of our proposed method of lower mobility, as the most of proposed MANET IDSs, is better than that of higher mobility.

Figure 7 shows the detection and false positive rates of our proposed scheme for detecting both flooding and black-hole attacks. The results shown in this figure are averages of different scenario runs. The results of flooding attacks show that, 81 ± 1% of the anomalous events can be detected with 11 ± 1% false positive rate. Also, similar results for the black-hole attack show that, 80 ± 1% of the anomalous events can be detected with 10 ± 1% false positive rate. In general, the average of detection and false positive rates show that, our proposed scheme brings more than 80% detection rate, and in its worst status, the false positive rate have not exceeded 14%, which are good rates.

6. Conclusions and Future Work

In this paper, we propose a distributed and cooperative scheme using statistical methods to detect routing attacks in MANETs. The proposed scheme uses both direct and indirect observations to characterize the behaviors of both neighboring and remote nodes. Simple threshold and *Grubb's Test* are utilized to propose our new methods for analyzing audit data to detect any anomalous event in routing functions. The paper also presents innovative methods to compute the Maximum Accusation Number and Accusation Number, which are used to make decision about the node's behavior. The experimental results show that our proposed scheme performs well in detecting the anomalous events.

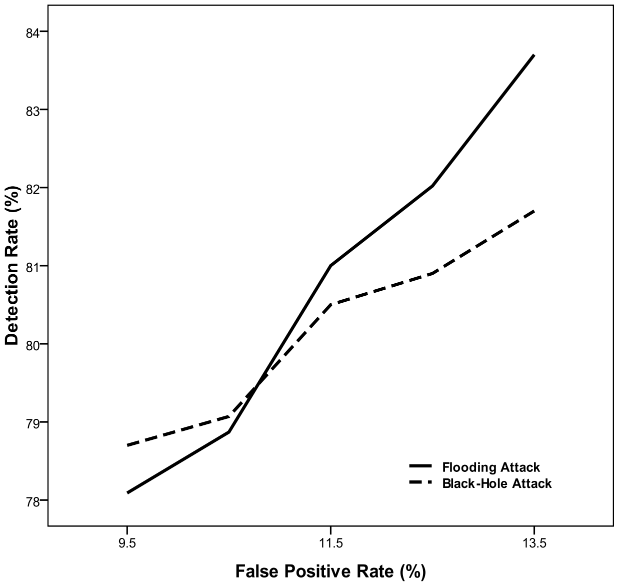


Figure 7. **Averages of detection and false positive.**

With a few exceptions, most of the proposed schemes for MANET do not really apply the response of attacks. Our future work includes exploring the concepts of response and mitigation of attacks within our proposed scheme. It also includes identifying the applicability of our proposed scheme to more attack types.

REFERENCES

[1] Y. G. Zhang, W. K. Lee and Y. A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, 2003, pp. 545-556.

[2] H. W. Kim, D. W. Kim and S. H. Kim, "Lifetime-Enhancing Selection of Monitoring Nodes for Intrusion Detection in Mobile Ad Hoc Networks," *AEU-International Journal of Electronics and Communications*, Vol. 60, No. 3, 2006, pp. 248-250.

[3] H. Mustafa and Y. Xiong, "Routing Attacks Detection and Reaction Scheme for Mobile Ad Hoc Networks Using Statistical Methods," *Proceedings of The* 22nd *Wireless and Optical Communication Conference on Security for Wireless Networks*, Chongqing, 16-18 May 2013, pp. 659-664.

[4] W. Y. Zhang, Q. B. Yang and Y. S. Geng, "A Survey of Anomaly Detection Methods in Networks," *Proceedings of Computer Network and Multimedia Technology* (CNMT 2009), Wuhan, 18-20 January 2009, pp. 1-3.

[5] P. Albers, O. Camp, J. Percher, B. Jouga, L. Me and R. Puttini, "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches," *Proceedings of the* 1st *International Workshop on Wireless Information Systems* (WIS-2002), 2002, pp. 1-12.

[6] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," *Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks* (SASN'03), October 2003, pp. 135-147. http://dx.doi.org/10.1145/986858.986877

[7] P. Kruus, D. Sterne, R. Gopaul, M. Heyman, B. Rivera, P. Budulas, B. Luu, T. Johnson, N. Ivanic and G. Lawler, "In-Band Wormholes and Countermeasures in OLSR Networks," *Proceedings of SecureComm*, Baltimore, 28 August 2006, pp. 1-11.

[8] S. S. Zheng, T. Jiang, J. S. Baras, A. Sonalker, D. Sterne, R. Gopaul and R. Hardy, "Intrusion Detection of In-Band Wormholes in MANETs Using Advanced Statistical Me-

thods," *Proceedings of Military Communications Conference* (MILCOM), San Diego,16-19 November 2008, pp. 1-7.

[9] S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proceedings of the* 6*th Annual International Conference on Mobile Computing and Networking* (MOBICOM), August 2000, pp. 255-265.

[10] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes-Fairness in Dynamic Ad-hoc NeTworks)," *Proceedings of the* 3*rd ACM International Symposium on Mobile Ad Hoc Networking and Computing* (MobiHoc'02), June 2002, pp. 226-236.

[11] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Advanced Communications and Multimedia Security*, *IFIP*: *The International Federation for Information Processing*, Vol. 100, 2002, pp. 107-121.

[12] David S. Moore and George P. McCabe, "Introduction to the practice of statistics," 5th Edition, W. H. Freeman, New York, 2005.

[13] V. Chandola, A. Banerjee and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys* (*CSUR*), Vol. 41, No. 3, 2009, Article No. 15.