True: A Trust Evaluation Service for Mobile Ad Hoc Networks Resistant to Malicious Attacks

Eduardo da Silva[1,3], Mehran Misaghi[2], Luiz Carlos P. Albini[3]
[1]Department of Informatics
Catarinense Federal Institute, IFC
PO Box 21-89.245-000
Araquari – SC. Brazil
[2]MEP – Research Department
Educational Society of Santa Catarina
[3]NR2 – Department of Informatics
Federal University of Paraná
PO Box 19.081 - 81.531-980
Curitiba – PR. Brazil
{eduardos, albini}@inf.ufpr.br, mehran@sociesc.org.br

JDIM
Journal of Digital Information Management

Abstract. *Trust evaluation is an essential service to ensure reliability on security relationships on networks, including Mobile Ad Hoc Networks (MANETs). However, the implementation of an effective trust evaluation service is very difficult in these networks, due to their dynamic characteristics. Though many trust evaluation services for MANETs can be found in the literature, they were not designed considering malicious attacks or were not evaluated under these attacks. This work presents TRUE, a distributed trust evaluation service for MANETs which creates a self-organized context-based trust network. To estimate the trustworthiness of other nodes, nodes form trust chains based on behavior evidences maintained within the context-based trust network. Periodically, nodes exchange trust information with the neighbors, providing an efficient method to disseminate these information through the network. Simulation results show that TRUE is very efficient on gathering evidences to build the trust networks, maintaining a small communication and memory overhead. Further, it is the first trust evaluation scheme evaluated under bad mouthing and newcomers attacks and it maintains its effectiveness in such scenarios.*

Categories and Subject Descriptors: **D.4.6 [Security and Protection]**; Authentication: **C.2.3 [Network Operations]**

General Terms: Mobile Adhoc-Networks, Network Security

Keywords: Trust Evaluation, Security, Attacks. Self-organization, MANETs

Received: 13 March 2012, Revised 28 April 2012, Accepted 8 May 2012

1. Introduction

In spite of the several researches in the recent years to cope the security vulnerabilities and treats on Mobile Ad Hoc Networks (MANETs), this area continues being one of the most challenging issues for such networks [29]. MANETs are highly vulnerable to security threats due to wireless communication and dynamic topology. The wireless communication channel allows adversaries to easily perform attacks, while the dynamic topology requires that all security mechanisms must be distributed. All these characteristics difficult the implementation of security applications for MANETs [31].

Though cryptography may be used to ensure communication security, it does not provide information about the reliability of the nodes [15]. Further, many cryptographic mechanisms, such as key management [16, 19], rely on some degree of pre-established trust between nodes. However, trust in any kind of open network is very difficult to be valued and has received a lot of attention from the security community [4].

Trust can be defined as *"the trustworthiness of a trustor, or howmuch it is willing to take the risk of trust, in a trustee"* [7]. In this context, trust management can be defined as a mechanism to allow nodes, without any previous interactions, to establish connections with a pre-defined level of trust among themselves [3]. Examples of using trust management include support in decisions as intrusion detection [1], authentication [11], access control [17], and isolation of misbehaving nodes for effective routing [18].

The use of trust evaluation techniques to mitigate security threats is very relevant in open networks [2]. In MANETs, trust can be used in routing strategies, distributed storage, location management, and key management or establishment. Though trust evaluation schemes are essential for several security services, most of schemes found in the literature for MANETs either did not consider or were evaluated under misbehavior attacks. Besides, the use of a non-secure trust evaluation scheme can harm the entire secure solution of the system. Further, the few schemes which considers the presence of malicious nodes are limited to a single network operation, such as routing.

This work presents TRUE (TRUst Evaluation service for MANETs) to support applications in a dynamic and autonomic way, while being able to resist to misbehavior attacks. In TRUE, each node creates a context-based trust network in a self-organized way to support and provide trust information within a predetermined context. The context-based trust network contains all trust information that a node has about other nodes in such a context. These information, or evidences, are gathered via direct interaction or via recommendation, considering the system security policies. The trustworthiness of a node is always locally computed, without any message exchange, based on the trust network of the node.

TRUE was evaluated in scenarios under two kinds of attacks: bad mouthing and newcomer ones. Bad mouthing attacks consist of malicious nodes providing dishonest trust evidences to defame good nodes or enhance trust values of bad ones [10]. Newcomer attacks consist of malicious nodes registering a new identity and assigning high trust values to it. If the trust evaluation scheme suffers from the newcomer attack, a malicious node might remove its bad history by registering itself with a new identity [25].

Simulations performed in Network Simulator version 2.34 (ns-2.34) confirm that TRUE is robust and efficient. Results show that trust evidences are quickly disseminated through the network and nodes are able to effectively estimate the trustworthiness of other nodes. Also, it is possible to notice that the scheme is resistant to bad mouthing and newcomer attacks, in which malicious nodes try to jeopardize other nodes.

The rest of the article is organized as follows: Section 2 lists the related work, their characteristics and limitations; Section 3 details the operation of the TRUE and its procedures; Section 4 contains the evaluation of the proposed service; finally, Section 5 contains the conclusion and future work.

2. Related Work

Several trust evaluation schemes have been proposed in order to support and maintain trust evidences of nodes in MANETs . In [14], it is proposed the Ant-Based Evidence Distribution (ABED), based on the swarm intelligence, which is claimed to be highly distributed and adaptive to nodes mobility. In ABED, nodes interact with each other through agents ("*ants*"), which are able to identify an optimal path to accumulate trust evidence. However, it was not evaluated under any type of attack.

In [26], a trust evidence evaluation scheme is proposed. It is modeled as a path problem in a direct graph. This scheme considers a source node as a trusted entity to support the infrastructure, violating the decentralized characteristics of MANETs. Further, trust and confidence values are binary represented rather than continuousvalued.

A concept of self-organizing trust-based physical-logical domains for grouping nodes and support for distributed control in the network is presented in [28]. It introduces a security architecture based on trust-domain which uses trust to establish keys between nodes and to establish secure distributed control in MANETs. Nodes use trust information to form groups and to establish pair-wise keys in the groups. Even though authors describe trust formalization and trust evaluation, the scheme was not evaluated under attacks, and it is suitable just for establishing group keys.

A distributed reputation evaluation which claims to prevent malicious nodes from entering the trusted community was proposed in [5]. However, no specific attack model was addressed. In [32], a trust calculation algorithm was proposed, to evaluate trust based on a trust certificate graph. However, the use of trust certificates implies in digital signatures verification within a trusted node or entity.

Trust evaluation schemes have also been used to support other applications in MANETs, such as authentication and packet routing. In [8], for example, it is proposed a trust evaluation scheme to support secure authentication for MANETs. It assumes that nodes form groups with primary and backup certificate authority servers inside.

Trust values of nodes are augmented from their previous trust values using a Markov chain trust model. Then, the node with the highest trust value in the group is selected as the certificate authority server, and the node with the second highest trust value is selected as the backup server. However, the scheme creates a centralized certificate authority, which is not desirable in MANETs.

In [13], is presented SORI, which uses cooperation incentive based on reputation, stimulating packet forwarding and disciplining selfish nodes through punishments. In SORI, the reputation of a node is calculated using objective metrics, such as effectiveness in packet forwarding. However, it considers that the reputation of a node is only useful to the physical neighbors of such node. This characteristic makes the implementation of SORI to support other applications very difficult. Other schemes that use reputation and trust

estimation to enforce packet routing can be found in the literature [6,9,20]. However, none of them were evaluated under attacks and are limited only to support routing strategies.

In [27] is presented a trust model which claims to be resistant to slander attacks, a variance of the bad mouthing ones. Such a scheme provides nodes with a mechanism to build a trust relationship with their neighbors. However, the scheme just allow the nodes to evaluate the trustworthiness of direct neighbors. Thus, the solution is not suitable for applications that require trust information of nodes out of the radio range. In [23] is presented a trust evaluation scheme which considers malicious attacks. However, it is designed just to secure routing operations and detects only malicious nodes acting in the routing strategies.

3. TRUE: TRUst Evaluation service for MANETs

This section describes the operations of the proposed trust evaluation scheme, called TRUE (TRUst Evalution service for MANETs). Initially, the notation and the system model which is used through the rest of this article. Thus, it is presented how nodes create their own context-based trust network graphs and how they can update these graphs, gathering evidences from other nodes. Then, it is described how nodes evaluate trust values of other nodes, and how they can integrate the information from different nodes.

3.1 Notation and System Model

Table 1 summarizes the notation used in the rest of the article.

Notation	Description
n_i	identity of node *i*
$TV_{(n_x,\ n_v)}$	trust value from a trustor *nx* to a trustee *nv*
$TC^{x}_{(n_x,\ n_v)}$	trust chain *x* from node *nx* to node *nv*
$a \parallel b$	information *a* concatenated with information *b*
G_{tr}	context-based trust network graph
G^{x}_{tr}	context-based trust network graph of node *nx*
$\lvert Z \rvert$	size of a given set *Z*
$n_a \rightarrow n_b$	node *na* trusts node *nb*
Δ_{Tex}	interval of information exchanges
α	threshold of trust exchanges
β	threshold of trust evaluations
$\cong$	approximately

Table 1. Notation

Due to the unique characteristics of MANETs, some concepts and features of trust should be carefully defined [12,24]:

• *trust is not necessarily transitive*: if node n_a trusts node n_b, and node n_b trusts node n_c, it is not true that node n_a trusts node n_c, but it might be considered.

• *trust is asymmetric*: the fact that node n_a trusts node n_b does not necessarily means that node n_b also trusts node n_a.

• *trust is subjective*: as trust is inherently a personal opinion, two nodes can often evaluate trustworthiness about another node differently.

• *trust is context-dependent*: node n_a may trust in node n_b to provide a routing service but it does not trust in node *nb* to provide another service.

• *trust evaluation should be fully distributed*: trust management schemes must not rely on a trusted third party to determine the trustworthiness of nodes.

• *trust management should consider non-cooperative nodes*: resource-restricted environments, like MANETs, are composed by nodes which can present selfish behavior.

• *trust value must be continuous*: the level of trust in a node must be measured by a continuous real value.

• *trust is dynamic*: as the trust value represents a personal opinion, nodes can change its evaluation about other nodes.

Based on these concepts, TRUE is proposed. The service focuses on self-organized mobile ad hoc network consisting of a set of N nodes identified by $n_1, n_2, ..., n_n$. Without losing generality, nodes are considered to have similar functionalities, contributing to network operations and maintenance. In TRUE, each node creates a context-based trust network represented by a direct graph $G_{tr} = (V_{tr}, E_{tr})$, in which the vertices V_{tr} are the nodes and edges E_{tr} represent the trust relationship between them. All trust information stored in the trust network is related with a context, and cannot be evaluated out of it. For simplicity, this article considers only one context at a time. However, it is trivial to represent additional context information on context-based trust networks.

3.2. Building context-based trust networks

When joining the system, each node creates its own trust networks $G^{i}_{tr} = (V^{i}_{tr}, E^{i}_{tr})$ in a self-organized way. Initially, nodes have knowledge only about nodes with which they have direct trust relations, and only such data are stored in the trust network. Then, in predetermined time intervals (ΔT_{ex})), nodes exchange trust evidences stored in their local trust network with their physical neighbors. Thus, trust values will quickly travel through the network following an epidemic behavior [21,30].

Trust information exchange occurs as follows :

• In ΔT_{ex} intervals, each node n_x creates a Trust Information Message, denoted by $TIM = [G^{x}_{tr} \parallel n_x \parallel timestamp]$. This message contains all trust evidences stored in its context-based trust network, its identity, and a timestamp.

• After creating it, node n_x sends this message to all of its neighbor.

• Upon receiving a TIM message, node n_v evaluates the relevance of the received evidences by calculating the trustworthiness of node n_x($TV_{(n_v,\ n_x)}$). Then, it decides whether it accepts or not such evidences, based on local policy rules. For that, each node has a threshold value, α, in which it accepts trust evidences iff. $TV_{(n_v,\ n_x)} \geq \alpha$.

• If n_v accepts the trust evidences, it incorporates the received information on its context-based trust network.

• Otherwise, trust evidences are discarded.

3.3 Trust Evaluation

To evaluate the trust on node n_u, node n_x must either have a direct connection with node n_u in G_{tr}^{x} or it finds at least one trust chain (TC) from n_x to n_u in G_{tr}^{x}. Trust chains represent a transitive trust from *nx* to n_u. The trust network graph G_{tr}^{x} is depicted in Figure 1. As node n_x can find several different trust chains between itself and n_u in G_{tr}^{x}, each chain is denoted as $TC^{i}_{(n_x,\ n_u)}$.

If n_x has a direct trust with n_u, only this value is considered in the trust evaluation. Considering the example of Figure 1, it is possible to notice that n_x has a direct trust relationship with n_q, and it has 80%of confidence in services provided by n_q in this context. However, in this example n_x does not have a direct trust relationship with n_u. Hence, it tries to find a trust path in G_{tr}^{x}, estimating the trustworthiness of each chain, and calculating a weighted mean for each one.

Upon finding a chain, node n_x must compute its trust. Consider n_1 to n_m the *m* intermediary nodes in the *i*th trust chain, denoted as $TC^{i}_{(n_x,\ n_u)}$, equation 1 estimates the trustworthiness of $TC^{i}_{(n_x,\ n_u)}$:

$$TC^{i}_{(n_x,n_u)} = TV_{(n_x,n_1)} \times \prod_{j=1}^{m-1} TV_{(n_j,n_{j+1})} \times TV_{(n_m,n_u)} \qquad (1)$$

Returning to figure 1, there are several chains between n_x e n_u, for example:

1. chain ($n_x \rightarrow n_q \rightarrow n_m \rightarrow n_u$), trust chain value
$TC^{1}_{(n_x,\ n_u)} = 0.8 \times 0.6 \times 0.7 = 0.336$;

2. chain ($n_x \rightarrow n_q \rightarrow n_b \rightarrow n_f \rightarrow n_m \rightarrow n_u$), trust chain value
$TC^{2}_{(n_x,\ n_u)} = 0.8 \times 0.3 \times 0.5 \times 0.8 \times 0.7 = 0.067$.

Furthermore, nodes can use a threshold value for each edge of the trust chain (β value). If at least one edge of the trust chain has a trust value below this threshold, the chain is disconsidered before even compute the trust chain value. For example, if node n_x consider $\beta > 0.4$, it would discard chain 2 of the above example, as it has an edge with trust value equals to 0.3.

After calculating the trust value for all chains, the trust value $TV_{(n_x,\ n_u)}$ can be calculated applying a weighted mean, as follows (equation 2):

$$TV_{(n_x,n_u)} = \frac{\sum_{i=1}^{k} \left(TC^{i}_{(n_x,n_u)} \times 1 \Big/ \left| TC^{i}_{(n_x,n_u)} \right| \right)}{\sum_{i=1}^{k} \frac{1}{\left| TC^{i}_{(n_x,n_u)} \right|}} \qquad (2)$$

The weighted mean reduces the impact of transitivity in trust chains. In fact, the greater the chain, the less reliable it is. Thus, this method aims to privilege small chains, following a social perspective.

4. Evaluation

The Network Simulator(NS) version 2.34 was used to evaluate the performance and effectiveness of TRUE. Simulations were made considering both honest and malicious nodes. Malicious nodes alter trust values of other nodes unpredictably and arbitrarily aiming to jeopardize the system.

In the simulations, 100 nodes use the IEEE 802.11 with distributed coordination function (DCF) as the medium access control protocol. The radio propagation follows the two-ray ground propagation model and the communication range is 120m. Nodes move on an area of 1000m x 1000m, following the random waypoint model with a maximal speed of 20 m/s, and pause time of 20s. The total time of simulations is 2000s and results are averages of 35 simulations with 95% of confidence interval.

During network formation, each node randomly generates trust values for the nodes it trusts. Initial trusts relations follow a power-law distribution, in which only few nodes have many trust relationships (at most 15). The power-law distribution correctly approximates the trust operation in dynamic networks, as P2P and MANETs [22]. Then, trust values are set randomly following a normal distribution of continuous values from 0 to 1. The exchange information interval ΔT_{ex} is set to 10 seconds.

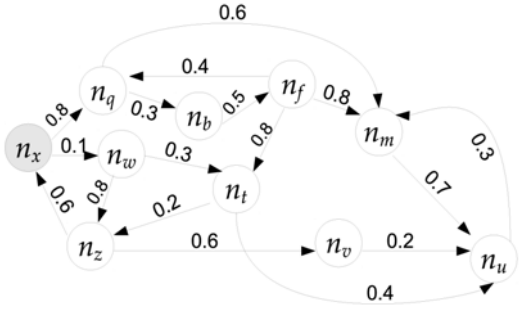


Figure 1. Example of trust chain G_{tr}^{x} from node n_x

TRUE was evaluated under three aspects: (*i*) the communication cost; (*ii*) the average calculated trust in trust networks and the percentage of nodes which are considered reliable in scenarios without attackers; (*iii*) the average calculated trust in trust networks and the percentage of nodes which are considered reliable in scenarios under bad mouthing and newcomer attacks.

4.1 Communication cost

The communication overhead is extremely small. TRUE uses only one hop messages to update trust networks, while it does not use any messages to build trust chains, i.e. it does not need any message to estimate the trust of other nodes. Note that it is even possible to piggyback update messages within other control messages. Thus, its communication cost depends exclusively on update messages.

Moreover, it is possible to increase ΔT_{ex} to reduce its communication cost. This function can be useful to postpone the battery exhaustion of a node. However, the time to disseminate trust evidences depends directly on ΔT_{ex}, a higher ΔT_{ex} implies on a higher delay to disseminate evidences.

The memory overhead is also small. Nodes must maintain only the context-based trust networks. On the other side the computational overhead to maintain the scheme updated might be significant. Nodes must compute trust values for every TIM message received. If the node decides to accept a TIM message, it must recompute the entire trust network graph considering such information. Consequently, the computational overhead depends directly on ΔT_{ex} and on the number of neighbors each node has.

4.2. Scenarios without attackers

Considering scenarios without attackers, TRUE was evaluated varying the threshold for information exchanges (α) and threshold for trust chains values (β). It is expected that in scenarios with more rigorous threshold values, nodes will be able to obtain information about a smaller set of nodes and, consequently, to estimate the trustworthiness of fewer nodes.

Figure 2 shows the average calculated trust in context-based trust networks. Estimated trust values are also represented in Table 2. In scenarios with $\alpha = 0.1$ and $\beta = 0.1$, the average trust value is also approximately to 0.2 due to node accepting recommendations from nodes with small trust value. In this case, trust chains can be formed using unreliable nodes.

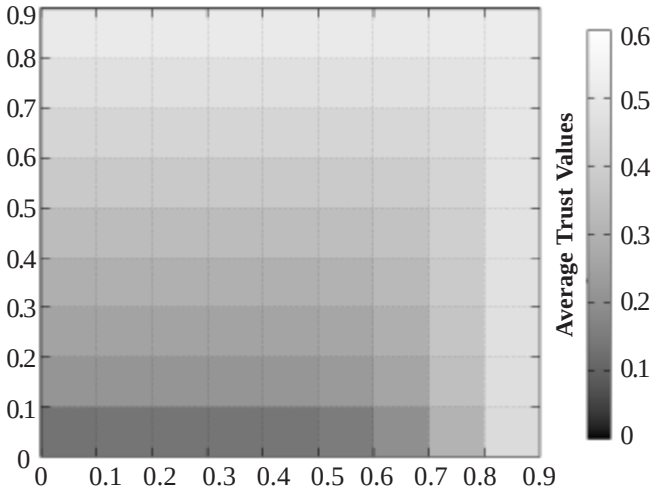


Figure 2. Average of estimated trust values

On the other hand, in scenarios with $\alpha = 0.9$ and $\beta = 0.9$, the average trust value is 0.53. It is possible to observe that β value has a higher impact on the results. With $\alpha = 0.6$, the average of calculated trust values is always higher than 0.4, independent of β. It is important to point out that the objective of the scheme is not to increase the trustworthiness of nodes, but to estimate it.

Figure 3 shows the percentage of nodes which are considered reliable by each node according to α and β values. Percentage of reliable nodes are also represented in Table 3This result is directly related with the ones presented in Figure 2. In scenarios with both $\alpha \leq 0.4$ and $\beta \leq 0.5$, the percentage of nodes which are considered reliable is higher than 95%. If $\alpha = 0.8$, the percentage of trust nodes is around 30%. If $\alpha = 0.9$ and $\beta = 0.9$, this percentage is close to 15%.

Table 4 shows the average time (in seconds) necessary to propagate a trust information through the network and the average size of the context-based trust networks, both considering the threshold for information exchanges (α). Note that the time to disseminate trust information is smaller with $\alpha = 0.0$ or $\alpha = 0.9$ and it is higher with $\alpha = 0.4$ and $\alpha = 0.5$. It occurs because with $\alpha = 0.0$ nodes accept trust evidences from any other node. Thus, data will be

β	α									
	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
0.0	0.07	0.19	0.23	0.27	0.31	0.35	0.40	0.44	0.49	0.52
0.1	0.07	0.19	0.23	0.27	0.31	0.35	0.40	0.44	0.49	0.52
0.2	0.07	0.19	0.23	0.27	0.31	0.35	0.40	0.45	0.49	0.52
0.3	0.08	0.19	0.23	0.27	0.31	0.35	0.40	0.45	0.49	0.52
0.4	0.08	0.19	0.23	0.27	0.31	0.35	0.40	0.45	0.49	0.52
0.5	0.09	0.20	0.24	0.28	0.31	0.35	0.40	0.45	0.49	0.52
0.6	0.11	0.21	0.25	0.29	0.32	0.36	0.40	0.45	0.49	0.52
0.7	0.19	0.27	0.30	0.33	0.35	0.38	0.41	0.45	0.49	0.52
0.8	0.36	0.39	0.40	0.42	0.43	0.44	0.45	0.47	0.49	0.53
0.9	0.51	0.52	0.52	0.52	0.52	0.52	0.52	0.52	0.52	0.53

Table 2. Average of estimated trust values - Graphic values

β	α									
	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
0.0	99.00	99.00	99.00	98.79	97.06	90.48	75.61	52.76	31.11	15.70
0.1	99.00	99.00	99.00	98.79	97.06	90.48	75.61	52.76	31.11	15.70
0.2	99.00	99.00	99.00	98.79	97.06	90.48	75.58	52.73	31.09	15.68
0.3	98.93	98.95	98.96	98.76	96.99	90.41	75.54	52.66	31.06	15.67
0.4	98.48	98.54	98.51	98.33	96.71	90.23	75.33	52.56	31.01	15.64
0.5	96.99	97.07	97.05	96.92	95.64	89.60	74.93	52.28	30.83	15.54
0.6	92.62	92.73	92.85	92.75	91.68	86.84	73.82	51.71	30.42	15.32
0.7	79.23	79.59	79.92	79.95	79.09	75.53	66.24	49.56	29.53	14.99
0.8	50.71	50.78	50.94	51.07	51.09	50.22	46.84	38.90	27.90	14.71
0.9	17.41	17.41	17.42	17.42	17.42	17.44	17.44	17.41	16.94	14.58

Table 3. Percentage of reliable nodes without attackers - Graphic values

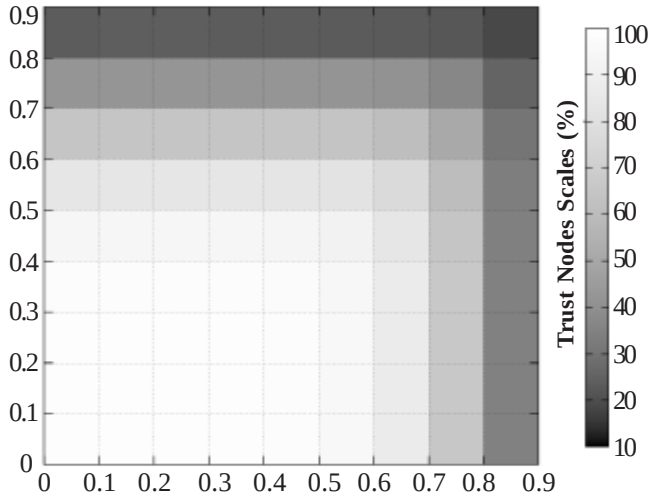


Figure 3. Percentage of reliable nodes without attackers

exchanged very quickly. At the other extreme, if $\alpha = 0.9$, nodes accept trust evidences only from very close friends. In this case, even if it does not have many evidences stored locally, it will not accept information from other nodes. Also, increasing the value of α, less information is exchanged and the trust networks are smaller, i.e. fewer nodes are locally stored in context-based trust networks.

4.3 Scenarios considering attackers

TRUE was also evaluated in scenarios under two kinds of attacks: bad mouthing and newcomer (or Sybil) attacks. Bad mouthing attacks consist of malicious nodes providing dishonest trust evidences to defame good nodes or enhance trust values of bad ones [10]. Newcomer attacks consist of a malicious node registering a new identity and assigning high trust values to it. If the trust management suffers from the newcomer attack, a malicious node can remove its bad history by registering itself with a new identity [25]. In all scenarios, attacks start after nodes build their trust networks.

First, TRUE was evaluated under bad mouthing attacks. In such attacks, malicious nodes change the value of other nodes to 1.0. It was also considered that malicious nodes can perform an attack in collusion, in which several attackers choose the same node to change the trust value.

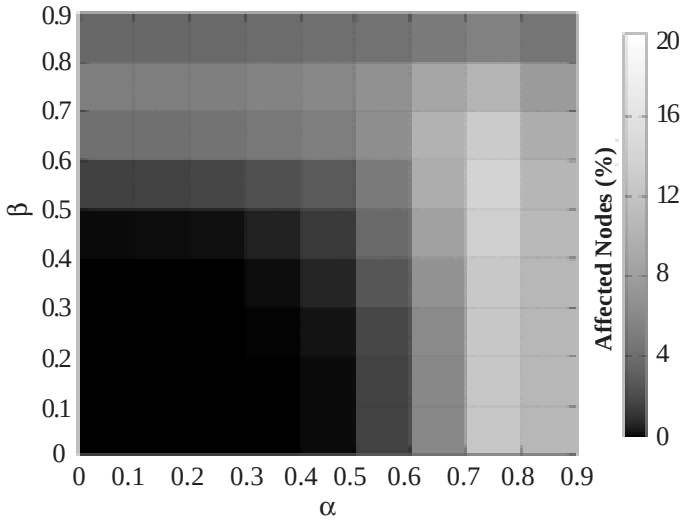
α	Time (sec.)	Nodes (%)
0.0	198.51	100.00%
0.1	713.54	99.99%
0.2	801.49	99.96%
0.3	885.14	99.92%
0.4	936.97	99.35%
0.5	926.96	96.94%
0.6	878.08	92.57%
0.7	768.51	78.98%
0.8	598.22	50.37%
0.9	281.08	17.34%

Table 4. Time to disseminate trust evidences and percentage of nodes in trust networks

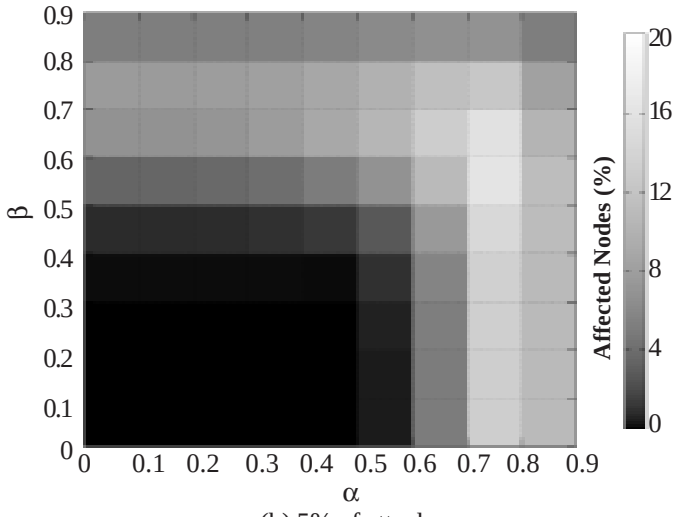
Figure 4 shows the impact of bad mouthing attacks in the TRUE. Note that in scenarios with small α and β the percentage of affected nodes is close to 0, as all nodes already trust on almost all nodes. Results also show that the worst case occurs with $\alpha \cong 0.7$ and $\beta \cong 0.7$ and 10% of attackers (Figure 4(c)). In this case, the percentage of compromised nodes are only 15%.

Table 5 shows how much the system is affected in scenarios with attackers, evaluating the variation of trust values calculated by nodes. Such an evaluation considers just scenarios with $\alpha = 0.0$, i.e scenarios in which nodes exchange trust evidences with all other nodes. Note that under 5% of attackers and $\beta = 0.9$, the variation of trust values is 0.3277. Also, in scenarios with 10% of attackers and $\beta < 0.6$, the variation is always below 0.2.

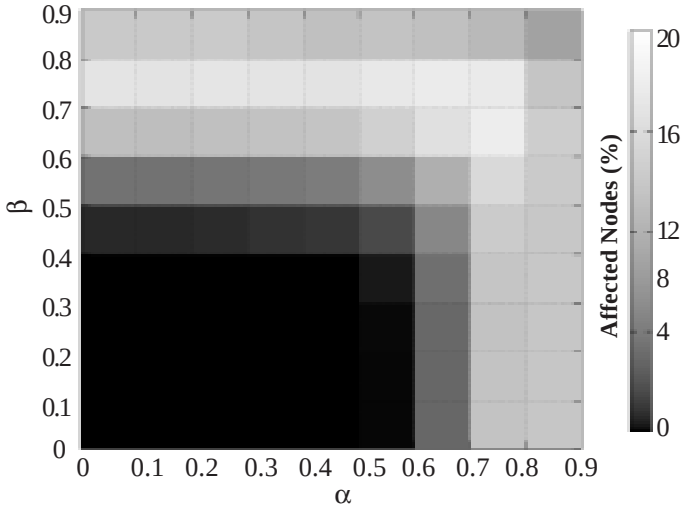
Finally, TRUE was evaluated under newcomers attack. In such attacks, after the system initialization and construction of trust networks, malicious nodes create a new identity and assign a high trust value to it. This attacks was also evaluated considering that malicious nodes act in collusion. Presented results on Figure 5 consider $\alpha \geq 0.7$, in which nodes accept recommendations only from more reliable nodes.



(a) 2% of attackers



(b) 5% of attackers



(a) 10% of attackers

Figure 4. Scenarios under bad mouthing attack

β	Attackers		
	2%	**5%**	**10%**
0.0	0.0055	0.0116	0.0158
0.1	0.0271	0.0503	0.0671
0.2	0.0365	0.0655	0.0868
0.3	0.0432	0.0803	0.1045
0.4	0.0561	0.0987	0.1290
0.5	0.0884	0.1355	0.1700
0.6	0.1619	0.2081	0.2390
0.7	0.3258	0.3403	0.3574
0.8	0.4300	0.4403	0.4339
0.9	0.2829	0.3277	0.3377

Table 5. Trust variation in scenarios under attack

Finally, TRUE was evaluated under newcomers attack. In such attacks, after the system initialization and construction of trust networks, malicious nodes create a new identity and assign a high trust value to it. This attacks was also evaluated considering that malicious nodes act in collusion. Presented results on Figure 5 consider $\alpha \geq 0.7$, in which nodes accept recommendations only from more reliable nodes.

Figure 5 shows increasing the values of α and β decreases the impact of the attack. In scenarios with with $\alpha = 0.9$, independent of value of β and the number of attackers, the percentage of affected nodes is always less than 10%. Also, in scenarios with $\alpha = 0.8$ and $\beta = 0.8$, about 25% of nodes are compromised. With $\alpha = 0.7$ and $\beta = 0.7$ and 10% of attackers, less than 10% of nodes are affected, showing that the proposed scheme is still valid even in the presence of several attackers.

5. Conclusions

Cryptography has been the main technique employed to provide security in MANETs. Besides, several cryptographic mechanisms rely on pre-established trust relations between nodes. However, trust is very difficult to be valued in MANETs. Several trust management schemes have been proposed [5,6,8,9,13,14,20,23,32], but none of them were evaluated in scenarios under misbehavior attacks. Attacks such as bad mouthing or newcomer, if

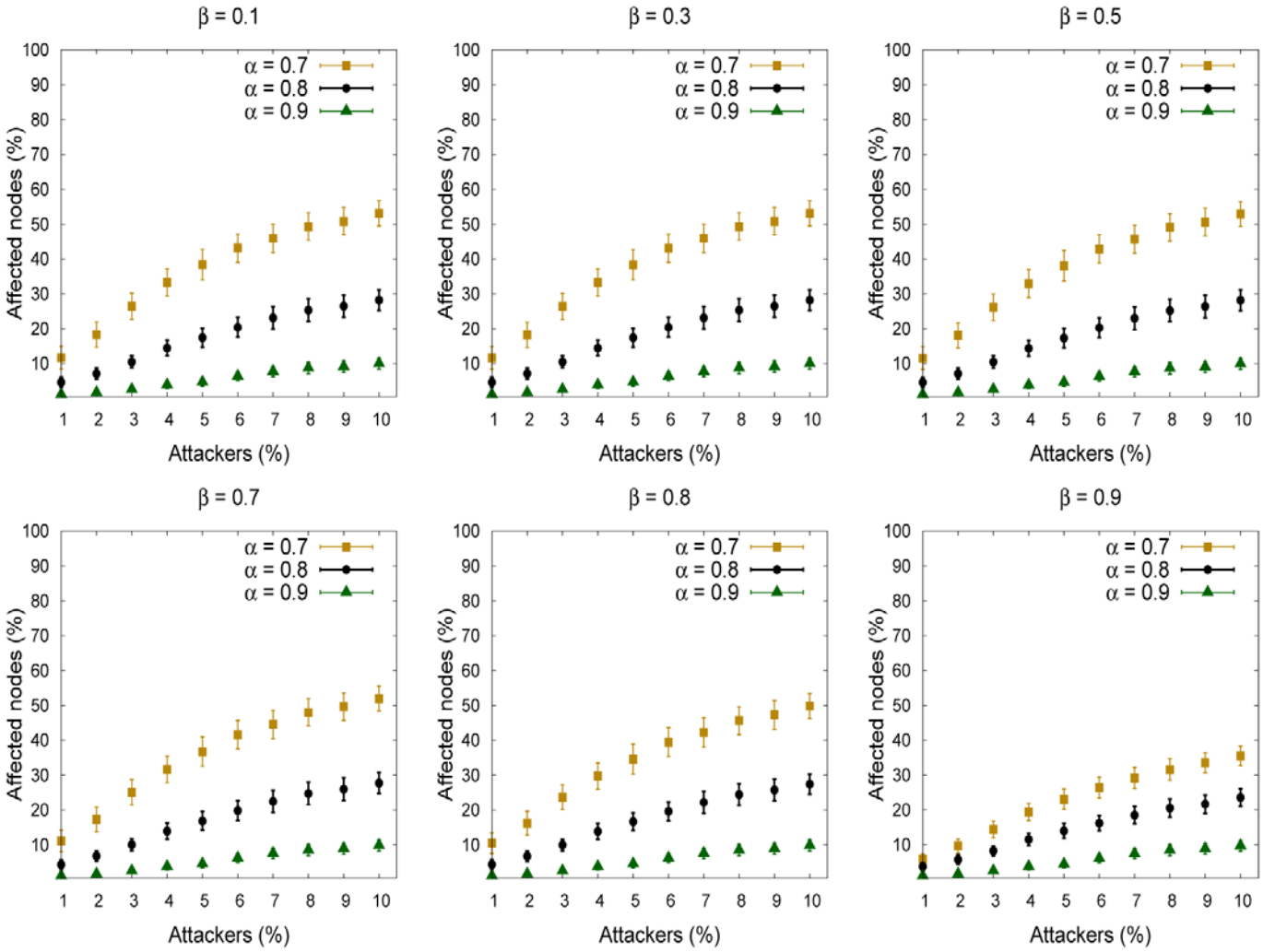


Figure 5. Scenarios under newcomer attack

performed successfully against the trust management system, can compromise the entire security of the system. Moreover:

• No specific attack model was addressed nor evaluated on [5,6,9,20].

• Some schemes are limited only to support routing strategies [6,9,20].

• Support for other applications is very difficult in [13].

This work presents a new trust evaluation scheme in which nodes create a context-based trust network, called TRUE (TRUst Evaluation service for MANETs). Such trust network contains trust information about other nodes, gathered via direct observations or via recommendations. Then, each node estimates the trustworthiness of other nodes which it does not have previous interaction building trust from the information stored in the trust network.

Simulation results show that TRUE is very efficient on gathering evidences to build the trust networks. Moreover, though the scheme has not been described to prevent attacks, it was evaluated under bad mouthing and newcomer attacks. The evaluations show that the scheme is able to resist up to 10% of attackers, if it is configured to take rigorous decisions. Future work includes the evaluation of the scheme under other kinds of attacks, such as on/off and conflicting behavior ones.

References

[1] Albers, P., Camp, O., Percher, J. M., Jouga, B., Mé, L., Puttini, R. S. (2002). Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches. In: Proceedings of the 1st International Workshop on Wireless Information Systems (WIS '02). p. 1–12. ICEIS Press (April)

[2] Beth, T., Borcherding, M., Klein, B. (1994). Valuation of trust in open networks. *In*: Proceedings of the 3rd European Symposiumon Research in Computer Security (ESORICS '94)). p. 3–18. Springer-Verlag, London, UK.

[3] Blaze, M., Feigenbaum, J., Keromytis, A. D. (1999). The role of trust management in distributed systems security. In: Secure Internet Programming. Lecture Notes in Computer Science, 1603, 185–210. Springer.

[4] Blaze, M., Feigenbaum, J., Lacy, J. (1996). Decentralized trust management. *In*: Proceedings of the 1996 IEEE Symposium on Security and Privacy (SP '96). p. 164. IEEE Computer Society.

[5] Boukerche, A., Ren, Y. (2008). A security management scheme using a novel computational reputation model for wireless and mobile ad hoc networks. *In*: Proceedings of the 5th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (PE-WASUN '08). p. 88–95. ACM.

[6] Buchegger, S., Le Boudec, J. Y. (2002). Performance analysis of the CONFIDANT protocol. *In*: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '02). p. 226–236. ACM, New York, NY, USA.

[7] Buskens, V. (2002). Social Networks and Trust. Kluwer Academic Publishers, Dordrecht, The Netherlands.

[8] Chang, B. J., Kuo, S. L., Liang, Y. H., Wang, D. Y. (2009). Markov chain-based trust model for analyzing trust value in distributed multicasting mobile ad hoc networks 59, 1846–1863.

[9] Dai, H., Jia, Z., Qin, Z. (2009). Trust evaluation and dynamic routing decision based on fuzzy theory for manets. JSW – Journal of Software 4(10) 1091–1101.

[10] Dellarocas, C. (2000). Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems. *In*: Proceedings of the 21th International Conference on Information Systems (ICIS '00). p. 520–525. Association for Information Systems, Atlanta, GA, USA.

[11] Ghosh, T., Pissinou, N., Makki, K. (2005). Towards designing a trusted routing solution in mobile ad hoc networks. *Mobile Networks and Applications* 10(6) 985–995.

[12] Golbeck, J. (2006). Computing with trust: Definition, properties, and algorithms. *In*: Proceedings of the 1st International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm '06). p. 1–7. IEEE Press (August).

[13] He, Q., Wu, D., Khosla, P. (2004). SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. *In*: Proceedings of the 2004 IEEE Wireless Communications and Networking Conference (WCNC '04). p. 825–830. IEEE Communications Society.

[14] Jiang, T., Baras, J. S. (2004). Ant-based adaptive trust evidence distribution in manet. In: Proceedings of the 24th InternationalConference on Distributed Computing Systems Workshops(ICDCSW'04). p. 588–593. IEEE Computer Society.

[15] Li, X., Slay, J., Yu, S. (2005). Evaluating trust in mobile ad hoc networks. *In*: Proceedings of the 2005 Workshop of International Conference on Computational Intelligence and Security (CIS '05). Springer.

[16] Lima, M. N., Pujolle, G., Silva, E., Santos, A. L., Albini, L. C. P. (2009). Survivable keying for wireless ad hoc networks. *In*: Proceedings of the 2009 IFIP/IEEE International Symposium on Integrated Network Management (IM '09). p. 606–613. IEEE Communications Society (Jun).

[17] Luo, H., Kong, J., Zerfos, P., Lu, S., Zhang, L. (2004). Ursa: ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Transaction on Networking (TON) 12(6) 1049–1063.

[18] Marti, S., Giuli, T. J., Lai, K., Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. *In*: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00). p. 255–265. ACM.

[19] Van der Merwe, J., Dawoud, D., McDonald, S. (2007). A survey on peer-to-peer key management for mobile ad hoc networks. ACM Computing Survey 39(1) 1.

[20] Michiardi, P., Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *In*: Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security. p. 107–121. Kluwer, B.V., Deventer, The Netherlands, The Netherlands.

[21] Mickens, J. W., Noble, B. D. (2005). Modeling epidemic spreading in mobile environments. *In*: Proceedings of the 4th ACM Workshop on Wireless Security (WiSe '05). p. 77–86. ACM, New York, NY, USA.

[22] Ripeanu, M., Foster, I., Iamnitchi, A. (2002). Mapping the gnutella network: Properties of large-scale peer-to-peer systems and implications for system. IEEE Internet Computing Journal 6.

[23] Sun, Y. L., Han, Z., Yu, W., Liu, K. J. R. (2006). A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. *In*: Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM '06). p. 1–13. IEEE Communications Society.

[24] Sun, Y. L., Yu, W., Han, Z., Liu, K. J. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications 24(2) 305–317.

[25] Sun, Z., Han, Y.L., Liu, K.J.R.: Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine p. 112–119 (2008)

[26] Theodorakopoulos, G., Baras, J. S. (2006). On trust models and trust evaluation metrics for ad hoc networks. IEEE Journal on Selected Areas in Communications 24 (2) 318–328.

[27] Velloso, P. B., Laufer, R. P., Duarte, O.C., Pujolle, G. (2008). A trust model robust to slander attacks in ad hoc networks. In: Proceedings of 17th International Conference on Computer Communications and Networks. (ICCCN '08). p. 1–6. IEEE Communications Society.

[28] Virendra, M., Jadliwala, M., Ch, M., Upadhyaya, S. (2005). Quantifying trust in mobile ad-hoc networks. *In*: Proceedings of the IEEE International Conference on Integration of Knowledge Intensive Multi-Agent Systems (KIMAS '05. p. 65–71. IEEE Computer Society.

[29] Wu, B., Chen, J., Wu, J., Cardei, M.: A survey on attacks and countermeasures in mobile ad hoc networks, chap. 12, pp. 103–136. Springer-Verlag, New York, NY, USA (2006)

[30] Zhang, X., Neglia, G., Kurose, J., Towsley, D.: Performance modeling of epidemic routing. Computer Networks 51(10), 2867 – 2891 (2007)

[31] Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Network 13 (6), 24–30 (1999)

[32] Zuo, Y., Hu, W.c., O'Keefe, T.: Trust computing for social networking. In: Proceedings of the 6th International Conference on Information Technology: New Generations (ITNG '09). pp. 1534–1539. IEEE Computer Society, Washington, DC, USA (2009)