I. J. Computer Network and Information Security, 2020, 6, 14-29
Published Online December 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2020.06.02

Robust and Accurate Trust Establishment Scheme for Wireless Sensor Network

Audrey NANGUE
University of Dschang, Dschang, Cameroon
E-mail: nangueaudrey@yahoo.fr

Elie FUTE TAGNE
University of Dschang, Dschang, Cameroon
University of Buea, Buea, Cameroon
E-mail: eliefute@yahoo.fr

Emmanuel TONYE
University of Yaoundé1, Yaoundé, Cameroon
E-mail: tonye2018@hotmail.com

Received: 24 September 2020; Accepted: 30 October 2020; Published: 08 December 2020

Abstract: The success of the mission assigned to a Wireless Sensor Network (WSN) depends heavily on the cooperation between the nodes of this network. Indeed, given the vulnerability of wireless sensor networks to attack, some entities may engage in malicious behavior aimed at undermining the proper functioning of the network. As a result, the selection of reliable nodes for task execution becomes a necessity for the network. To improve the cooperation and security of wireless sensor networks, the use of Trust Management Systems (TMS) is increasingly recommended due to their low resource consumption. The various existing trust management systems differ in their methods of estimating trust value. The existing ones are very rigid and not very accurate. In this paper, we propose a robust and accurate method (RATES) to compute direct and indirect trust between the network nodes. In RATES model, to compute the direct trust, we improve the Bayesian formula by applying the chaining of trust values, a local reward, a local penalty and a flexible global penalty based on the variation of successful interactions, failures and misbehaviors frequency. RATES thus manages to obtain a direct trust value that is accurate and representative of the node behavior in the network. In addition, we introduce the establishment of a simple confidence interval to filter out biased recommendations sent by malicious nodes to disrupt the estimation of a node's indirect trust. Mathematical theoretical analysis and evaluation of the simulation results show the best performance of our approach for detecting on-off attacks, bad-mouthing attacks and persistent attacks compared to the other existing approaches.

Index Terms: Attack, penalty, reward, security, trust, trust management system.

1. Introduction

Because of their ease of deployment, collection and routing of information, wireless sensor networks (WSNs) have gained obvious interest in various application areas such as environmental, medical, military or industrial. The success of their mission after deployment depends greatly on good cooperation between different sensors (nodes) present in the field in order to forward the collected information to the decision center. However, due to the WSNs deployment in open and unprotected environments, some sensors can be captured, compromised and placed back in the field to launch attacks inside the network to spy on or cripple the network operation. The paralysis of the network is reflected through the deletion of certain data collected and routed through the network. Faced to these so-called internal attacks, network security is greatly affected. Thus, the security of wireless sensor networks has become an attractive research topic. In particular, the problem of detecting compromised nodes leading to the judicious choice of reliable nodes to ensure data routing is now the major axis of research in wireless sensor network security. Conventional security techniques such as cryptography and authentication have proven to be effective against external attacks, but as soon as a node is compromised inside the network, these techniques become ineffective [1,2,9]. There should be some mechanism by which a node gets an idea about its neigbors prior to the communication [18]. Thus, developing new techniques to protect WSNs against internal attacks becomes a necessity.

To address such attacks, numerous researchers have proposed defense techniques using a human behavior pattern called trust [16]. Trust is a vital factor that allows an entity to choose with whom to interact and exchange sensitive

information [17]. Modern techniques for protecting WSNs against internal attacks (persistent attack, on-off attack, bad mouthing attack, ballot stuffing attack ...) focus on trust management systems used to estimate the trust level of network nodes by analyzing their interactions and behaviors [11]. The estimated trust level is used by network nodes to distinguish compromised nodes from reliable nodes. This allows them to build routing paths free of intruders and thus guarantee the correct data routing to the decision center.

Several works [3,9,10,13] on trust management systems have been proposed to defend WSNs against internal attacks. The approach proposed in [10] is particularly interesting in that it combines the innovative concepts of reward and penalty in its model for evaluating the trust of network nodes. This improves the distinction between compromised and trusted nodes through the network. However, this approach produces quite high false positive rates because of the rigidity of the reward and penalty factors that are systematically always applied simultaneously when estimating the trust of network nodes. Furthermore, because of this inflexibility, this approach does not adequately adapt to the frequent behavioral changes performed by the smart compromised nodes that have the desire to paralyze the network without being detected.

To overcome the limitations of existing approaches, we propose a new robust and effective model for trust assessment called RATES. The main features proposed in RATES to improve the detection of compromised nodes are listed as follows:

- RATES improves the formula of the beta distribution function by incorporating a local reward factor or a local penalty factor and trust chaining based on the variation in the number of successful and unsuccessful interactions between two consecutive units of observation time. In this way, we avoid the systematic and simultaneous application of penalty and reward factors during the evaluation of node trust.
- In addition, at the end of an observation time window (consisting of L observation units), we calculate the global trust value by applying a flexible global penalty factor whose severity automatically adapts itself according to the misbehavior frequency during the considered time window. This allows RATES to obtain the global trust value which is much more robust, precise and allows us to deal with persistent and on-off attacks.
- To deal with bad mouthing attack and ballot stuffing, we introduce the establishment of a modified confidence interval to filter recommendations used to estimate the indirect trust of a network nodes.

Mathematical theoretical analysis and simulations have been used to prove the validity and efficiency of our model. The rest of the paper is organized as follows: Section 2 presents the existing work. Section 3 illustrates the methodology used. Section 4 describes our contribution. Section 5 is devoted to theoretical analysis and evaluation. Section 6 presents the simulation results and section 7 concludes the paper.

2. Related Works

Many works proposed on trust management system in wireless sensor networks demonstrate the interest which they are granted in this field. We will present in the following the essentials of some existing trust management systems. In [12] Shaikh et al. proposes a group-based trust management system in which trust is estimated at each cluster member node, cluster head, and base station. To estimate trust, nodes observe their neighbors'behaviors during sliding time windows consisting of a fixed number of time units Δ. During each unit of time Δ a node x counts the number of good $(S_{x,y})$ and bad $(U_{x,y})$ behaviors of a neighbor y and calculates its trust as follows:

$$T_{x,y} = \left[100 \times \frac{S_{x,y}^2}{\left(S_{x,y} + U_{x,y}\right)\left(S_{x,y} + 1\right)} \right] \quad (1)$$

This trust value categorizes a neighbor as trustworthy, uncertain, or unreliable. The authors claim that the robustness of this approach is only verified when the number of bad behaviors is greater than or equal to the number of good behaviors. So, this approach is suitable to detect persistent attack. But it fails to detect on-off attack because the hypothesis about the number of bad behaviors which is greater than or equal to the number of good behaviors is not realistic since the primary purpose of a compromised node is to damage the network without being detected. Moreover, this approach does not propose a mechanism for filtering recommendations when estimating indirect trust.

As Shaikh et al. [12], Daojing et al. proposes ReTrust [9]: A trust estimation scheme in which the estimation of the direct trust of a node y by a node x is done using the formula:

$$T_{x,y} = \left[\lambda \times \frac{\sum_{j=1}^{m} \beta_j \times (1-p^j) \times p^j}{\sum_{j=1}^{m} \beta_j \times (1-p^j)} \right] \quad (2)$$

where $s_{x,y}^{j}$ and $f_{x,y}^{j}$ denote the number of successful and failed interactions respectively during the $j-th$ time unit of the time window. This approach is lightweight and efficient to resist against bad mouthing attack. However, it does not take into account the cases of persistent bad behavior of a compromised node. And the lack of using misbehavior frequency during trust evaluation make it inefficient to correctly mitigate on-off attack.

In 2014, Ishmanov et al. [13] have proposed a secure trust establishment scheme able to detect compromised nodes based on past and actual misbehavior. Simulation results show the effectiveness of this scheme in detecting persistent attacks. However, without having integrated the misbehavior frequency, the authors assert that this scheme is also effective in detecting on-off attacks. Yet, it is almost impossible to design an effective trust management scheme against on-off attacks without taking into account the misbehavior frequency.

In [3], a robust trust establishment scheme is proposed to estimate only the direct trust of the network nodes. The use of misbehavior frequency and misbehavior weight allows this approach to resist persistent and on-off attacks. However, no mechanism is provided for assessing indirect trust and dealing with ballot stuffing and bad mouthing attacks.

More recently in 2018, Sahoo et al. [10] proposed penalty-based, reward based, sliding-size-time-based trust estimation system to evaluate the direct trust of nodes. Thus, a node i evaluates the direct trust $DT_{i,j}(t)$ of a node j at a time t by the formula:

$$DT_{i,j}(t) = \left[10 \times \left(\frac{S_{i,j}(t)}{S_{i,j}(t)+U_{i,j}(t)} \right) \times \left(\frac{S_{i,j}(t)}{1+U_{i,j}(t)} \right) \times \left(\frac{1}{\sqrt{U_{i,j}(t)}} \right) \right] \quad (3)$$

Where $S_{i,j}$ represents the successful number of interactions and $U_{i,j}$ the number of failures. In addition, the authors use the periodicity of misbehavior to vary size of the sliding time window. Which improves the resistance of this approach to the attack on-off. To evaluate indirect trust, a statistical method based on the median absolute deviation is used to filter the recommendations received. The main disadvantage of this approach is its high false-positive rate in estimating direct trust and detecting compromised nodes. This high rate of false positives is due to the fact that the penalty function used $\left(\frac{1}{\sqrt{U_{i,j}(t)}} \right)$ is very severe. In addition, the reward function used $\left(\frac{S_{i,j}(t)}{1+U_{i,j}(t)} \right)$ tends to lower the trust value rather than bring added value.

3. Methodology

The approaches presented in Section II address the problem of assessing trust between WSN nodes by rewarding nodes with good conduct and penalizing those with poor conduct. The trust values evaluated make it possible to detect the malicious nodes responsible for persistent attacks, on-off attacks, bad mouthing attacks, and consequently to ensure a judicious choice of nodes to execute network services. However, these approaches are still weak with regard to detection errors that are still high in terms of false positives and false negatives. Moreover, these approaches are not sufficiently protected against biased recommendations sent by malicious nodes to discredit reliable nodes or to promote certain dishonest nodes misleading these trust assessment systems. To address the shortcomings of these existing approaches, we propose in this paper RATES, an efficient and flexible method of applying reward and penalty to correctly estimate the direct trust of nodes. Then a filtering of the recommendations is performed before estimating the indirect trust of the nodes. The calculated trust values are regularly updated as time passes and new observations are made. Finally, the trust values obtained are compared to a threshold value in order to detect and revoke malicious nodes. Fig.1 globally illustrates the method used in RATES.

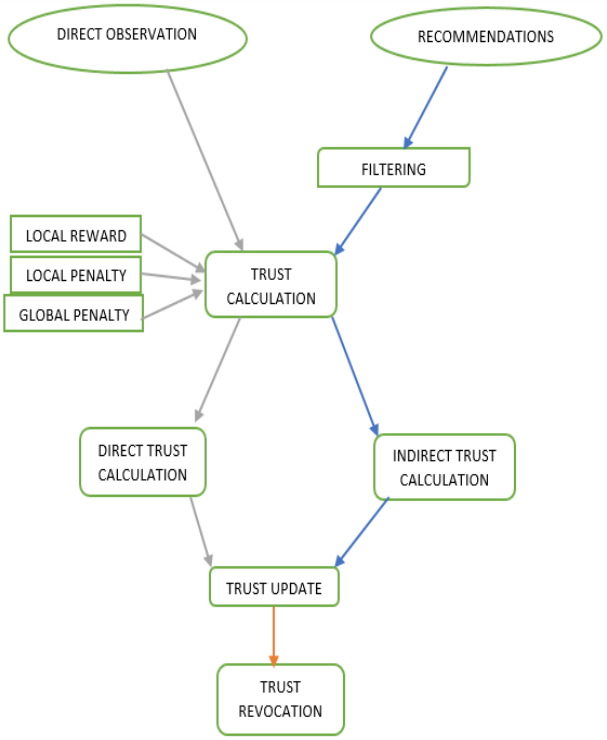


Fig.1. RATES estimation method

4. Robust and Accurate Trust Estimation Scheme

In this section, we present a trust management scheme named RATES (Robust and Accurate Trust Estimation Scheme) able to estimate direct and indirect trust in order to make efficient trust decision of sensor nodes and prevent the WSN from various attacks.

4.1. Assumptions

The trust estimation model we propose is based on the following assumptions:

- All nodes have a unique identifier and a method of authentication which prevents identity theft
- The nodes are static in the network and each node is able to monitor its neighbors' activities
- The number of interactions between two nodes is fixed

4.2. Attacker Behavior Pattern

Here, we are dealing with so-called smart compromised nodes. A smart compromised node is an attacker that tries to maintain a high level of trust while damaging the network. To impair network performance, a compromised node may behave in a selfish manner, delete or modify data packets persistently (persistent attack) or alternately (on-off attack). In addition, it can compromise the trust estimating system by providing poor recommendations about reliable nodes (Bad Mouthing Attacks) or by providing good recommendations about unreliable nodes (Ballot stuffing attack).

4.3. Direct Trust Estimation Method During a Unit of Time t_i

In RATES, direct trust of node x for node y is evaluated based on the number of successful interactions $\left(S_{x,y}^{t_i}\right)$ and unsuccessful $\left(U_{x,y}^{t_i}\right)$ counted during each direct observation in time unit t_i. In order to take past experiences into account, we use the sliding time windows (Δt) consisting of L time units. Thus, as shown in Fig.2, after L units of time, the time window shift one unit to the right to erase the experience recorded in the first unit of time by adding the experience of the most recent unit.

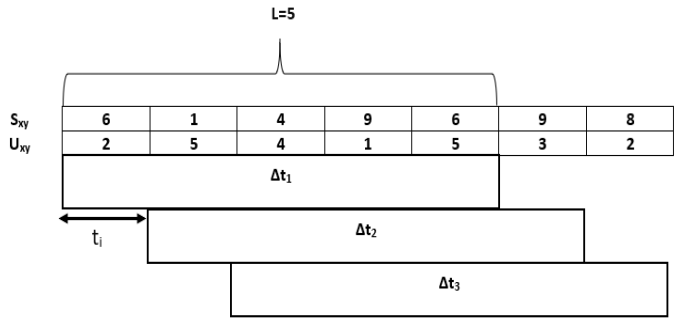


Fig.2. Mechanism of the sliding time window

It has already been justified in the literature that the reputation of a node x with respect to a node y can follow the beta distribution of parameter $\left(S_{x,y}^{t_i}, U_{x,y}^{t_i}\right)$ [14]. Therefore, the direct trust of a node x with respect to a node y is obtained by applying the statistical expectation of the reputation distribution by the formula:

$$T_{x,y}(t_i) = E\left(Beta(S_{x,y}^{t_i}, U_{x,y}^{t_i})\right) = \frac{S_{x,y}^{t_i} + 1}{S_{x,y}^{t_i} + U_{x,y}^{t_i} + 2} \tag{4}$$

In RATES scheme, we improve this formula by applying to each time unit t_i, either a local reward or a local penalty and never both at the same time as in existing approaches. In addition, we apply trust chaining which means that trust at time unit t_i depends on trust at time unit t_{i-1}. The local reward is used to encourage nodes that succeed in more and more interactions in the network. We use trust chaining to prevent a malicious node from being able to rapidly increase its trust value just by increasing the number of successful interactions over a small time period. We apply the local penalty to punish nodes that try to damage the network by increasing the number of failed interactions for a short period of time. Indeed, when between two consecutive time units the number of successful interactions between x and y is increasing, then we integrate a local reward materialized by the parameter α. So, we have the new formula:

$if\ (S_{x,y}^{t_i} - S_{x,y}^{t_{i-1}} > 0)$ then,

$$T_{x,y}(t_i) = \frac{1}{2}\left(T_{\max} \times \frac{\alpha S_{x,y}^{t_i} + 1}{\alpha S_{x,y}^{t_i} + U_{x,y}^{t_i} + 2} + T_{x,y}(t_{i-1})\right) \tag{5}$$

with $\alpha > 1$ and $T_{x,y}(t_i) \in [0, T_{\max}]$.

On the other hand, when between two consecutive time units the number of failed interactions between x and y is increasing, then we integrate instead a local penalty materialized by the parameter β. Which leads us to the formula:

$if\ (U_{x,y}^{t_i} - U_{x,y}^{t_{i-1}} > 0)$ then,

$$T_{x,y}(t_i) = \frac{1}{2}\left(T_{\max} \times \frac{S_{x,y}^{t_i} + 1}{S_{x,y}^{t_i} + \beta U_{x,y}^{t_i} + 2} + T_{x,y}(t_{i-1})\right) \tag{6}$$

with $\beta > 1$.

Conversely, if the number of successful and unsuccessful interactions remains stable between two consecutive units of time, then neither reward nor penalty is applied. Which brings us to the formula:

If $(U_{x,y}^{t_i} - U_{x,y}^{t_{i-1}} = 0)$ and $(S_{x,y}^{t_i} - S_{x,y}^{t_{i-1}} = 0)$ then,

$$T_{x,y}(t_i) = T_{\max} \times \frac{S_{x,y}^{t_i} + 1}{S_{x,y}^{t_i} + U_{x,y}^{t_i} + 2} \tag{7}$$

Equations (5), (6) and (7) are effective in assessing the trust level of a node initiating persistent attack during time unit t_i. However, with these formulas, it is not possible to evaluate with a good accuracy, the trust level of a node initiating on-off attacks. In order to effectively address on-off attacks, we evaluate the global trust level $GT_{x,y}(\Delta t)$ of the nodes observed after each time window (Δt) corresponding to L=5 time units t_i. To do so, we first calculate the misbehavior frequency $(F_{\Delta t})$ of the evaluated node during this time window. A time unit t_i of a time window (Δt) is considered (on) if $T_{x,y}(t_i) < th$, and is considered (off) if $T_{x,y}(t_i) \geq th$. As a result, we calculate:

$$F_{\Delta t} = \frac{\sum_{i=1}^{L} on(t_i)}{\sum_{i=1}^{L} on(t_i) + \sum_{i=1}^{L} off(t_i)}. \tag{8}$$

This misbehavior frequency thus allows us to calculate the global trust of the observed node by integrating a flexible global penalty whose severity automatically adapts according to the level of the calculated misbehavior frequency. The global trust is obtained by the formula:

$$GT_{x,y}(\Delta t) = T_{\max} \times \left(\prod_{i=1}^{L} \sqrt[L]{\frac{k_i \times S_{x,y}^{t_i} + 1}{k_i \times (S_{x,y}^{t_i} + U_{x,y}^{t_i}) + 2}} \right) \left(\frac{1}{K^V} \right) \tag{9}$$

Where $\left(\frac{1}{K^V} \right)$ is the global penalty factor. The value of parameter K changes as a function of the misbehavior frequency as follows:

$$\begin{aligned} &if\,(F_{\Delta t} = 1) \rightarrow K = 6 \\ &if\,(F_{\Delta t} = 0.8) \rightarrow K = 5 \\ &if\,(F_{\Delta t} = 0.6) \rightarrow K = 4 \\ &if\,(F_{\Delta t} = 0.4) \rightarrow K = 3 \\ &if\,(F_{\Delta t} = 0.2) \rightarrow K = 2 \end{aligned} \tag{10}$$

We handle the following special case separately:

$$if\,(F_{\Delta t} = 0) \rightarrow GT_{x,y}(\Delta t) = T_{\max} \times \frac{\sum S_{x,y}^{t_i} + 1}{\sum S_{x,y}^{t_i} + \sum U_{x,y}^{t_i} + 2} \tag{11}$$

We realize that when the misbehavior frequency is high, the global penalty factor automatically adjusts and becomes more harsh. $V = \prod_{i=1}^{L} \sqrt[L]{U_{x,y}^{t_i}}$ and $k_i = F_{\Delta t}^{L-i}$ is forgetting factor which also depends on the misbehavior frequency. Its role is to assign more importance to recently interactions and less importance to old. This implies the relationship $k_1 < k_2 < \cdots < k_L$. According to our formula, when a node has a high misbehavior frequency, then the weight of its past interactions is more strongly felt compared to a node with a very low misbehavior frequency.

Thus, the use of local reward, local penalty, global penalty and trust chaining allows RATES scheme to more accurately assess the trust level of network nodes and to more effectively resist persistent and on-off attacks.

4.4. Indirect Trust Estimation Method

Indirect trust $IT_{x,y}$ is used by a node x when it wants to communicate with a node y but it has no passed experience with it. In other words, it has no direct interaction that allows it to estimate its direct trust. But the node x must be able to trust y before interacting with it. Having no experience with node y, node x uses recommendations of neighboring nodes that it shares with y. However, these recommendations may be biased by their issuers. Indeed, a neighbor can provide a recommendation that disfavors a normal node (bad mouthing attack) or favors a compromised node (ballot stuffing attack). This imposes recommendations filtering method before the computation of indirect trust in order to reduce effects of bad recommendations and obtain reliable indirect trust value.

The filtering method that we propose is based on the establishment of a confidence interval centered on the median to validate reliable recommendations. Indeed, in our approach, when a node x wishes to evaluate the indirect trust of a node y, it seeks all trustworthy neighbors z_i that it has in common with y by sending them a request for their recommendations in respect of y. If we stop at this single criterion, for filtering recommendations, a node can skew recommendations once it has obtained a high trust value from evaluator. To deal with this issue, we establish confidence interval based on recommendations received and the trusts in the issuers of these recommendations. So consider

$\Gamma = \left\{T_{x,z_1}, T_{x,z_2}, \cdots, T_{x,z_n}\right\}$ the set of trusts that the node x have with respect to the trustworthy neighbors and $R = \left\{R_{z_1,y}, R_{z_2,y}, \cdots, R_{z_n,y}\right\}$ all the recommendations sent by these neighbors. We build the set $\Psi = \left\{\frac{R_{z_1 y}}{T_{xz_1}}, \frac{R_{z_1 y}}{T_{xz_2}}, \cdots, \frac{R_{z_n y}}{T_{xz_n}}\right\}$. Subsequently, we calculate the median $med(\Psi)$ and the standard deviation $\sigma(\Psi)$ of the set Ψ. The confidence interval is obtained by the formula:

$$\left[med(\Psi) - Z \times \sigma(\Psi), med(\Psi) + Z \times \sigma(\Psi)\right] \tag{12}$$

The parameter Z is used to adjust the size and accuracy of confidence interval. Thus, the indirect trust of x for y is given by:

$$IT_{x,y} = \left\lceil \frac{\sum_{i=1}^{l} R_{z_i y}}{l} \right\rceil \tag{13}$$

Where $\frac{R_{z_i y}}{T_{xz_i}} \in \left[med(\Psi) - Z \times \sigma(\Psi), med(\Psi) + Z \times \sigma(\Psi)\right]$, l is the number of values belonging to the confidence interval.

5. Theoretical Analysis and Evaluation of the Approach rates

In this section, we analyze and proof that RATES scheme is resilient against attacks on trust management system. This theoretical analysis is done for direct trust estimation method. For that, we broadly categorized the nodes of WSN into two types of node: good nodes and bad nodes. We assume that a good node always exhibits OFF behaviors and provides honest recommendations. However, malicious nodes always exhibit ON behaviors and give fake recommendations by launching various attacks like:

- Blackhole attack where the malicious node try to misroute forwarded data through its position and then delete all these data which can contain correct trust value;
- Bad mouthing attack where a good node receive lower trust value because of fraudulent recommendations sent by malicious nodes;
- Ballot stuffing attack where malicious node receive higher trust value because of the fraudulent recommendations sent by another malicious nodes;
- Persistent attack where a malicious node continuously damage network by failing all interactions with other nodes.

These behaviors are formally describe in the following definitions and are used to validate our model.

5.1. Resilience Analysis of Direct Trust Evaluation Scheme

Let us consider the following definitions:

Definition 1: In RATES protocol, during a time unit t_i, when the measured direct trust of node x on node y is less than $\frac{T_{\max}}{2}$ i.e. $\left(T_{x,y}(t_i) < \frac{T_{\max}}{2}\right)$ then we consider that node y exhibits ON behavior. When a node y always shows ON behavior in a time window (Δt), it's said to be a malicious node. Moreover, for ON behavior the number of bad interactions is more than the good interactions $\left(U_{x,y}^{t_i} > S_{x,y}^{t_i}\right)$.

Definition 2: On the other hand, during a time unit t_i, when the measured direct trust of node x on node y is greater than or equal to $\frac{T_{\max}}{2}$ i.e. $\left(T_{x,y}(t_i) \geq \frac{T_{\max}}{2}\right)$ then we consider that node y exhibits OFF behavior. When a node y always shows OFF behavior in a time window (Δt), it's said to be a legitimate node.

Definition 3: A bad node y is said to have deceived node x if x considers y as a legitimate node.
Claim 1: *Our direct trust estimation method is resilient against deception by a bad node.*

Proof. By using the method of contradiction, we assume that a malicious node y deceives a node x. Then according to definition 1 in which $\left(U_{x,y}^{t_i} > S_{x,y}^{t_i}\right)$ and definition 2 in which $\left(T_{x,y}(t_i) > \frac{T_{\max}}{2}\right)$, we follow three situations:

Situation 1. $S_{x,y}^{t_i} \geq 1$. This means that node y has interacted with node x during the time unit t_i. To prove (7), we proceed by changing the variable as follows:

Let $S'_{x,y} = S_{x,y}^{t_i} + 1$ and $U'_{x,y} = U_{x,y}^{t_i} + 1$

So, (7): $T_{x,y}(t_i) = T_{\max} \times \frac{S_{x,y}^{t_i} + 1}{S_{x,y}^{t_i} + U_{x,y}^{t_i} + 2}$,

becomes

$T_{x,y}(t_i) = T_{\max} \times \frac{S'_{x,y}}{S'_{x,y} + U'_{x,y}}$. Now let $w = \frac{U'_{x,y}}{S'_{x,y}}$

Since $U_{x,y}^{t_i} > S_{x,y}^{t_i} \Rightarrow U_{x,y}^{t_i} + 1 > S_{x,y}^{t_i} + 1$

$$\Rightarrow \frac{U_{x,y}^{t_i} + 1}{S_{x,y}^{t_i} + 1} = \frac{U'_{x,y}}{S'_{x,y}} = w > 1$$

$$\Rightarrow T_{x,y}(t_i) = T_{\max} \times \frac{1}{1 + \frac{U'_{x,y}}{S'_{x,y}}} = \frac{T_{\max}}{1+w}$$

$$\text{Since } w > 0 \Rightarrow 1 + w > 2$$

$$\Rightarrow \frac{1}{1+w} < \frac{1}{2}$$

$$\Rightarrow \frac{T_{\max}}{1+w} < \frac{T_{\max}}{2}$$

$$\Rightarrow T_{x,y}(t_i) < \frac{T_{\max}}{2}$$

Which leads to the contradiction since it is given that

$$T_{x,y}(t_i) \geq \frac{T_{\max}}{2}.$$

To prove (5), apply the same reasoning by taking: $S'_{x,y} = \alpha S_{x,y}^{t_i} + 1$ and $U'_{x,y} = U_{x,y}^{t_i} + 1$. Similarly, to prove (6), apply the same reasoning by taking: $S'_{x,y} = S_{x,y}^{t_i} + 1$ and $U'_{x,y} = \beta U_{x,y}^{t_i} + 1$. For equations (5) and (6), proof requires the use of recurrence reasoning by considering that initially $T_{x,y}(t_0) < \frac{T_{\max}}{2}$.

Situation 2. $S_{x,y}^{t_i} = 0$ and $U_{x,y}^{t_i} > 1$. It means that node x has some unsuccessful interaction with node y, but has no successful interaction with y in time unit t_i. According to (7),

$$T_{x,y}(t_i) = T_{\max} \times \frac{S_{x,y}^{t_i} + 1}{S_{x,y}^{t_i} + U_{x,y}^{t_i} + 2}, \text{since } S_{x,y}^{t_i} = 0$$

$$T_{x,y}(t_i) = T_{\max} \times \frac{0+1}{0+U_{x,y}^{t_i}+2} = \frac{T_{\max}}{U_{x,y}^{t_i}+2}$$

$$\text{We know that } U_{x,y}^{t_i} > 1 \Rightarrow U_{x,y}^{t_i} + 2 > 3$$

$$\Rightarrow \frac{1}{U_{x,y}^{t_i}+2} < \frac{1}{3} < \frac{1}{2}$$

$$\Rightarrow T_{x,y}(t_i) = \frac{T_{\max}}{U_{x,y}^{t_i}+2} < \frac{T_{\max}}{2}$$

Which contradicts the assumption $T_{x,y}(t_i) \geq \frac{T_{\max}}{2}$ and prove **Claim 1**.

To prove (5) and (6), you just have to apply the same principle by integrating recurrence reasoning and considering that initially $T_{x,y}(t_0) < \frac{T_{\max}}{2}$.

Situation 3. $S_{x,y}^{t_i} = 0$ and $U_{x,y}^{t_i} = 0$. This means there is no interactions between nodes x and y in time unit t_i. As there are no interactions in t_i, it's possible that node x may interact with node y during other time unit of sliding window Δt. If it interacts, then either through situation 1 or situation 2, its maliciousness can be proved. If it does not interact throughout the sliding window Δt, then indirect trust is estimated through recommendations.

6. Simulation Results

In this section, we attest to the efficiency and robustness of our model through simulations carried out on the following aspects:

- Detection of a reliable node: In this scenario, we vary the probability of good behavior of reliable node between 0.7 and 0.9. In this case, we expect to observe the trust values of this node oscillating above the threshold trust value. In addition, the rate of false positive generated must be at its lowest.
- Detection of a compromised node: In this scenario, we vary the misbehavior probability of compromise node between 0.7 and 0.9. Thus, we expect to observe the trust values of this node oscillating below the threshold trust value. This should result in a very low false negative rate.
- On-off attack detection: To validate this detection, we consider a first case where the malicious node frequently attacks with a misbehavior probability ranging from 0.6 to 0.9. Then we consider a second case where the malicious node attacks rather rarely with a misbehavior probability ranging from 0.1 to 0.4. The detection rate of nodes responsible for the on-off attack is expected to increase as the attacks frequency increases.
- Bad mouthing attack detection: In this scenario, we vary between 10% and 50%, the percentage of malicious nodes sending bad recommendations about a reliable node. We hope to see our approach correctly detect and filter out these false recommendations as the percentage of malicious nodes decreases. In addition, we hope that the trust values estimated after filtering these false recommendations will oscillate above the threshold trust value.

We evaluate and compare RATES to GATE [10], STES [13], and RTES[3]. Simulations were performed using Omnet++5.6 simulator. All these approaches were tested under the same conditions using the same data set generated during each experiment. Each experiment is run over 100 iterations and then repeating a measurement multiple times and averaging the results allows us to ensure the reliability and accuracy of the results. In addition, all implemented approaches are calibrated on identical common simulation parameters. The simulation parameters used are presented in table 1.

6.1. Bad Behavior Detection and Error Rate

Here, we present the impact of good and bad behaviors adopted by a node on its direct trust evaluation. To represent the behavior of nodes, at each time unit, we randomly generate 10 behaviors. Each of these behaviors is defined as good or bad based on a random integer generated between 1 and 10. Note that this modelling fits best with the behaviors of the nodes as observed in reality. Indeed, a legitimate node can sometimes behave badly temporarily (for example, to delete packets) because of the conditions imposed by the network (congestion at a point in the network, for example). Therefore, the behavior of a legitimate node may be similar to that of a compromised node launching on-off attack. However, the misbehavior of a legitimate node is random and temporary while that of on-off compromised node is predetermined.

Table 1. Simulation parameters

Parameters	Value
Initial trust value	10
Trust range [0, Tmax]	[0,10] Tmax=10
α	1.5
β	2
Trust estimation time interval	Δ
Simulation time	1000 Δ
Sliding window length	L=5

In this first simulation case, we define three high probabilities P=0.7, 0.8 and 0.9 to model the behavior of a node that is a priori malicious. So, for each probability, if the generated number is less than or equal to 7, 8, 9 respectively, the behavior is considered bad. Fig.3, Fig.4 and Fig.5 show that our RATES approach is successful in correctly estimating the trust values of malicious nodes regardless of their misbehavior probability. However, other approaches only succeed in doing so when the misbehavior probability of the malicious node is very high (P=0.9). These approaches fail to correctly detect malicious nodes when the misbehavior probability decreases. The accuracy of our scheme is confirmed in Fig.6 where we can see that RATES does not present false negatives contrary to existing approaches. The high accuracy and robustness of our scheme is justified by the application of the trust chaining, local reward, local and flexible global penalties that prevent malicious nodes from misleading RATES.

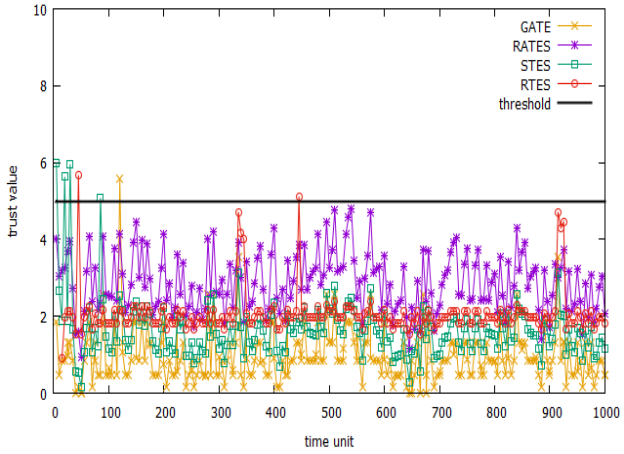


Fig.3. Bad behaviors detection: Case of compromised node (P=0.7)

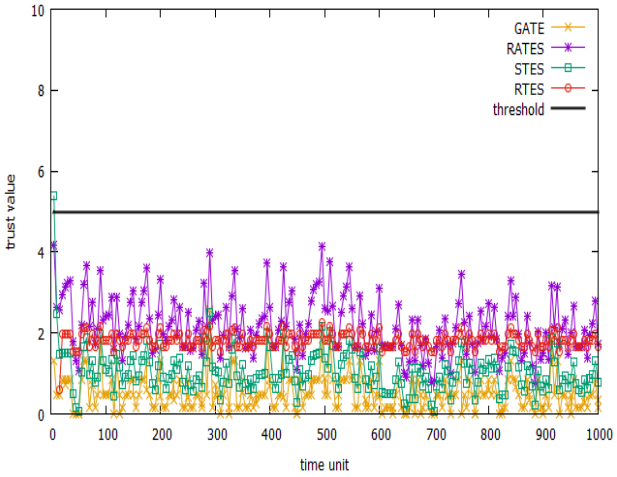


Fig.4. Bad behaviors detection: Case of compromised node (P=0.8)

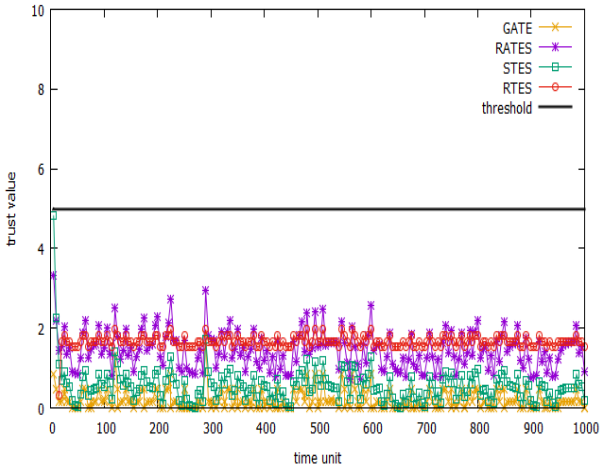


Fig.5. Bad behaviors detection: Case of compromised node (P=0.9)

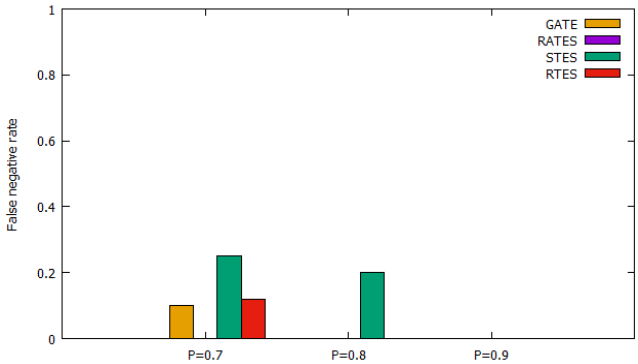


Fig.6. False negative rate

In the second case presented, we model the behavior of a node a priori legitimate. That is, a node whose probability of adopting a good behavior is the highest. As the probability of adopting a good behavior, we always consider the values P = 0.7, 0.8, 0.9.

Fig.8 and Fig.9 show that when a node performs good behaviors with high probabilities (P=0.8 and 0.9), our RATES approach is very successful in estimating their trusts in the right range, while other approaches are ineffective. Our approach therefore takes advantage of the flexibility of its global penalty factor, which allows a better trust estimation in this context. Unfortunately, as shown in Fig.7, RATES makes some errors in estimating the trust of nodes that adopt good behaviors with a probability P=0.7; but compared to existing approaches, RATES commits the smallest margin of error. We can confirm this in Fig.10, which shows that RATES is the scheme with the lowest false positive rate compared to other schemes.

In general, the strong resilience of our approach to false positives and false negatives is achieved through our local penalty, local reward, flexible global penalty and trust chaining.

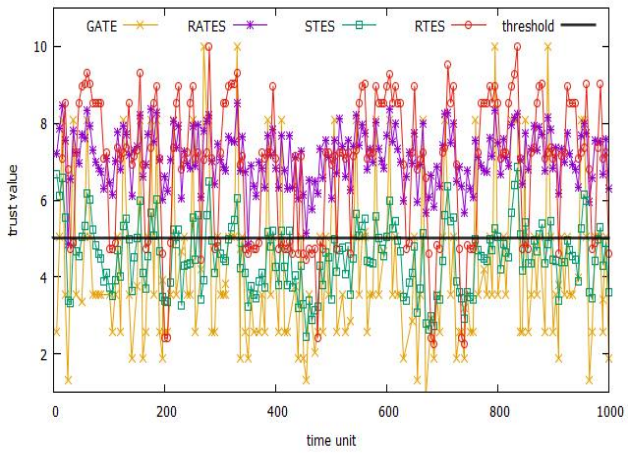


Fig.7. Bad behaviors detection: Case of reliable node (P=0.7)

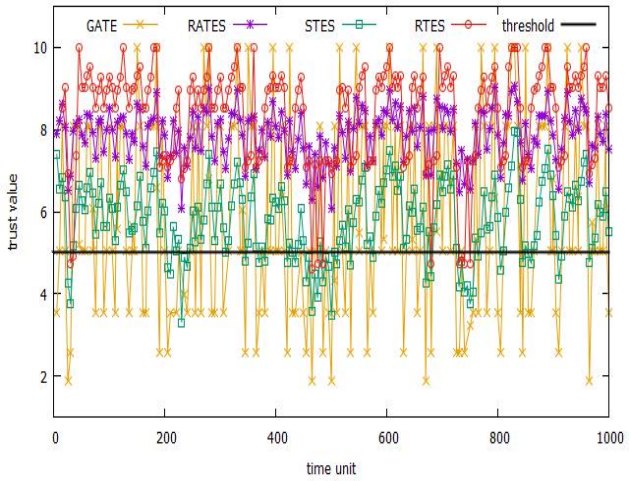


Fig.8. Bad behaviors detection: Case of reliable node (P=0.8)

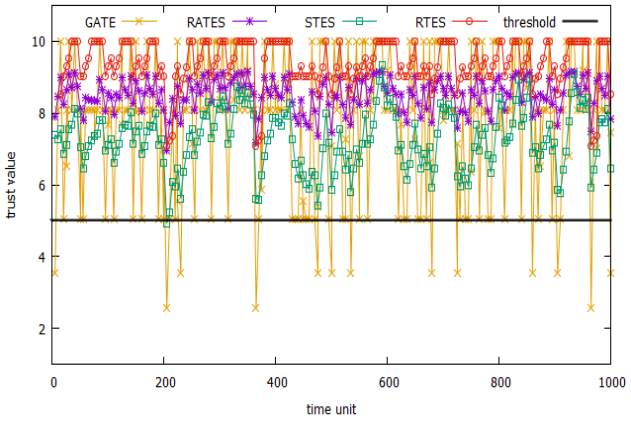


Fig.9. Bad behaviors detection: Case of reliable node (P=0.9)

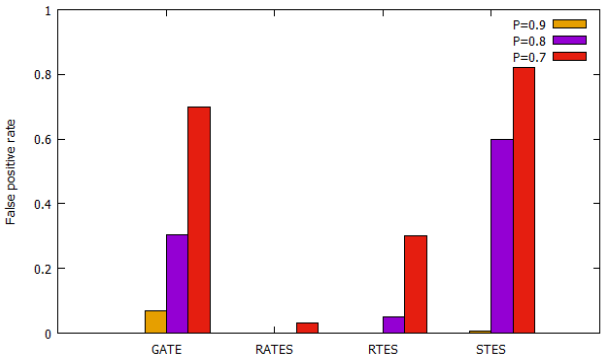


Fig.10. False positive rate

6.2. On-Off Attack Detection

In this section, we evaluate and compare RATES in presence of compromised nodes initiating on-off attack. We define two modes of on-off attack:

- Mode 1: The compromised node frequently attacks with respectively probabilities P=0.9, 0.8, 0.7 and 0.6 of obtaining an On-unit during a time window.
- Mode 2: The compromised node rarely attacks with respectively probabilities P=0.4, 0.3, 0.2 and 0.1 of obtaining an On-unit during a time window.

The diagrams presented in Fig.11 compare our approach RATES to GATE, STES, RTES from the point of view of rate detection of different On-Off attacks modes. We can observe that globally, for each of the approaches, the on-off

attack detection rate decreases as the attack frequency decreases. But once again, our RATES approach stands out from the others by offering a better on-off attack detection rate. This efficiency of RATES is due to the fact that we alternate the allocation of local rewards and penalties based on variations in the number of successful and failed interactions between two consecutive time units. Furthermore, to prevent malicious nodes that will try to rapidly increase their trust just by slightly increasing their number of successful interactions during a short interval of time, we integrate trust chaining so that the current trust value is influenced by the previous trust value. Finally, because of the misbehavior frequency, we integrate a flexible global penalty factor whose severity increases as a node has a high misbehavior frequency. This further enhances accuracy when detecting on-off attacks. All these components integrated in RATES contribute to make it more robust, more accurate and more flexible compared to existing approaches.

6.3. Defense against Bad-mouthing and Ballot Stuffing attacks

In bad-mouthing attack, a set of compromised neighbors transmit bad recommendations aimed to decrease trust of a legitimate node while in the ballot stuffing attack, these bad recommendations are intended to increase the trust of a compromised node. In this section, we evaluate the resilience of our approach based on the percentage of bad recommendations delivered to evaluator node. This percentage varies between 10 and 50% for 20 recommendations generated for each indirect trust assessment. The proposed defense strategy for filtering bad recommendations being the same for the bad mouthing and ballot stuffing attack, we will only present the results regarding bad mouthing attack. Thus, for our simulations, we consider that an honest neighbor randomly generates recommendations between 5 and 10 with respect to a legitimate node whereas a dishonest neighbor randomly generates recommendations between 2 and 4 with respect to a legitimate node before passing it to the evaluator node. The simulation parameters are summarized in table 2.

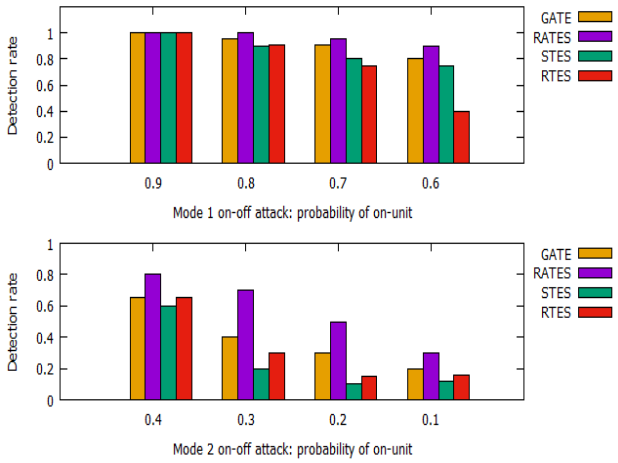


Fig.11. Detection rate of On-Off attack

Table 2. Simulation parameter for bad mouthing attack

Parameters	Value
Number of recommendations of each evaluation	20
Number of evaluations	100
Trust threshold	5
Z	1.96
Honest recommendations	Generated Between [5;10]
Dishonest recommendations	Generated Between [2;4]

To show the efficiency of our filtering model, we compare it to the models proposed in [10], and [13] in presence of 10, 20, 30, 40 and 50% of bad recommendations. We respect the optimal performance conditions of the compared approaches by setting their detection factors to 1 for the other two approaches and Z=1.96 for our approach.

As shown in Fig.12, in presence of 10% to 40% of dishonest recommendations (BR), our model succeeds to correctly estimate indirect trust. On the other hand, in presence of 50% of dishonest recommendations, the estimation of indirect trust is skewed. The graph in Fig.13 shows that for all approaches, the detection rate decreases as the percentage of bad recommendations increases. However, our model RATES has a better detection capacity compared to others. In the worst case, our model succeeds in filtering 27% of bad recommendations against 10% for Gate and 7% for STES.

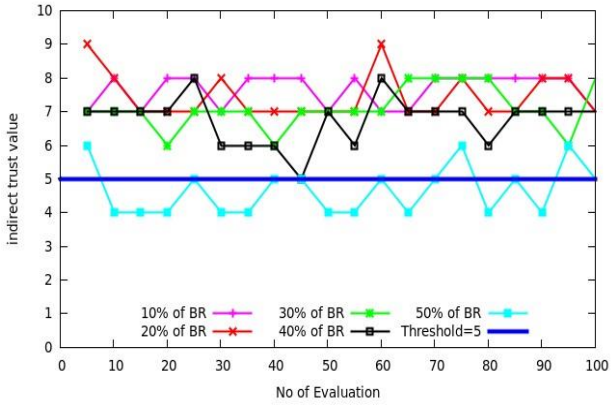


Fig.12. Indirect trust values in presence of bad recommendations (BR)

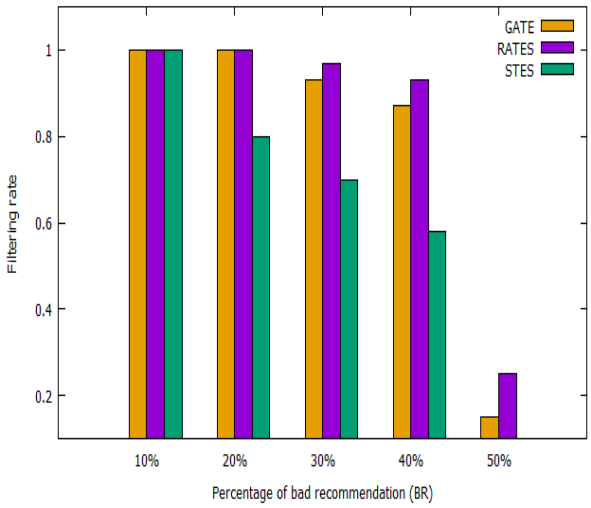


Fig.13. Detection rate of dishonest recommendations

In summary, the results of the multiple simulations carried out prove the efficiency and robustness of our RATES approach, which on the whole surpasses existing approaches from the point of view of detecting persistent and on-off attacks. The good performance obtained by RATES is mainly explained on the one hand by the alternate application of local reward and penalty factors and on the other hand by the application of a very flexible global penalty based on the misbehavior frequency. This makes RATES stable and less sensitive to false positives and false negatives. Finally, through the simple method of establishing the confidence interval described, RATES manages to resist the bad mouthing attack by improving the filtering of fraudulent recommendations and by making the indirect trust value obtained more realistic.

7. Conclusions

In this paper, we have proposed a flexible and accurate trust estimation scheme based on reward and penalty called RATES. The RATES approach proposes a new flexible method of alternately integrating reward and penalty based on the misbehavior frequency when estimating the direct trust of nodes. Furthermore, based on the established confidence interval, the RATES approach improves the filtering of recommendations in order to produce more accurate indirect trust values. The mathematical theoretical analysis and simulations presented show the feasibility and applicability of our model in improving the protection of wireless sensor networks against internal attacks initiated by malicious nodes. With the accuracy of the trust values obtained, our RATES model can be integrated into the routing protocols used in wireless sensor networks in order to improve the choice of nodes to be used as relays for routing data through the network. Thus, nodes with high trust values will be chosen as a priority when establishing routing paths.

The major disadvantage of our model is that it is designed for a flat, static and homogeneous wireless sensor network. Increasingly, however, in order to save the nodes energy or to better cover the monitored area, WSNs are organized in clusters containing nodes with different features, different roles and that can move from one cluster to another.

For future work, a promising line of research would be to propose a trust management model suitable for heterogeneous and hierarchical wireless sensor networks that takes into account the mobility and energy of nodes when

evaluating their trust. In consideration of the growing exploits of machine learning in various aspects of security, another line of research to be considered would be to design a trust management model based on machine learning.

References

[1] Wang Yong, Attebury Garhan and Ramamurthy Byrav.. A Survey of Security Issues In Wireless Sensor Networks. IEEE Communications Surveys and Tutorials. 8:2 p. 2-23. , Second Quarter. 2006

[2] Lopez Javier, Roman Rodrigo, Agudo Isaac and Fernandez Gago Carmen. Trust management systems for wireless sensor networks: Best practices. Computer Communications. 33:9 p. 1086-1093. 2010

[3] Ishmanov Farruh, Kim Sung and Nam Seung Yeob. A Robust Trust Establishment Scheme for Wireless Sensor Networks. Sensors. 15:3 p. 7040-7061. 2015.

[4] Jadidoleslamy Hossein. TMS-HCW: A trust management system in hierarchical clustered wireless sensor networks. Security and Communication Networks. Security and Communication Networks. 8:18 p. 4110-4122. 2015.

[5] Sivagurunathan S., K. Prathapchandran and Thirumavalavan Aarthi. Authentication Using Trust to Detect Misbehaving Nodes in Mobile Ad hoc Networks Using Q-Learning. International Journal of Network Security & Its Applications. 8: p. 47-64. 2016.

[6] Basan Alexander, Barannik Elena and Makarevich Oleg. Development of the Hierarchal Trust management System for Mobile Cluster-based Wireless Sensor Network. P. 116-122. In Proceedings of the 9th International Conference on Security of Information and Networks (SIN '16). Association for Computing Machinery, New York, NY, USA.2016.

[7] Salehi Mohsen and Karimian Jamal. A Trust-based Security Approach in Hierarchical Wireless Sensor Networks. International Journal of Wireless and Microwave Technologies. 7: p. 58-67. 2017.

[8] Wang Jian, Jiang Shuai and Fapojuwo Abraham. A Protocol Layer Trust-Based Intrusion Detection Scheme for Wireless Sensor Networks. Sensors. 17: p. 1-19. 2017.

[9] He Daojing, Chen C., Chan Sammy, Bu Jiajun and Vasilakos Athanasios. ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks. IEEE transactions on information technology in biomedicine: a publication of the IEEE Engineering in Medicine and Biology Society. 16: P. 623-32. 2012.

[10] Sahoo Rashmi, Ray Sudhabindu, Sarkar Souvik and Bhoi Sourav. Guard against trust management vulnerabilities in Wireless Sensor Network. Arabian Journal for Science and Engineering. 43: p.1-23 2018.

[11] Alzaid Hani, Alfaraj Manal, Ries Sebastian, Jøsang Audun, Albabtain Muneera and Abuhaimed, Alhanof.. Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review. IFIP Advances in Information and Communication Technology.401: P. 66-82. 2013.

[12] Shaikh Riaz, Jameel Hassan, d'Auriol Brian, Lee Heejo, Lee Sungyoung and Song Young Jae. Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks. IEEE Trans. Parallel Distrib. Syst.. 20(11): p.1698-1712. 2009.

[13] Ishmanov Farruh, Kim Sung and Nam Seung Yeob. A Secure Trust Establishment Scheme for Wireless Sensor Networks. Sensors. 14: P. 1877-97. 2014.

[14] Ganeriwal Saurabh, Balzano Laura a,d Srivastava Mani. Reputation-based framework for high integrity sensor networks. ACM Trans. Sen. Netw. 4:3. 2003

[15] Khan Tayyab, Singh Karan, Son Le, Abdel-Basset Mohamed, Long Hoang, Singh Satya and Manjul Manisha. A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks. IEEE Access. PP. 1-20. 2019.

[16] P. Raghu Vamsi and Krishna Kant. Self-Adaptive Trust Model for Secure Geographic Routing in Wireless Sensor Networks. International Journal of Intelligent Systems and Applications (IJISA).7:3 pp.21-28, 2015.

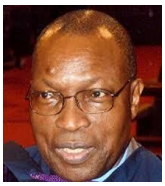
[17] Randhawa Sukhchandan, Jain Sushma and Ritu. Trust Models in Cloud Computing: A Review. International Journal of Wireless and Microwave Technologies. 7. 2017.

[18] Matthew Kiran and Md Abdul. An Effective Way of Evaluating Trust in Inter-cloud Computing. International Journal of Computer Network and Information Security. 9: pp 36-42. 2017.

Authors' Profiles

Audrey NANGUE, is a Ph.D student in Computer Science from the University of Dschang (Cameroon). His main research interests include data security in wireless sensor networks and Secure routing protocols.

Elie FUTE T., is currently a lecturer in the Department of Mathematics and Computer Science of the University of Dschang, and HOD of the Department of Computer Engineering at the Faculty of Engineering and Technology of the University of Buea. Modeling, Simulation, optimization, security and wireless sensor networks are his major research specialities.



Emmanuel TONYE, is currently professor in the Department of Electrical Engineering and telecommunications at the National Polytechnic School of Yaoundé I. His field of study is Multi-sensors, electromagnetism and antennas, data communication networks, security of telecommunications networks

How to cite this paper: Audrey NANGUE, Elie FUTE TAGNE, Emmanuel TONYE, "Robust and Accurate Trust Establishment Scheme for Wireless Sensor Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.6, pp.14-29, 2020. DOI: 10.5815/ijcnis.2020.06.02