Evaluation of the Energy Consumption Introduced by a Trust Management Scheme on Mobile Ad-hoc Networks

Andrea Lupia, Floriano De Rango
DIMES Dept., University of Calabria, Rende (CS), Italy
Email: {alupia, derango}@dimes.unical.it

Abstract—Nodes in mobile ad-hoc networks communicate each other using the wireless transmission. Many protocols have been proposed allowing the establishment of multi-hop paths to connect source and destination nodes. The absence of a physical link between the nodes and the multi-hop routing lead to a lack of security. Different typologies of attack effective against MANETs have been investigated thoroughly, and many solutions have been proposed to take the required countermeasures. Many of them are based on the cryptography, protecting data with digital signatures and hash chains, but they are not useful when a fair node is compromised later in time. Using a Trust Management Scheme can help in these situations, allowing to evaluate dynamically if a node is trustworthy or not. The computation of a trust value requires the monitoring of the interactions between nodes, therefore it has an effect on the energy consumption, which is an important issue of ad-hoc networks. Energy availability is limited for the nodes in a MANET, so the security measures that they adopt must not excessively increase the consumption.

Index Terms—MANET, Ad-hoc, SAODV, Security, Black hole, Gray hole, Trust, Energy, Power, Consumption

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) allow nodes to communicate each other in mobility. These networks are useful in many environments where the infrastructure is not available and cannot be installed. Two of the major issues of these networks concern the security of data exchanged and the energy consumption, and they are in contrast because to achieve a better security, more operations and data exchanges are needed, therefore more energy is consumed. On the security side, many proposals use encryption to avoid attacks from malicious nodes external to the network. Some works proposed trust management mechanisms to protect the network when an internal node is compromised. Regarding the energy consumption, its management in the network is critical, because the nodes are powered by batteries. In some works the energy consumption of wireless interfaces is evaluated, but actually the relationship between security and energy needed to run these measures in MANETs is not well investigated.

In our previous work in [1] we have evaluated the performance of a trust management scheme in the MANETs, analyzing the energy consumption introduced by this solution. In the following paragraphs a deeper analysis of the protocol reactions to the threats is done, using two different attack typologies. A more detailed description of the trust model adopted is presented, and new related works are taken into account.

The paper is organized as follows: the related work on the trust management, the attack typologies, the security and the energy consumption are described in the section II; in section III we present our proposal and the trust model adopted; the performance evaluation with the simulation results analysis and the conclusions are discusses in sections IV and V.

II. RELATED WORK

MANETs are used in very dynamic environments, so scalable routing protocols are needed to allow the communication between the nodes. Various routing metrics could be used, depending on which is the main aim of the protocol. In [2] a protocol combining link state and geographical routing is proposed. The link-state routing is used for short distances, while for long distances the geo-forwarding is applied. The results show the high scalability of the proposal for increasing number of nodes. Usually the routing in MANETs follows the shortest path metric, but many proposals took into account metrics to reduce interference [3], [4], [5], or based on multiobjective minimization using also the link duration probability [6], [7], [8].

A. Trust management

A trust management scheme could help to build safer paths. Trust could be described as the probability wherewith an agent will perform an action, before this action could be detected. The trust value of an agent could be defined through interactions and opinions of the other agents regarding an action of the agent. In previous works [9], [10], the SAODV protocol was extended by applying an Intrusion Detection Mechanism (IDM) and a Trust-Based Mechanism (TBM) to promote the collaboration of the cooperating nodes, penalizing the selfishness. The approach proposed in [11] manages the trust between nodes by using a monitoring module and a reputation handling module. Each node monitors the packet forwarding to its neighbors, computing the percentage of packets correctly forwarded with respect to the total number of them in a time interval. If an anomaly
is detected, the reputation manager will be informed. This is the main component for trust management, with four main activities, which are reputation information collection, reputation information formatting, reputation information maintenance and reputation information rating. The information collection is achieved in two different ways: by direct monitoring and by recommendations and accusations. The information formatting is about the exchanging of information about reputation between the nodes. When a change of reputation value about a node is detected by direct monitoring or by information received from other nodes, the information maintenance requires an update of the data stored in the nodes. The rating is a value between 0 and 1, and it takes in account the previous rating stored and the new interactions. The work proposed in [12] uses a Dynamic Trust Mechanism (DTM) to give higher importance to last interactions. The behavior of a MANET is not stationary, because it changes with time, so a trust updating algorithm is introduced to assure a slow rise, a rapid decreasing and a fading with time of the trust. The algorithm uses multiple constraints to achieve these properties. A collaborative filtering is also used to manage trust recommendation of a node. If many nodes have a similar trust value about a target node, then the recommendation credibility is high. The framework proposed in [13] uses 3 modules to monitor energy, interactions and packet integrity. These modules contribute to compute the final trust value of a target node. The node with the highest final trust value is elected as Certificate Authority. The multi-hop recommendation based trust management scheme (TRUISM) presented in [14] uses a probabilistic approach for calculating trust from multiple contradictory recommendations. Moreover, it implements an aging factor based on the time, the distance and the path reliability, to manage trust values over the time.

B. Attack typologies

Due to their decentralized way to exchange information, MANETs are subject to many kinds of attack. One possible categorization divides the attacks in two typologies: route-disruption and resource-consumption. Route-disruption attacks attempt to manipulate route messages with the aim of disrupting routes between nodes, while resource-consumption attacks try to consume energy, bandwidth or storage memory of the nodes in the network by transmitting fake or wrong packets. Attacks can be divided also in modification, impersonation and fabrication attacks [15]. Modification consists in altering routing packets content, modifying information contained in its fields. A node can impersonate one or many nodes, redirecting the traffic directed to it or generating loops in routes. Fabrication attacks are made by generating fake packets, containing wrong information to break links in the network, consuming the nodes energy and the network bandwidth. Malicious nodes can also take advantage of trust-based systems, spreading false information about other nodes [16]. They can use high trust values to recommend other malicious nodes, or low trust values for nodes behaving correctly. The survey done on MANET intrusion detection and prevention approaches presented in [17] categorizes the various attacks in two categories: passive and active attacks. The first category includes eavesdropping, traffic analysis and location disclosure, which are attacks that do not directly affect the functionalities of the network, but they can be dangerous in some scenarios. Regarding the active attacks, MANETs are prone to various threats. The sleep deprivation attack can consist in sending route requests with a destination address that does not exist in the network, or in sending many requests without waiting the time between them. It has a high impact on the energy consumption in the network. A malicious node performing a black hole attack tries to redirect the most of the traffic in the network through it, then dropping all the data packets that it receives. The gray hole attack is very similar to the previous one, but it does not drop all packets, but just a part of them, based on the data contained in the packet of probabilistically. An effective attack against reactive routing protocols in MANETs is the rushing attack, which consists in spreading the route requests quickly or advising them as the latest ones. Therefore, the malicious node takes part of the routes, because to control the packet overhead, only the first request is forwarded. The sybil attack is effective when there is not an authority to verify the identities, thus the malicious node can send requests using different identities (existing or not). The authors in [18] evaluated the effects and the detection of the wormhole attack in the MANETs. It consists in tunneling the packets received from a point of the network to another. For tunneled distances longer than the wireless range, the packet sent by the malicious node arrives before the packet that follows the multi-hop route, so the malicious node gains a powerful position in the network.

C. Secure protocols

As stated in previous paragraphs, ad-hoc networks suffer of many vulnerabilities. Lack of infrastructure and wireless communication expose the MANETs to internal and external attacks. Techniques like the cryptography and trust management reduce the threats of attacks. The Secure Ad-hoc On-demand Distance Vector protocol (SAODV) [19] protects the protocol packets by applying digital signatures to authenticate non-mutable information, and hash chains to ensure the accuracy of the hop count field. The authentication is obtained in a point-to-point manner: each node that receives the packet, verifies the packet signature, so it can authenticate the sender. The hop count changes at each forwarding of the packet, so the hash function is computed on the hop count field at each step. If the nodes are allowed to reply to route requests not directed to them but to another node for which they have an active path, they store the keys of that node attaching it to the route replies. A secure protocol based on Destination-Sequenced Distance Vector routing (DSDV) is the SEAD protocol [20]. It protects from multiple uncoordinated malicious nodes that try destroying the network by creating fake packets about the network status. It uses one-way hash chains
instead of asymmetric cryptography, so it can be used when the nodes have limited computational power. The Ariadne protocol [21] is based on the Dynamic Source Routing (DSR) protocol. To authenticate the routing packets, it allows using three different authentication schemes: symmetric keys shared by each pair of nodes, digital signatures or symmetric keys authenticated by a broadcast authentication scheme. Recently there are new proposals to improve security in MANETs. The work in [22] proposes a new approach to protect the network from tampering and node selfishness. It uses a payment mechanism to avoid selfishness, and a hop-by-hop identification with signatures to detect malicious behavior. Another work proposed in [23] secures the DSR protocol combining some features of the Ariadne extension with a trusted authority that could revoke the privileges of some nodes by disseminating revocation lists. Other approaches do not use the encryption to protect the network against malicious behaviors. The authors in [24] used a monitoring mechanism based on the statistical analysis of the protocol messages properties by means of supervised machine learning tools to detect DNS tunneling. In [25] a “honeypot” system is used to collect and analyze the data concerning the characteristics of the monitored attacks.

D. Energy consumption and security

In the mobile ad-hoc networks, the energy consumption is a key factor, because nodes power source are batteries, so they have a limited amount of energy to communicate each other. A routing protocol must take in account this constraint, limiting the overhead generated by protocol packets. Security have also an impact on power consumption, because the encryption algorithms and, in minor part, the hash functions are expensive operations for the CPU. The authors in [26] applied various energy-aware routing metrics to the Optimized Link State Routing (OLSR) protocol, analyzing their effectiveness in reducing the energy consumption. The Minimum Drain Rate routing strategy was used to calculate paths between the nodes. In [27] the authors evaluated the energy performance of the DSR and the OLSR protocols, showing that a reactive protocol takes advantage from its routing policy, but for high traffic load and variable traffic pattern, a proactive protocol has good performance. In [28] the authors proposed an extended approach using epidemic schemes aimed at the routing optimization in terms of energy consumption and message delivery probability. The authors in [29] analyzed the energy consumption of various routing protocols in DTNs, evaluating the impact on the performance of the protocols. In the work in [30] the authors proposed an algorithm to achieve an energy efficient, secure and stable routing over MANETs. It uses the Diffie-Hellman algorithm to generate and exchange secret keys, and it implements the energy efficient routing by adding an energy threshold value to route requests, so the reply is sent only if the residual energy of the node is above this threshold. A review of security and power consumption challenges in ad-hoc networks [31] explains what the issues in the MANETs are. Transmission and receiving of data is the first factor to energy consumption. The amount of packets exchanged on the network affects directly the power consumption. More packets are transmitted and received, more is the battery discharging. Tests on algorithms for digital signature [32] reveal that RSA (with 512 and 1024 bits) is the lightest one. One important statement regards the correlation of power consumption between encryption and transmission. The energy consumed for cryptography has a minor impact, but the introduction of hash functions and digital signatures increases the packet size and the time needed to the protocol to execute its processes, so the power consumption depends more from these features.

III. TRUST MANAGEMENT ON SECURE PROTOCOL

Introducing a trust management procedure in a protocol that provides already encryption procedures to authenticate messages and hash functions to protect mutable fields could increase the kind of attacks that the network can detect. The proposal regards an extension of SAODV, introducing a trust management scheme to protect against malicious nodes that participate correctly to the route establishment phase, but then they behave maliciously by dropping packet, in addition to the attacks already protected by SAODV using encryption and hash functions.

A. Secure Ad-hoc Distance Vector Routing

SAODV is a routing protocol for MANETs based on AODV. Its principal task is securing the route discovery process. The major vulnerabilities of AODV that SOADV solves are the following:

- impersonation made by a node that generates requests in name of another node;
- decreasing of the hop count or increasing the sequence number of the destination by an intermediate node, to be part of the path connecting two nodes. This could happen if the node wants to analyze the packets exchanged by the nodes, or to break the link dropping packets;
- impersonation of a node, generating a route reply with its address as destination address;
- generation and transmission of a route error packet, impersonating another node. Using a high sequence number, next route discoveries regarding that node will fail;
- impersonation of a node generating and transmitting a route reply packet, declaring that the node is the destination and it is the leader of a subnet. Doing so, the node could drop all the packet of the subnet;
- sending of route request packet using the maximum sequence number possible for the destination. When it happens, the sequence number will start again from zero, so it invalidates all previous routes discovered.

The primary security requirement that SAODV satisfies is the import authorization, which is the authorization to update routing information only when the information is received by the destination itself. It needs
other security services, such as integrity and source authentication. Integrity ensures that the message information was not modified by intermediate nodes, whilst source authentication is needed to verify that the node is who claims to be. These properties combined define data authentication, and they are obtained with digital signatures and message authentication techniques.

1) Digital signatures

To protect the field integrity, SAODV protocol uses the digital signatures to secure the packet. In this way, the fields cannot be modified by any node except the one that generates the packet. The only field not involved in this process is the hop count field, because each node that retransmits the packet needs to increase the value in the field. To address the issue of allowing the intermediate nodes to reply to route requests if they have an active path to the destination, the protocol takes in account two possibilities. In the first, each intermediate node will not reply to the request also if it has a route to destination. The second one allows the reply by other nodes, which need to include the original signature of the destination (stored in a cache), signing the fields modified by them. These two approaches are called respectively Single Signature Extension and Double Signature Extension. Packets generated using these extensions allow each node to verify the validity of messages. If the verification fails, the node discards the information in the packet.

2) Hash chains

The hop count field has to be modified by each node that forwards the packet, so the hash chains are used for this aim. Each node generating a route request or a route reply put a random number (seed) in the “hash” field, and the TTL in the “max hop count” field. The “top hash” field is filled by applying “max hop count” times the hash function to the value in the “hash” field.

\[ Top\ _\ Hash = h^{Max\_Hop\_Count}(seed) \]

An intermediate node can verify the field by using the hash function “max hop count” minus “hop count” times to the value in the “hash” field.

\[ h^{Max\_Hop\_Count-Hop\_Count}(Hash) \]

If the result of this operation is equal to the information contained in the “top hash” field, the information is verified. A forwarding node increases by one the value in the “hop count” field and it applies the hash function to the “hash” field one time.

3) Vulnerabilities

The SAODV protocol solves many vulnerabilities of the AODV protocol, but it does not take in account the possibility that a fair node will be compromised later in time. Furthermore, a node could forward a packet without incrementing the hop count. On this chance, the consequence is not so relevant, because the final hop count reduction will be only of one unit. The protocol has no protection against rushing and wormhole attacks. The first one could be avoided by forwarding a random route request instead of the first received. Regarding the wormhole attacks, if the neighbor nodes have a mechanism to listen to packets received by the malicious node, they could detect that it is forwarding a packet with hop count \( X + 1 \) without receiving the same one with the hop count \( X \). The protection offered by the SAODV protocol is only on the routing packets. The data packets are not protected, so a malicious node could drop these packets without any countermeasure taken by the protocol to avoid this behavior.

B. Trust management scheme

The digital signatures and the hash chains used in SAODV protect from many attack typologies. To improve the security, a trust management scheme is introduced, so the packets will follow routes composed by trusted nodes, avoiding the malicious ones. The protocol manages the route requests as SAODV do, forwarding in broadcast only the first one and discarding others with the same sequence number, but updating routing table adding the new hop to the originator. When a node with a valid route to the destination is discovered, or the packet reaches the destination, a route reply will be sent to the node that forwarded the request. For the route requests with the same sequence number, a maximum number of route replies to generate is fixed. The route replies follow the path to the originator, a node will forward it only if the entire record on the table is updated with the information they contain.

Figure 1. Example of routing using trust as metric

1) Trust relationships

Using trustworthiness as metric, a node can choose the next hop of a route based on its trust value. There are two ways to calculate the trust value of a node:

- directly, if a node had already interactions with the target node;
- indirectly, if no interactions between the two nodes happened, or the interactions happened too far in the past.

We adopted a framework of trust modeling and evaluation [33], implementing the trust management capabilities to the SAODV protocol. Trust can be defined as the certainty whereby an agent will perform such an action from subject point of view. A trust relationship is defined as follows:

\[
\{subject \_agent, action\} \quad (3)
\]
The definition of trust value of the relationship is:

\[ T_{\text{subject: agent, action}} \] (4)

The probability that an agent will perform an action is defined as:

\[ p = P_{\text{subject: agent, action}} \] (5)

This framework bases the trust value on the entropy. It is proportional to the execution probability of that action for that agent in the subject point of view. The probability can vary in a [0, 1] interval, whilst the trust value varies continuously in a [-1, 1] interval. The definition of the entropy function \( H(p) \) is:

\[ H(p) = -p \log_2(p) - (1-p) \log_2(1-p) \] (6)

The entropy is a value of uncertainty. The trust value based on the entropy is calculated in the following method:

\[
T = \begin{cases} 
1 - H(p), & \text{for } 0.5 \leq p \leq 1 \\
H(p) - 1, & \text{for } 0 \leq p < 0.5 
\end{cases} \] (7)

To establish the trust towards the agents with which no previous interactions happened, a recommendation system is used. Few simple properties has to be taken in account when the trust is obtained through recommendations:

- the trust in a node should not be higher than the trust for recommendation of the recommender agent;
- when more than one recommendation is received, the trust value for the agent should not be lower than the value obtained if only one of those recommendations was received;
- the trust based on multiple recommendations coming from a single source should not be higher than the recommendations coming from independent sources.

In Fig. 2 the configuration in which the first property has to be respected is shown. Its mathematical representation is:

\[ T_{AC} \leq \min(|R_{AB}|, |T_{BC}|) \] (8)

The second property has to be respected in a situation similar to the one shown in Fig. 3. This constraint is represented by the following equations:

\[ T_{AC} \geq 0, \text{ for } R_1 > 0, T_2 \geq 0 \] (9)

\[ T_{AC} \leq 0, \text{ for } R_1 > 0, T_2 \leq 0 \] (10)

When multiple recommendations are received from the same source, as shown in Fig. 4, the third constraint defined before has to be respected, and it is described as follows:

\[ T_{AC_1} \geq 0, \text{ if } T_{AC_1} \geq 0 \] (11)

\[ T_{AC_2} \leq T_{AC_1} \leq 0, \text{ if } T_{AC_1} < 0 \] (12)

The actions on which a subject \( A \) needs to establish a trust value for an agent \( B \) are: the packet forwarding, which is indicated as \( T_{AB} \), and the recommendation, which is indicated as \( R_{AB} \). The entropy-based adopted model respects the properties stated previously in (8). If the node \( A \) requires a recommendation for the node \( C \), and it receives the recommendation from node \( B \), the calculation of the trust value is as follows:

\[ T_{ABC} = R_{AB} \cdot T_{BC} \] (13)

If the subject \( A \) receives more than one recommendation (e.g. from \( B \) and \( D \)), the following formula is used:

\[ T_{AC} = \omega_1 (R_{AB} \cdot T_{BC}) + \omega_2 (R_{AD} \cdot T_{DC}) \] (14)

Equation 14 respects the constraint defined in (9), (10), (11) and (12). Its coefficients are calculated as:

\[ \omega_1 = R_{AB} / (R_{AB} + R_{AD}) \] (15)
\[
\omega_2 = \frac{R_{AD}}{(R_{AB} + R_{AD})} 
\]  

(16)

A subject having direct interactions with the agent can evaluate the probability that the action will be executed correctly:

\[
P\{A \rightarrow B, action\} = \frac{1 + \sum_{i=1}^{t} \beta^{t-i} k_j}{2 + \sum_{i=1}^{t} \beta^{t-i} N_j} \]  

(17)

The different observations of the action are indexed from 1 to \(t\), \(t\) denotes the current time, \(t_j\) represents the time of the observation \(j\), \(k_j\) has the value of 1 or 0 respectively if the requested action was executed or not, and for each request the \(N_j\) value is 1. To give less importance to the older observations, a remembering factor \(\beta\) is used. It can assume values from 0 to 1: the higher is its value, more is the weight of old observations. If a node does not have interactions with an agent for enough time, the probability goes to 0.5, so the trust value becomes 0.

2) Recommendation packets

Two new packet typologies are introduced allowing the nodes to send and receive recommendations:

- Trust Recommendation Request (TRREQ);
- Trust Recommendation Reply (TRREP).

TRREQ contains the request originator and a list of the requests about the agents of which the originator needs to know if they are reliable or not. TRREP contains the request originator, the recommender, who generates the reply, and a list of couples \(<agent, trust value>\). To secure those packets, a signature extension is added to the packets, in a similar way in which other SAODV packets are secured.

3) Trust management

The nodes need to store the trust values about the agents. Concurrently with the routing table, a trust table is introduced. Each entry of the table contains the agent and the parameters that allow computing the trust value and updating it when needed. The table is updated periodically, so the recommendations and the direct observations are stored in buffers until the update. If a node has a trust value about forwarding packet less than 0, it is included in a blacklist, and it is removed from all the routes stored. If a route has only the blacklisted node as next hop, the route is invalidated, and a new route discovery process is launched when the node needs to reach that destination. For \(\beta < 1\), the trust becomes 0 when enough time elapses, and the blacklisted node is removed from the blacklist.

C. Energy model

The most power consuming operations carried out by a node in MANETs are the wireless transmission and eventually the cryptography. We used an energy consumption model for performance analysis of routing protocols for MANETs described in [34] to analyze the consumption regarding wireless transmission, while for the encryption we used the results obtained from a study about the energy consumption of cryptographic algorithms presented in [35].

Communication costs have a linear model, with fixed costs \(b\) of channel acquisition and incremental costs \(m\) related to packet size.

\[
\text{Cost} = m \times \text{size} + b 
\]  

(18)

The total cost of a packet in the network is the sum of the transmission cost by the sender and all the costs of the potential receivers, which include nodes in transmission range of the sender and the destination. The wireless interface has four different states: receiving, transmission, idle and sleep. The last one is not used in the ad-hoc networks because it does not allow receiving or transmitting data. Therefore, the nodes not involved in transferring data stay in the idle state. For a broadcast transmission, the cost includes listening to the channel by the sender as fixed cost \(m\), while transmitting the packet and receiving it for all the nodes in sender wireless range is a variable cost, as shown in the following formula:

\[
\text{Cost}_{\text{broadcast}} = m_{\text{send}} \times \text{size} + b_{\text{send}} + \sum_{n \in S} (m_{\text{recv}} \times \text{size} + b_{\text{recv}}) 
\]  

(19)

Set \(S\) refers to all the nodes included in the transmission range of the sender node. Point-to-point transmission has a cost that includes RTS, CTS and ACK messages used in the 802.11 MAC protocol. The cost to send or receive one of them indifferently is represented by \(b_{\text{send}}\) and \(b_{\text{recv}}\). The cost for the destination is similar, with the sending and the receiving phases inverted respect to the sender. These costs are respectively shown in (20) and (21).

\[
\text{Cost}_{\text{source}} = b_{\text{send}} + b_{\text{recv}} + m_{\text{send}} \times \text{size} + b_{\text{send}} + b_{\text{recv}} 
\]  

(20)

\[
\text{Cost}_{\text{destination}} = b_{\text{recv}} + b_{\text{send}} + m_{\text{recv}} \times \text{size} + b_{\text{recv}} + b_{\text{send}} 
\]  

(21)

The nodes in the range of the sender or the destination discard the packet if the transmission is point-to-point and they are not in promiscuous mode. Some MAC implementations allow entering in an energy-saving mode state when a transmission directed to another node is detected. The cost at non-destination nodes is the following:

\[
\text{Cost}_{\text{non-dest}} = \sum_{n \in S} b_{\text{discardctl}} + \sum_{n \in D} b_{\text{discardctl}} + \sum_{n \in S} (m_{\text{discard}} \times \text{size} + b_{\text{discard}}) + \sum_{n \in D} b_{\text{discardctl}} 
\]  

(22)

The cost for discarding control packets is represented by \(b_{\text{discardctl}}\). If a node works in promiscuous mode (e.g. when it needs to sense if a node forwards a packet for computation of the trust value), the cost calculation is the same as in (22), except for \(m_{\text{discard}}\) and \(b_{\text{discard}}\), which are substituted respectively by \(m_{\text{recv}}\) and \(b_{\text{recv}}\).
For cryptographic operations, the three main operations taken in account during the cost evaluation are:

- computation of the digital signature;
- verification of the digital signature;
- application of the hash function.

All these costs depend from the algorithm used. The cost for signing and verifying the digital signature of the packet is assumed as fixed cost for each of them, while for the hash function, the cost depends from the size of the data on which the algorithm is applied.

IV. SIMULATION RESULTS

The Secure and Trusted AODV protocol (STAODV) is compared with the SAODV protocol under the performance and the energy consumption point of view. For this purpose, we developed a simulator, whose architecture is shown in Fig. 5. The parameters used to obtain the results are shown in the Table I.

![Simulator architecture](image)

**Figure 5. Simulator architecture**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>1000x1000 m²</td>
</tr>
<tr>
<td>Duration</td>
<td>600 seconds</td>
</tr>
<tr>
<td>Transient time</td>
<td>10% of the total</td>
</tr>
<tr>
<td>Nodes</td>
<td>50</td>
</tr>
<tr>
<td>Transmission range</td>
<td>250 m</td>
</tr>
<tr>
<td>Transmission rate</td>
<td>4 packets/second</td>
</tr>
<tr>
<td>Data packet size</td>
<td>128 bytes</td>
</tr>
</tbody>
</table>

**TABLE I. SIMULATION PARAMETERS**

Regarding the consumption analysis, the values used for the energy model are shown in the Table II, as obtained empirically in [34], [35].

**A. Attacking model**

The malicious nodes in the network execute a modified version of the black hole and gray hole attacks, because the SAODV protocol is already resistant to these attacks. The attack is done participating fairly in the routing discovery phase, but dropping the data packets received. These versions of the attacks are called Authentication-Resistant Black Hole (ARBH) and Authentication-Resistant Gray Hole (ARGH). The ARBH nodes drop all the data packets they receive, while the ARGH nodes drop a percentage of them, so it is more difficult to detect. In our simulations, the ARGH dropping percentage is 75% if not stated differently.

To evaluate the reliability of the recommendation system, nodes disseminating false recommendations were included in the network. Performing this kind of attack has two main purposes: distrust a fair node, or trust a malicious node. The protocol has to detect the nodes running that kind of attack, so their recommendations can be excluded from the indirect trust computation process.

**B. Simulation results**

The simulation were run to compare the performance of the two protocols with and without malicious nodes in the network. The following graphs will show the improvement that could be achieved using a trust management scheme in the mobile ad-hoc networks under different points of view.

1) **Packet delivery ratio**

The evaluation of the Packet Delivery Ratio (PDR) is one of the most important characteristic of a protocol. By analyzing it, we can understand if a protocol is susceptible to a threat or not. To compute this ratio for the entire network, the following equation was used:

\[
PDR = \frac{\text{packets received}}{\text{packets sent}} \times 100
\]

(23)

In the MANETs, the PDR decreases when the nodes speed increases, even if no malicious nodes are in the network. The cause is the breakage of links that incurs
frequently when the nodes move faster. The performance of the two protocols in a network without malicious nodes are very similar, as shown in Fig. 6. PDR is always above 98% until a maximum speed of 20 m/s. There is a small decrement in both protocols when the speed increases, due to the reasons explained before.

In Fig. 7 we can observe the PDR when malicious nodes executing an ARGH attack are in the network. The ratio decreases in both protocols when the number of malicious nodes increases. Comparing the two protocols, STAODV maintains a ratio of almost 90% even when the 30% of the nodes in the network execute this attack, while the SAODV achieves a PDR lower than the 75%. When 5 nodes are malicious, the PDR of the SAODV is near the 90%, but it is less than the result obtained with the trust management scheme. With almost 1/3 of the nodes executing an ARGH attack, the protocol can deliver less than 3 packets each 4 packets sent.

The performance of the protocols when some nodes of the network performs an ARBH attack is shown in Fig. 8. The difference between the two protocols is higher with respect to the previous attack. The STAODV protocol continues to keep a PDR higher than the 90%, while the PDR of the SAODV protocol decreases under the 65% when the ARBH nodes are the 30% of the entire network. Therefore, the SAODV is able to deliver only the packets that follow paths composed of few nodes, which have a minor probability to include a malicious node. The comparison of the effects that the ARGH and the ARBH attacks have on the PDR for the STAODV protocol is shown in Fig. 9. The protocol reacts well against both the threats, reaching a better result in detecting and avoiding the ARBH nodes when they are the 10% of the nodes that compose the network. When the number of malicious nodes increases, the STAODV achieves almost the same PDR for both the attacks.

2) False recommendations detection
A trust management scheme must be able to distinguish the fair recommendations from the false ones. For this reason, the nodes maintain a trust value about recommendations for each node.

<table>
<thead>
<tr>
<th>5 false recommenders</th>
<th>10 false recommenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.06 0.07 0.07 0.03 -0.02</td>
<td>0.05 0.05 0.04 0.00 -0.3</td>
</tr>
<tr>
<td>0.09 0.06 0.01 0.06 0.02</td>
<td>0.00 0.11 0.05 0.02 -0.3</td>
</tr>
<tr>
<td>0.08 -0.04 0.14 -0.01 0.08</td>
<td>0.05 0.01 0.04 0.07 -0.3</td>
</tr>
<tr>
<td>0.06 -0.03 0.04 0.03 0.01</td>
<td>0.10 -0.01 0.07 0.03 -0.3</td>
</tr>
<tr>
<td>0.02 -0.01 0.03 0.03 0.01</td>
<td>0.08 0.08 0.09 0.09 -0.4</td>
</tr>
<tr>
<td>0.01 0.01 0.07 0.02 -0.3</td>
<td>0.08 0.04 0.05 0.04 -0.3</td>
</tr>
<tr>
<td>0.06 0.03 0.05 0.04 -0.3</td>
<td>0.06 0.05 0.03 0.06 -0.3</td>
</tr>
<tr>
<td>0.10 -0.02 0.08 0.09 -0.3</td>
<td>0.07 0.05 0.01 0.05 -0.4</td>
</tr>
<tr>
<td>0.08 0.08 0.07 0.05 -0.3</td>
<td>0.03 0.09 0.00 0.02 -0.3</td>
</tr>
<tr>
<td>0.10 0.00 0.04 0.05 -0.3</td>
<td>0.04 0.11 0.05 0.03 -0.3</td>
</tr>
</tbody>
</table>

In the Table III the average trust values of the nodes in the network is shown. The highlighted cells correspond to the values concerning the malicious nodes. From the analysis of these values, we can state that the protocol
detects the nodes acting maliciously by spreading false information, because their average trust value on recommendations in the network is notably under zero. There are also other negative, but near to zero, values for some fair nodes. The reason can be found in the link breakages that sometimes happen in a MANET, so a node cannot forward a packet to its path and a fair recommendation could be evaluated as malicious. This situation happens rarely with respect to the malicious recommendations, so the values are not so distant from zero, and a node can raise its trust value over the zero if its opinion is needed to other indirect trust evaluations.

To avoid the distrust of a fair node, the protocol provides a threshold before considering a node as malicious. A recommendation is evaluated exact if the difference between it and the computed direct trust value is in a range of ±0.25.

3) Erroneous detections

When a scheme to detect malicious nodes is used, the detections made have to be correct, because distrusting a fair node increases unnecessarily the length of the paths, increasing the end-to-end delay. However the links between the nodes in a MANET break often, therefore avoiding erroneous detections completely is impossible. After enough time elapses, the STAODV protocol allows any node to participate again to the communication in the network also if it was detected as malicious.

4) Energy consumption analysis

The nodes in the MANETs are powered by batteries, so their energy availability is limited. A protocol for ad-hoc networks needs to take in account this limitation, providing a way to route data without exceeding in energy consuming to run the protocol. The main operations required by a MANET routing protocol that need a notable amount of energy are the wireless transmission of packets and the cryptography. With this analysis we study the consumption of the SAODV and the STAODV protocol, trying to analyze the impact of the introduction of a trust management scheme in an ad-hoc routing protocol.

The energy consumption of the wireless transmission when only fair nodes are in the network is shown in Fig. 13. The STAODV protocol requires more energy than the SAODV. When the maximum speed increases, the
consumption increases too in both protocols. The main difference in terms of power consumption is introduced by the promiscuous mode used in STAODV to let the nodes sensing when their neighbors forward a packet correctly.

Fig. 13 shows that the difference between the two protocols is higher when the network is under attack. The SAODV consumption seems to not increment when the maximum speed increases, because only the packets that follow a short path can reach their destinations, otherwise the probability that a malicious node is included in the path is higher, so the packet will be dropped. When this happens, the energy saving comes from the nodes that do not receive, and then forward, the packet. The energy consumption of the STAODV protocol increases at higher speeds, because with more link breakages and more distrusted nodes, the nodes have to run more route discovery processes, and the found paths are longer.

The cryptography operations consume energy because computing a digital signature, verifying it and applying a hash function are expensive operations in terms of CPU use. The STAODV protocol requires the signing of a higher amount of packets than SAODV because it introduces two new protocol packets to manage recommendation exchanging between nodes. When only fair nodes participate in the MANET, as shown in Fig. 15, the consumption of the STAODV protocol is higher when nodes are moving, whilst it is almost the same of the SAODV when the nodes stay still. Moreover, there is an increment in energy consumption in both protocols when the nodes move faster, but it is higher when a trust management scheme is used. In the SAODV protocol, the consumption increases due to the more routing discovery phases that need to be run. It is true also for the STAODV protocol, but it requires that the nodes ask for recommendation if they have to send a packet to a neighbor on which they have no trust information, and it usually happens when a new route is discovered.

Fig. 14 shows that the difference between the two protocols is higher when the network is under attack. The SAODV consumption seems to not increment when the maximum speed increases, because only the packets that follow a short path can reach their destinations, otherwise the probability that a malicious node is included in the path is higher, so the packet will be dropped. When this
In Fig. 16, we can see that the presence of malicious nodes in the network involves a higher energy consumption for the STAODV. Using the trust management scheme, the routes are invalidated when a malicious node takes part in them, so the STAODV launches more route discovery processes, and the amount of signatures, verifications and hashes increases. Despite a packet is signed only when generated, while it is verified each time a node receives it, the consumption in signing is higher, because the generation of a signature using the RSA algorithm requires more than 30 times the energy needed to verify it. All the previously analyzed graphs do not show the energy consumption due to the execution of the hash function, because it is much lower than other cryptographic operations.

The percentage of consumption due to wireless transmission and cryptography respect to total energy consumption seems not to depend from the presence of malicious nodes in the network, as can be seen in Fig. 17. When nodes are static, cryptography consumption is almost the 20% of the overall consumption in nearly all the cases. The wireless transmission has a higher impact on the overall energy consumption when the nodes in the network move, reaching almost the 90%.

V. CONCLUSIONS

The introduction of a trust management scheme over the STAODV protocol allowed increasing the network security. The communication between the nodes is not disrupted if some nodes in the MANET drop maliciously packets that have to be forwarded, and the transmission will reach its destination, because the nodes that do not behave correctly are excluded from the routes. The proposal introduces new packets in the protocol, therefore the energy consumption increases. The main difference in terms of consumption is due to the use of promiscuous mode to detect nodes behaving maliciously, so a node receives all the data transmitted in its wireless range, and consequently it consumes more energy to receive and analyze them. If the nodes in the network has an energy availability that can sustain this increase in terms of energy consumption, the network security is improved using the STAODV protocol. When the energy is constrained, but the network is prone to attacks, there is the need of finding a right trade-off between these two contrasting requirements.

REFERENCES


Andrea Lupia was born in 1985. He received the master degree cum laude in computer science engineering at the University of Calabria, Italy, in May 2013. Since January 2014 he is participating to the PhD school in “Information and Communication Engineering for Pervasive Intelligent Environments” at the D.I.M.E.S. department of the University of Calabria, Italy. In July 2014, he has attended the “J.T. Schwartz International School for Scientific Research” on network design and optimization. His main research interests include the data dissemination and safety applications in vehicular ad-hoc network, and the security on the mobile ad-hoc networks.

Floriano De Rango received the degree in computer science engineering in October 2000, and a Ph.D. in electronics and communications engineering in January 2005, both at the University of Calabria, Italy.

From January 2000 to October 2000, he worked in the Telecom Research LAB C.S.E.L.T in Turin as visiting scholar student. From March 2004 to November 2004, he was visiting researcher at the University of California at Los Angeles (UCLA). From November 2004 until September 2007, he has been a Research Fellow in the D.E.I.S. Department, University of Calabria where he is now Assistant Professor. Dr. De Rango was recipient of Young Researcher Award in 2007. He served as reviewer and TPC member for many International Conferences such as IEEE VTC, ICC, WCNC, Globecom, Med Hoc Net, SPECTS, WirelessCOM, WinSys and reviewer for many journals such as IEEE Communication Letters, JSAC, IEEE Trans.on Vehicular Technology, Computer Communication, Eurasis JWCN, WINET etc. His interests include Satellite networks, IP QoS architectures, Adaptive Wireless Networks, Ad Hoc Networks and Pervasive Computing. He has co-authored more than 130 papers among International Journal and Conferences Proceedings.