Macrothink Institute™

**Network Protocols and Algorithms**
ISSN 1943-3581
2015, Vol. 7, No. 2

# Secure Trust Management with Source Routing Protocol for MANETs

José Luis Tornos, José Luis Salazar

Dept. of Communications and Electronic Engineering, University of Zaragoza

Ada Byron Building, 50018, Zaragoza (Spain)

E-mail: {jltornos, jsalazar}@unizar.es

Joan Josep Piles

Max Planck Institute for Intelligent Systems

Heisenbergstraße 3, 70569, Stuttgart, Germany

E-mail: joan.piles@tuebingen.mpg.de

Received: June 14, 2015 Accepted: July 21, 2015 Published: July 31, 2015

DOI: 10.5296/npa.v7i2.7816 URL: http://dx.doi.org/10.5296/npa.v7i2.7816

**Abstract**

A MANET, in order to work properly, needs its nodes to work collaboratively. This is not always the case, and thus tools are developed to detect and identify uncooperative nodes. In this paper we present TADSR, a protocol based on an already existing secure routing protocol on top of which it adds trust management features. Our aim is to detect rogue nodes, and also to improve the overall performance of the original protocol. The information gathering process will encompass both direct means and an indirect process through which other nodes will provide their own assessments. Then, a punishments and prizes system will try to get involved as many nodes as possible to improve the network performance.

**Keywords:** MANET, secure routing, trust management, DSR, ADSR, TADSR

## 1. Introduction

Due to the lack of a predefined infrastructure, ad-hoc networks need a routing protocol in order to grasp the underlying network topology before starting the communication between any two nodes. Furthermore, in some cases the nodes are expected to be mobile, Mobile Ad hoc Network (MANET). In such networks the routing protocol is required to be able to react swiftly to the mobility of the nodes and their subsequent location changes. The communication between two nodes could be stopped abruptly because of these changes, and when it happens they must react quickly to find a new route if they are to keep the link alive.

There are long time established routing protocols designed specifically for this kind of networks [1]. They offer several choices so that the protocol can be tailored to the actual network where they will be operating.

Routing protocols are basic in MANETs in that they provide a key functionality needed to establish communications. However, they are not enough to fulfill by themselves all the requirements of the network, since they lack the means to assess the behavior of the nodes. Even when the routing protocol is working properly, there can still be rogue nodes that do not comply with their duty of forwarding packets. As the network lacks any kind of central infrastructure in charge of the transport layer among the nodes, and provided it also lacks ferry nodes [2], it needs the joined effort of all the nodes to make up for it.

Secure routing protocols [3] are the first step to allay the problems posed by eventual rogue or non-collaborative nodes. They require all the nodes to be identified/certified prior to its joining the network, in order to avoid the possibility of foreign nodes taking part of it. A shortcoming of this system is that even if there is an access control that verifies the nodes as they join the network, its future behavior cannot be controlled.

Trust management [4] is yet another system developed to mitigate the failures or loss of performance in the network due to non-cooperative nodes. Unlike secure routing protocols, which need credentials, is based upon ratings for each of the nodes. These ratings can be either direct, where a node provides information gathered about its neighbors, or indirect, where it merely passes along the opinion of a third node about the given one.

Even if trust management system can control the network by itself [5] without any external help, there are however more complex scenarios which also demand some kind of user control. In those cases a secure routing system, thus ensuring that only authenticated users can join the network, working together with a trust management system in charge of its operation are the tools needed for its proper working.

In this paper we present a protocol that combines both secure routing and trust management for its use in MANETs (TADSR). Although joining the network will still be granted after showing the proper credentials / certificate, from there on its behavior will be assessed through a trust management policy, and it shall be each node's task to evaluate the information gathered both by itself and by the rest of the nodes in the network.

The rest of the paper is organized as follows: Section 2 will deal with secure routing and trust management in MANETs. We will introduce our protocol in Section 3. Our results will be presented and discussed in Section 4. Finally, Section 5 will show our conclusions and future lines of work.

## 2. Routing and Trust Management in Ad Hoc Networks

### *2.1 Routing in MANETs*

MANET routing protocols [1] have several key features that sets them apart traditional ones. Since there is no predefined infrastructure or topology in the network, some messages must be exchanged to discover the current state of the network. There are three paradigms to carry out this process:

- **Reactive protocols** only start the route discovery when there it is needed, i.e. when a node tries to reach another one to which does not know a working path. Examples of such protocols are AODV [6] or DSR [7].

- **Proactive protocols** are continuously scanning the network in order to always keep an accurate map of the connections between the nodes. However, they need more control packets than reactive protocols. Examples of this protocol are DSDV [8] or OLSR [9].

- **Hybrid protocols** mix both approaches, usually using a proactive protocol at a local level and a reactive protocol at the global one. One protocol using this technique is ZRP [10].

Another relevant feature according to which we can categorize routing protocols is the kind of routing they use:

- **Source Routing:** The node starting the communications explicitly sets the route to follow until its destination, e.g. DSR [7]

- **Hop-by-hop Routing:** The node sending the packet just indicates their destination and the next hop / node to process it, e.g. AODV [6], DSDV [8].

Other significant features of MANET routing are whether they use a single path to reach their destination, or if on the contrary they use several paths simultaneously to reach the same node, multipath protocols [11]; and also whether there is a differentiation of functions among the nodes, hierarchical or non-hierarchical network [12].

Because of the great potential of MANETs, there are some scenarios where it is mandatory to put in place secure routing protocols, such as emergency, rescue teams or military deployments among others. Several MANET secure routing protocols were developed to give answer to this need, most of which were based upon any of the aforementioned routing protocols. Thus, we have ADSR [13], ARIADNE [14], SDSR [15] and SRDP [16] based on DSR [7]; ARAN [17], SAODV [18] and SEAR [19] based on AODV [6]; SEAD [20] based on DSDV [8]; or SOLSR [21] based on OLSR [9]. Each one of these protocols guarantees its security through different means such as symmetric or

asymmetric cryptography, digital signatures or Message Authentication Code (MAC).

*2.2 Trust Management in MANETs*

Reference [22] shows that the way of assessing trust is also dependent on the kind of network we are dealing with. Thus, we have to start by defining what we understand by trust, and we will do so beginning with the definition given in [23]: "Trust is defined as a belief level that one node can put on another node for a specific action according to previous direct or indirect information from observation of behaviors". This means we are implicitly trusting that a node's behavior will be the one we would expect according to its past actions.

After having defined what we consider "trust", we are going to classify the ways of managing it in the network, according to different criteria. In [24] is proposed that the network assessment can be either centralized or decentralized; either proactive or reactive; and, finally, either intensional or extensional. A different classification is shown in [25], where the management or evolution model is based on information theory, graph theory, collaborative game theory, non-cooperative game theory, or computational intelligence.

In addition to choosing the criteria according to which trust will be evaluated in the network, we also need to establish the procedures to follow in order to make the assessment. This means we have to define, among all the possible alternatives, how each node's trustworthiness is going to be measured. Reference [26] proposes a scheme in which trust management has three phases: information gathering, scoring and ranking, and response. Each of these three steps must be detailed, together with its relations, so that the trust management process gets the necessary consistence to work properly.

Rightly assessing the nodes of a network is a fairly complex task. It is indeed possible to exert a tight control of the cooperation of a node with which we have direct communication when we are a party to the conversation. However, this endeavor becomes much more complex the evaluation of those of its conversations we are not involved with, and even more so when we have not even got a direct link with the node. We have followed the proposal described in [26] and have organized the three steps of trust management as follows:

- **Information gathering:** Information about the behavior of the nodes will be taken into account regardless of whether it is direct (nodes with which there is a direct link) or indirect (that offered by a node about a third one), even if some models only give value to direct information. Direct information will be obtained comparing what packets are sent to a node for its forwarding, and which of those are actually sent to their next destination. Indirect information is gathered through suggestions, warnings, accusations, etc. that each node publishes about relevant behaviors. This information can be requested by a node, or broadcast spontaneously.

- **Reputation scoring and ranking:** After having gathered the information available about the nodes' behavior, they are evaluated, both according to the direct information received, and if present, the indirect one [26, 27]. The nodes will be classified after this assessment, and a node (or a path) will be picked depending on the action to be carried out.

- **Response:** In this last step decisions going beyond pathfinding are taken. There will be punitive measures for those nodes that, after examining its performance and responses, are deemed rogue or non-cooperative. In the same vein, there will be benefits for cooperative nodes.

## 3. TADSR Implementation

Trusted ADSR (TADSR) mixes concepts from secure routing and from trust management. On the one hand, all nodes wanting to take part in the network must be accredited through a key/certificate known to and accepted by the rest of the users. On the other hand, we track the behavior of all the participants in the network, and we improve its performance through the analysis of the information gathered both directly and indirectly. Such model makes our proposal best suited to be used in the so-called “managed ad-hoc networks” [29], since they require a previous step prior to being allowed to join the network. Trust management could also be used without secure routing, but then we would have to care about other risks, such as sibyl attacks [30].

Our protocol's aim is to find an equilibrium between security, efficiency, and ease of management. It tries to be fair to the nodes in the network, in that it locates and punishes those nodes that try to hamper the network or to get profit from gaming it. Trust management must be strict enough to be able to find bad-functioning nodes, without being so much of a drag on the network that its operation is hindered. The system, thus, shall be able to deliver both punishments and prizes without being a burden to the network as a whole.

This trust management model builds upon the secure routing protocol ADSR, which in turn is based on DSR. It uses elliptic curve cryptography and aggregate signatures to get a signature size as small as possible for the routing packets. In this line, trust management will piggyback on the routing packets to carry out indirect information exchange between nodes. This way we can keep constant the number of packets traversing the network, minimizing the bandwidth overload. Only a few packets will be needed to carry out specific punitive measures, as we will see in section III.B.

Proper trust management tasks are done, according to the classifications seen in [24, 25] through a distributed model. In this paradigm there is no single trusted third party (TTP) in charge of trust management; on the contrary, each node is responsible for doing its own assessments. This means that the evaluation of trust is neither symmetric nor transitive.

The protocol can be split in two processes: On the one hand, secure route discovery, based upon the features seen in ADSR, but with the functionalities needed for a trust management system. On the other hand, the route upkeep, where the information gathered both directly and indirectly is assessed, and decisions are taken regarding potential measures to increase the performance of the network, including the banishment of misbehaving nodes.

*3.1 Node and Route Assessment*

3.1.1 Information Gathering

Information gathering can be carried out using a number of means, both direct and indirect, with direct data being acquired by means of a watchdog [31]. Each node's direct trust value (1) is computed as the ratio between the total amount of packets the node is expected to forward, and the actual number of packets forwarded. Thus, we have a value between 0 and 1:

$$T^D = \frac{P_f}{P_f + P_{\mathrm{nf}}} \in [0,1] \quad (1)$$

where $T^D$ is the direct trust value, $P_f$ is the number of packets forwarded, and $P_{nf}$ is the number of packets that should have been forwarded, but actually have not. There will be two different counters $T^c$ (2) and $T^d$ (3), one for missed routing packets and another for missing data ones. These values will be used in the decision-making process regarding some suspicious node.

$$T^c = \frac{P_{cf}}{P_{cf} + P_{\mathrm{cnf}}} \in [0,1] \quad (2)$$

$$T^d = \frac{P_{df}}{P_{df} + P_{\mathrm{dnf}}} \in [0,1] \quad (3)$$

where $T^c/T^d$ is the control/data direct trust value, $P_{cf}$ / $P_{df}$ is the number of control/data packets forwarded, and $P_{cnf}$ / $P_{dnf}$ is the number of control/data packets that should have been forwarded, but actually have not.

Indirect information can be harvested through several ways. Proposed routes can be evaluated according to different models. The first one is an individual assessment of each of the nodes composing the path, while the second one is an evaluation of all the nodes in the route as a whole. In both approaches a trade-off must be done: with an individual judgment every node gets to know the opinion the rest of the network has about them. Should a node find itself aggrieved by another one's opinion, it is able to take reprisals. On the positive side, an isolated assessment of each node facilitates individual decisions without needing to know the full path.

We will use a node-by-node assessment in our protocol. Each of the assessment of the nodes composing the path will take a value between 0 and 1, $T^{Ii} \in [0,1]$, where $T^{Ii}$ is the indirect assessment of the i-th node in the path. These values are included into the route reply packets of the route discovery protocol sent by the destination node, and it will be the source node who, after gathering all the information about possible alternatives will determine the route through which packets will be sent.

Taking advantage of REP packets instead of using specific ones allows us to stay within the reactive philosophy of DSR, and keeps at a minimum the bandwidth overhead needed for indirect information exchange. Furthermore, since ADSR is a source routing protocol where the node wishing to start a communication is who will choose the route to be followed, this additional information will be a great aid when taking the decision.

The final aggregate value for the indirect information (4) will be computed according to a weighted average of the data supplied by the other nodes [32]:

$$T_{n,m}^{I} = \frac{\sum_{i \in O} T_{i,m} \cdot T_{n,i}}{\sum_{i \in O} T_{n,i}} \in [0,1] \quad (4)$$

where $T_{n,m}^{I}$ is the indirect trust value node n has about node *m*; $T_{i,m}$ is the trust value provided by node *i* about node *m*, $T_{n,i}$ is the trust value node *n* has about node *i* and *O* is the number of hops in the route.

3.1.2 Scoring and Ranking

As we are using a source routing protocol, when a communication is going to be established the starting node must pick one of the routes it has cached. We are going to start supposing a node has the full range of assessments, both direct and indirect, regarding every node in every path, and provided that none of the involved nodes is banned from the network nor carries any other penalty, since penalties will be studied in depth in section 4.2. In this case, it has all the data it needs to fully evaluate each possible path, taking into account both direct and indirect information. The final trust value for a given path shall be the weight summation of the direct and indirect information (5), averaged by the route length:

$$T_{n,m} = \alpha T_{n,m}^{D} + \beta T_{n,m}^{I} \in [0,1] \quad (5)$$

where $T_{n,m}$ is the aggregated trust value node *n* has about node *m*; $\alpha$ is the relative weight direct values are given; $\beta$=*1-*$\alpha$ is the relative weight of indirect values; $T_{n,m}^{D}$ is the direct trust value node *n* has about node *m*; and $T_{n,m}^{I}$ is the indirect trust value node *n* has about node *m*.

It must be noted that the opinion a node has about another is not commutative, and therefore all of them are relevant to the final value. There might be a node with a hostile attitude towards some others, and this will be included in the information gathered. Finally, after having gained the information concerning each of the possible paths, the originating node will rank them and will decide upon one.

The main difference with other previous trust management protocols based on DSR [33-36] is that we try to favor the involvement of the nodes, and one measure towards this goal is to reduce the workload of those nodes showing a collaborative behavior, lowering the amount of packets they are asked to forward.

The first step is the consideration for those routes above a given participation threshold. Even though the main criterion when choosing a path is still the number of hops so that the global number of forwarded packets is as low as possible, in the event of a tie a MINMAX(trust) [37], decision theory strategy, will be used as the deciding factor. This

means that the nodes with the highest trust in its path will be compared among each other, and the route with the "losing" one will be picked (should there be a tie, the next higher valued nodes will be compared and so on, and finally the most recently used route will be used, all other factors being equal).

This selection method rewards those nodes with highest trust (the most collaborative ones), since the bulk of the network traffic will be diverted away from them whenever possible, allowing them to keep their resources so long as it does not impact the overall performance of the network. In order to achieve this goal, and to avoid disrupting the network's operations, we must also set different decision thresholds regarding the categorization of the nodes defined in the response phase. The election of a different value for the threshold of suspicion and suspension will depend on various factors relating to the network such as security, node density, number of communications, etc. [36]

Other differences regarding thresholds protocols employing [33-36] to locate misbehaving nodes, is that although the path selection depends on the source node (it uses indirect information but it takes the final decision of the selected route), the policies of punishment will depend on the evaluation of a subset of nodes and not in the opinion of a single node, as detailed below.

3.1.3 Response

After having assessed all the available paths and picked the most suitable one, the only task remaining is to take those punitive measures due as a consequence of the assessments. Those measures will be defined according to two thresholds:

- **Suspicion threshold:** A node will be marked as suspicious when its trust value falls below *Ts*. When this happens its behavior will be examined more in depth.

- **Suspension threshold:** A trust value below this threshold will trigger a suspension procedure.

Since examining every action of every node is unfeasible, the suspicion threshold will act as a first alarm so that a suspicious node's full actions can be examined. Its transmission logs will be inspected, differentiating between routing and data packets. With this deep inspection it will be possible to discriminate, for instance, whether the node is behaving like a black or gray hole, forwarding only routing packets.

Once a node decides to launch a suspension initiative against a suspected offender, it generates a banishment proposal packet. A node receiving such a request will verify its own data and will check the suspect node's trusted value and whether its recorded levels of packet loss in both categories match those reported by the accusing node. If they match, and therefore it concurs, the node will send a "1" value indicating its agreement; on the other hand, a "-1" value will mean its rejection to the proposal; finally, the "0" value is to be used by those nodes unable to give a more definite answer. The accusing node will receive all the answers and will weight them according to its trust in each node, in order to decide whether there is a sufficient majority to support the suspension. If there is, the offending node will be

punished, and the accusing node will send a notification packet through the same path used for the proposal, including all the received assessments and the amount of times the node has already been suspended.

*3.2 Node suspension procedure*

Since a MANET depends on its conforming nodes to provide end-to-end connectivity, the punitive measures taken against one node can affect the performance of the network as a whole. Because of this risk special care is needed when delivering punishments, so as to not jeopardize proper operations.

Once the decision to suspend a node is made, the first measure to take would be to forbid any route involving it. However, in most cases, this would impose a greater burden on both ends of the communication, since the offending node would merely be acting as a relay or is part of the unique path available from the source to the destination node. Instead of this, only packets starting or ending in the rogue node will be dropped, while it will have to keep performing its usual forwarding duties so that no other nodes will be hindered.

No node suspension will be permanent in any case. The first offense will earn a suspension for a given time $T$. Next one will last twice as long, $2T$, and the duration will keep growing exponentially, i.e. the i-th sanction will last $2^{i-1}T$.

A rogue node is not guaranteed to start cooperating even after earning a punishment. On the contrary, it can remain non-cooperative even after being suspended, so its trust value will keep falling even lower. A node whose misbehavior does not subside will not be able to recover its trust, and therefore it will be eligible for a new punishment as soon as it fully rejoins the network and takes part in any route discovery process.

When a node receives a packet where either originating or targeting a suspended node, it will send back a message informing on when the block started (so that it can be verified that it is indeed in effect), together with the actual values and nodes involved in the decision. Affected nodes can then verify the validity of the measure, and not count this lack of forwarding of a packet as a transgression. Otherwise, the very fact of applying a suspension could be considered as a lack of cooperation by other nodes unaware of it.

## 4. Simulation, Results and Discuss

*4.1 Attacks*

MANET routing protocols have to face with different types of attacks. Following the description presented in [38] we can classify them into active or passive attacks. Passive attacks are these in which the attacker does not affect the performance of the network. These attackers try to extract information eavesdropping the network. Active attacks are these which try to disrupt the correct performance of the network. In these attacks is necessary to distinguish between internal and external attacks. External attacks are carried out by nodes which do not belong to the network. These nodes try to disrupt or use resources of the

network. Internal attacks are carried out by nodes which are part of the network and attack the network trying to use the network in their own benefit or trying to boycott the performance of the network.

Using a secure routing as is ADSR makes that sybil and newcomer attacks [30] cannot be employed because each participant in the network has to identify itself, with a certificate issued by a Certificate Authority, before it can be part of the network. But there are other attacks based on the behavior of the nodes which cannot be detected with a secure routing protocol and then a trust management protocol is needed. With the following simulations we are testing how the trust management protocol detects black nodes [39, 40]; bad-mouthing and conflicting behavior attacks [30] that impede the proper operations of the network, and at the same time we are assessing the protocol's behavior.

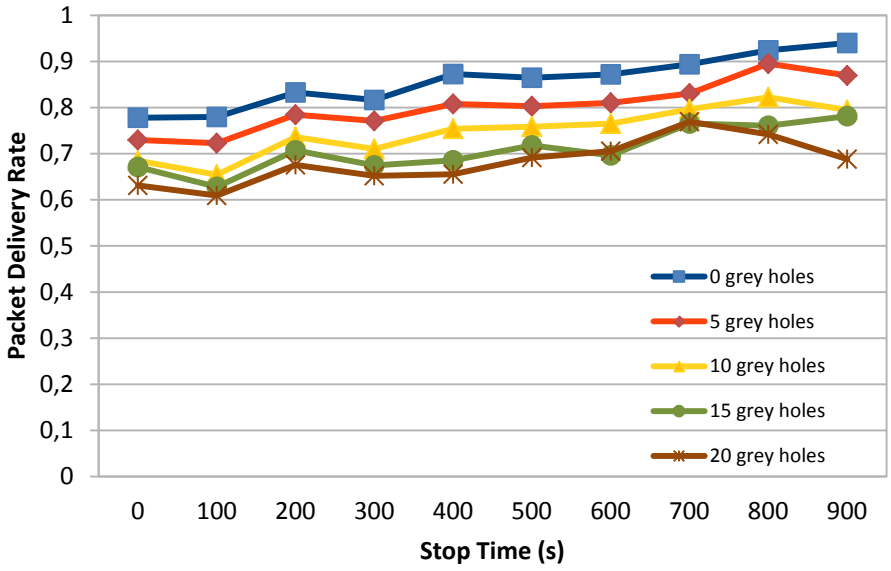


Figure 1. Original ADSR protocol

*4.2 Setup*

The protocol has been simulated using NS3 and the DSR protocol developed in [41], with several changes applied on top to mimic ADSR behavior. The simulations have been done for a 1500x300m area and 50 nodes, simulation parameters are listed in Table 1. The aim was to measure the Packet Delivery Rate (PDR) obtained for different stop times, $\alpha$ and $\beta$ parameters, and number of uncooperative nodes (between 0 and 20). Suspicion threshold has been 0.7, and suspension threshold has been 0.5. Suspicion threshold was selected as the mean of the values obtained in the simulation of DSR in [41]. Suspension threshold was set up as a lower value than the lowest value of PDR shown in [41]. We have used a random waypoint mobility pattern, with a random node speed between 0 and 20m/s. and at least ten simulations have been made for each of the values shown.

TABLE I. SIMULATION PARAMETERS

| | |
|---|---|
| Simulation time | 5000 s |
| Simulation area | 1500 x 300 m |
| Number of nodes | 50 |
| Transmission range | 250 m |
| Movement model | Random waypoint |
| Maximum speed | 20 m/s |
| Traffic type | CBR |
| Payload size | 512 bytes |
| Packet rate | 4 pkt/s |

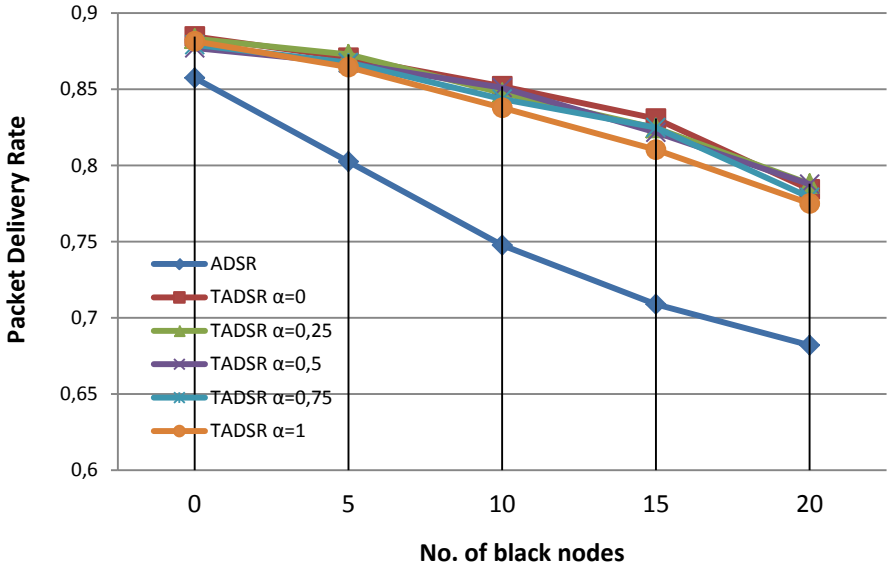


Figure 2. PDR of ADSR and TADSR

*4.3 Nodes' behavior*

Uncooperative nodes are modeled to correctly answer route discovery packets, but to skip packet forwarding. ADSR protects against Sybil and newcomer attacks [30], since route discovery packets are secured. Furthermore, conflicting behavior attack [30] is also mitigated because the source node is the one who actually chooses the path, so it could detect a systematic packet drop by one single node more easily. Figure 1 shows the Packet Delivery Rates (PDR) obtained in the original protocol without any trust management. The results shown in Figure 1 are not linear, this is due to the mobility of the nodes (for different stop times they create different scenarios) and for the existence of black nodes which are worsening the performance of the protocol (these black nodes can isolate a node if it is only surrounded of black nodes). There is also a very high variability of the results (more than 19% between the best and the worst result with a stop time of 200 seconds).

TABLE II. GLOBAL IMPROVEMENT RELATED TO ALPHA

| α | % relative improvement | % real improvement |
|---|---|---|
| 0 | 11,164873 | 8,4813561 |
| 0,25 | 11,005298 | 8,3601354 |
| 0,5 | 10,704079 | 8,1313157 |
| 0,75 | 10,424876 | 7,9192199 |
| 1 | 9,77048 | 7,4221099 |

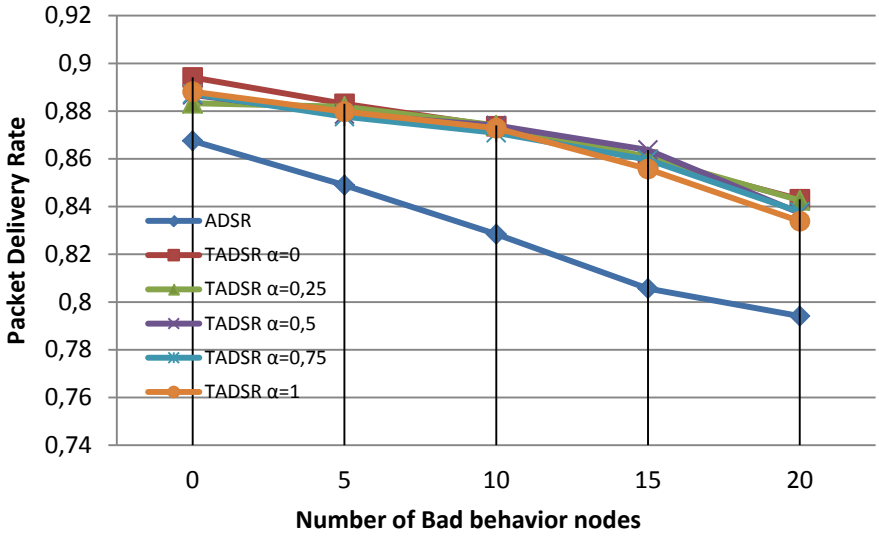


Figure 3. PDR of ADSR and TADSR (Bad Behavior attack)

*4.4 Results*

Our simulations have used values of α ranging from 0 to 1 (β=1-α), in 0.25 steps. This way we have obtained five datasets with which to compare the performance of the original ADSR protocol.

Figure 2 shows how the PDR average (stop time from 0 to 900 s) decreases as the number of black nodes increases, and how α = 0, and then β = 1, gives a slightly bigger improvement than any other value given all the weight of the final decision to the indirect trust value.

A clear improvement can be seen compared to the results obtained for the original ADSR protocol, with a better PDR even all the nodes behave properly. As the number of uncooperative nodes increases (black hole attack), so do the benefits of our protocol, achieving a 14% improvement over the global PDR (which translates into a 21% relative improvement compared with the original ADSR protocol), relative and real improvement for the different values of α are shown in Table II.

Figure 3 shows how the bad behavior affects the performance of the protocol. In this case, the bad behavior nodes attack to the 40% of the communications. It can be seen that the performance of the protocol is better when TADSR is activated. In Figure 4 are shown the results when added to de bad behavior attack the nodes deployed a bad mouthing attack. Also in this scenario, the trust management protocol improves the performance of the network.

*4.5 Discussion*

The results obtained in our simulations show that using a trust management protocol results in an improvement of the original ADSR protocol when there is up to a 40% of uncooperative nodes. This can be noticed in the PDR, where we get improvements over 14%. It is also important to note that the bandwidth consumption of our protocol is almost negligible (just one byte for each evaluated node), since it piggybacks on already necessary REP packets, and only small specific packets are used when evicting a node.

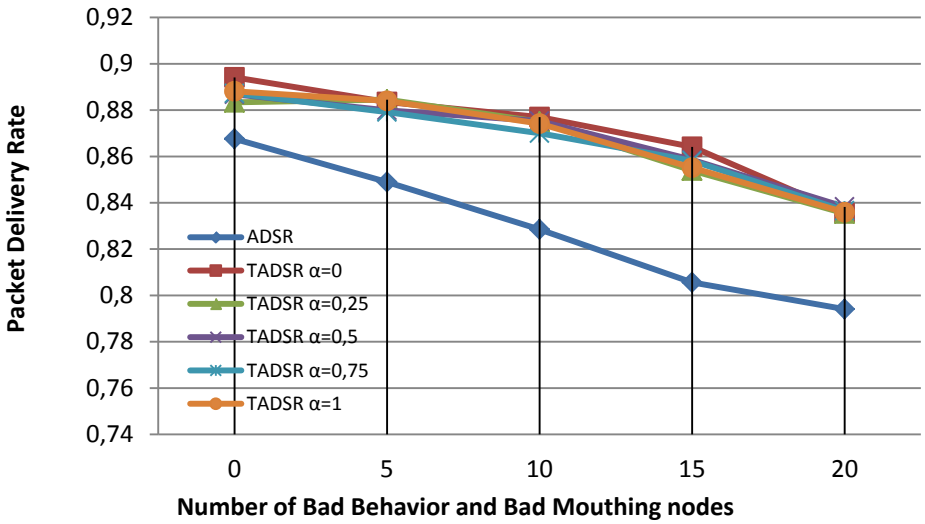


Figure 4. PDR of ADSR and TADSR (Bad Behavior and Bad Mouthing Atacks)

More so, using a trust management system also results in a better performance of the protocol even when all the nodes behave properly. There are several explanations for this, among which the most relevant are possible media saturation and node mobility. We have diminished the packet sizes and rates as much as possible in an effort to minimize saturation, but the parameters used allow speeds of up to 20m/s and the mobility model (Random Waypoint) of the simulation randomizes both the speed and the destination (random waypoint mobility model was chosen to ease the comparison with other trusted protocols [34-36]). Thus, a node can expect to have a certain neighbour, who has actually moved. If this happens often enough, with several potential neighbours of the same node, it will eventually be marked as uncooperative by the trust management protocol. While at first sight this can appear undesirable, it has in fact a net positive effect, as nodes tend to reject those with opposing speeds and/or destinations, and to link more strongly to those in their area of influence. Furthermore, evictions are not permanent but of a limited duration, and based on the opinions the nodes in the path, which allows the nodes to update their assessments each time a new route discovery takes place.

## 5. Conclusions and Future Lines

In this paper we have presented a trust management protocol (TADSR) based on a secure routing protocol that improves the performance of the original protocol. We have explored throughout the paper the different ways available to improve and secure MANET communications. We have also reviewed the state of the art in routing protocols and their features. Then, we have seen that while using secure protocols is a first step towards securing the network, it is not enough because once a node gets to join the network, it cannot be prevented from being uncooperative. A trust management system has been thus justified, in order to detect, identify and correct such rogue behaviors.

TADSR, following the lines laid down by its parent protocol (ADSR), tries to minimize the bandwidth overhead attributable to its extra functionality. This way, route reply packets are extended so that trust information regarding the nodes in the path can be exchanged almost costlessly. In addition, nodes are encouraged to take a more cooperative stance in the transmissions with the prospect of being freed from several forwarding duties.

Simulations have also shown that a trust management protocol can also somewhat manage the mobility of the nodes, improving PDR, because our protocol tends to favor choosing nodes with similar trajectories in an environment where they can be highly divergent.

As future lines of work, we are going to further analyze the response of the protocol in face of new kinds of attacks in addition to those considered so far. We also plan to test different mobility patterns and delve deeper in the way $\alpha$ affects the performance of the protocol.

## Acknowledgement

This work has been partially financed by Project UZ2014-TEC-02 (University of Zaragoza) and also by CeNITEQ (Communication Networks and Information Technologies for e-Health and Quality of Experience Group, University of Zaragoza)

## References

[1] Boukerche A, Turgut B, Aydin N, Ahmad MZ, Bölöni L,Turgut D. “Routing protocols in ad hoc networks: A survey”. Computer Networks, Volume 55, Issue 13, 2011; 3032–3080. http://dx.doi.org/ 10.1016/j.comnet.2011.05.010

[2] Zhao W, Ammar M. “Message Ferrying: Proactive Routing In Highly-Partitioned Wireless Ad Hoc Networks”. In FTDCS '03 Proceedings of the The Ninth IEEE Workshop on Future Trends in Distributed Computing Systems, Washington, DC, USA, 2003; 308 – 314. http://dx.doi.org/ 10.1109/FTDCS.2003.1204352

[3] Abusalah L, Khokhar A, Guizani M. “A survey of secure mobile Ad Hoc routing protocols”. Communications Surveys and Tutorials. Vol. 10, No. 4, 2008; 78-93. http://dx.doi.org/ 10.1109/SURV.2008.080407

[4] Cho JH, Swami A, Chen IR. "A survey on trust management for mobile ad hoc networks". IEEE Communications. Surveys and Tutorials, Vol. 13, No. 4, 2011; 562–583. http://dx.doi.org/ 10.1109/SURV.2011.092110.00088

[5] Michiardi P, Molva R. "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks". In Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. Portorož, Slovenia, 2002; 107-121. http://dx.doi.org/ 10.1007/978-0-387-35612-9_9

[6] Perkins CE, Royer EM. "Ad-hoc on-demand distance vector routing". In WMCSA: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications., New Orleans, Louisiana, 1999; 90–100. http://dx.doi.org/ 10.1109/MCSA.1999.749281

[7] Johnson DB, Maltz DA. "Dynamic source routing in ad hoc wireless networks". Mobile Computing. Volume 353. 1996; 153-181. http://dx.doi.org/ 10.1007/978-0-585-29603-6_5

[8] Perkins CE, Bhagwat P. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers". In SIGCOMM'94: Proceedings of the conference on Communications architectures, protocols and applications. London, UK, 1994; 234–244. http://dx.doi.org/ 10.1145/190314.190336

[9] Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L. "Optimized link state routing protocol for ad hoc networks". In INMIC 2001: IEEE International Multi Topic Conference 2001. Lahore, Pakistan 2001; 62- 68. http://dx.doi.org/ 10.1109/INMIC.2001.995315

[10] Haas Z, Pearlman M, Samar P. "The zone routing protocol (ZRP) for ad hoc networks". IETF Internet Draft, 2002. https://tools.ietf.org/html/draft-ietf-manet-zone-zrp-00

[11] Tarique M, Tepe KE, Adibi S, Erfani S. "Survey of multipath routing protocols for mobile ad hoc networks". Journal of Network and Computer Applications, Vol. 32, No. 6, 2009; 1125-1143. http://dx.doi.org/ 10.1016/j.jnca.2009.07.002

[12] Chiang CC, Wu HK, Liu W, Gerla M. "Routing in clustered multihop mobile wireless networks with fading channel". In SICON'97: proceedings of the 5th IEEE Singapore International Conference On Networks, Singapore, 1997; 197–211.

[13] Tornos JL, Piles JJ, Salazar JL. "ADSR: Authenticated DSR". In CRiSIS 2011: Proceedings of the 6th International Conference on Risk and Security of Internet and System. Timisoara, Romania 2011; 1-8. http://dx.doi.org/ 10.1109/CRiSIS.2011.6061839

[14] Hu YC, Perrig A, Johnson DB. "Ariadne: A secure on-demand routing protocol for ad hoc networks". In MobiCom 2002: Proceedings of the 8th annual international conference on Mobile computing and networking. Atlanta, USA, 2002; 12–23. http://dx.doi.org/ 10.1007/s11276-004-4744-y

[15] Kargl F, Geiβ A, Schlott S, Weber M. "Secure Dynamic Source Routing". In HICSS'05: Proceedings of the 38th Hawaii International Conference on System Sciences. Hawaii, USA, 2005; 320c. http://dx.doi.org/ 10.1109/HICSS.2005.531

[16] Kim J, Tsudik G. "SRDP: Secure route discovery for dynamic source routing in MANETs" Ad Hoc Networks, Vol. 7, No. 6. 2009; 1097-1109. http://dx.doi.org/10.1016/j.adhoc.2008.09.007

[17] Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM. "A secure routing protocol for ad hoc networks". In ICNP'02: Proceedings of the 10th IEEE International Conference on Network Protocols. Paris, France, 2002; 78-89. http://dx.doi.org/10.1109/ICNP.2002.1181388

[18] Zapata MG, Asokan N. "Securing ad hoc routing protocols". In Wise'02: Proceedings of the 3rd ACM workshop on Wireless security. Singapore 2002; 1-10. http://dx.doi.org/10.1145/570681.570682

[19] Li Q, Zhao M, Walker J, Hu YC, Perrig A, Trappe W. "SEAR: a secure efficient ad hoc on demand routing protocol for wireless networks". Security and Communication Networks Vol. 2, No. 4, 2009: 25–340. http://dx.doi.org/ 10.1002/sec.60

[20] Hu YC, Johnson DB, Perrig A. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks". Ad Hoc Networks, Vol.1, No. 1, 2003; 175-192. http://dx.doi.org/ 10.1016/S1570-8705(03)00019-2

[21] Hafslund A, Tonnesen A, Rotvik RB, Andersson J, Kure O. "Secure extension to the OLSR protocol". In proceedings of the OLSR Interop and Workshop. San Diego, USA, 2004; 1-4.

[22] Eschenauer L, Gligor VD, Baras J. "On trust establishment in mobile ad hoc networks". Lecture Notes in Computer Science, Vol. 2845, Proc. 10th Int. Security Protocols Workshop , 2004; 47–66. http://dx.doi.org/ 10.1007/978-3-540-39871-4_6

[23] Li J, Li R, Kato J. "Future trust management framework for mobile ad hoc networks". IEEE Communications Magazine, Vol.46, No.4, 2008; 108-114. http://dx.doi.org/10.1109/MCOM.2008.4481349

[24] Theodorakopoulos G, Baras JS. "On trust models and trust evaluation metrics for ad hoc networks". IEEE Journal on Selected Areas in Communications, Vol.24, No.2, 2006; 318-328. http://dx.doi.org/ 10.1109/JSAC.2005.861390

[25] Mejia M, Peña N, Muñoz JL, Esparza O. "A review of trust modeling in ad hoc networks". Internet Research, Vol. 19 No. 1, 2009; 88 – 104. http://dx.doi.org/10.1108/10662240910927849

[26] Marti S, Garcia-Molina, H. "Taxonomy of trust: categorizing P2P reputation systems". Computer Networks. Vol. 50, No.4. 2006; 472-484. http://dx.doi.org/10.1016/j.comnet.2005.07.011

[27] Govindan K, Mohapatra P. "Trust computations and trust dynamics in mobile adhoc networks: a survey". IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, 2011; 279–298. http://dx.doi.org/ 10.1109/SURV.2011.042711.00083

[28] Sun Y, Yu W, Han Z, Liu KJR. "Information theoretic framework of trust modeling and evaluation for ad hoc networks". IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, 2006: 305–317. http://dx.doi.org/ 10.1109/JSAC.2005.861389

[29] Pirzada AA, McDonald C. "Establishing trust in pure ad-hoc networks". In ACSC'04: Proceedings of the 27th Australasian conference on Computer science, Dunedin, New Zealand, 2004; 47-54.

[30] Sun Y, Han Z, Liu KJR. "Defense of trust management vulnerabilities in distributed networks". IEEE Communications Magazine Vol. 46 No.2, 2008; 112-119. http://dx.doi.org/ 10.1109/MCOM.2008.4473092

[31] Marti S, Giuli TJ, Lai K, Baker M. "Mitigating routing misbehavior in mobile ad hoc networks". In Mobicom'00: Proceedings of the 6th annual international conference on Mobile computing and networking. Boston, USA, 2000; 255-265. http://dx.doi.org/ 10.1145/345910.345955

[32] Virendra M, Jadliwala M, Chandrasekaran M, Upadhyaya S. "Quantifying trust in mobile ad-hoc networks". In KIMAS'05: proceedings of International Conference on the Integration of Knowledge Intensive Multi-Agent Systems. Waltham, USA, 2005; 65- 70. http://dx.doi.org/ 10.1109/KIMAS.2005.1427054

[33] Balakrishnan V, Varadharajan V, Tupakula UK, Lues P. "Trust and Recommendations in Mobile Ad hoc Networks". In ICNS'07: proceedings of the Third International Conference on Networking and Services. Athens, Greece, 2007; 64. http://dx.doi.org/ 10.1109/ICNS.2007.123

[34] Buchegger S, Boudec J. "Performance analysis of the confidant protocol: cooperation of nodes – fairness in distributed ad-hoc networks". In MobiHOC'02: proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing. Laussane, Switzerland 2002; 226-236. http://dx.doi.org/10.1145/513800.513828

[35] Pirzada AA, Datta A, McDonald C. "Incorporating trust and reputation in the DSR protocol for dependable routing". Computer Communications Vol. 29, No. 15 2006; 2806-2821. http://dx.doi.org/10.1016/j.comcom.2005.10.032

[36] Xia H, Jia Z, Li X, Ju L., Sha E.H. "Trust prediction and trust-based source routing in mobile ad hoc networks". Ad Hoc Networks Vol. 1, No. 7, 2013; 2096–2114. http://dx.doi.org/10.1016/j.adhoc.2012.02.009

[37] Grünwald PD, Dawid AP. "Game theory, maximum entropy, minimum discrepancy, and robust Bayesian decision theory". Annals of Statistics. 32. 2004; 1367-1433. http://dx.doi.org/10.1214/009053604000000553

[38] Sahadevaiah K, Prasad Reddy PVGD. "Impact of security attacks on a new security protocol for mobile ad hoc networks". Network Protocols and Algorithms, 3. 2011; 122–140. http://dx.doi.org/10.5296/npa.v3i4.1364

[39] Tseng FH, Chou LD, Chao HC. "A survey of black hole attacks in wireless mobile ad

hoc networks". Human-centric Computing and Information Sciences. (1.4) 2011; 1-16. http://dx.doi.org/10.1186/2192-1962-1-4

[40] Woungang I, Dhurandher SK, Obaidat MS, Peddi, RD. "A DSR-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks". Security and Communication Networks. 2013. http://dx.doi.org/10.1002/sec.766

[41] Cheng Y, Çetinkaya EK, Sterbenz JPG. "Dynamic source routing (DSR) protocol implementation in ns-3". In SIMUTOOLS'12: Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques. Brussels, Belgium. 2012; 367-374. http://dx.doi.org/10.4108/icst.simutools.2012.247749

## Copyright Disclaimer