# Survey: secure opportunistic routing protocols in wireless networks

Hanane Saidi*, Driss Gretete and Addaim Adnane

Département d'Informatique, Logistique et Mathématiques (ILM),
B.P. 241, Campus universitaire, 14000, Kenitra, Morocco
Email: hanane.saidi@uit.ac.ma
Email: driss.gretete@uit.ac.ma
Email: adnane.addaim@uit.ac.ma
*Corresponding author

**Abstract:** Opportunistic routing (OR) protocols in wireless network schemes are a rich research field. These protocols select the best path in order to send information and take the broadcasting medium into consideration. OR tends to reach better reliability and performance than traditional routing (TR). However, they are both equally vulnerable to the same attacks because wireless networks might be deployed in hostile or unwatched environments. The approaches in terms of routing are mainly focusing on energy preservation, robustness, etc. However few work has been done to secure routing protocols especially in OR. In this paper, we are going to give an analysis of OR protocols their classifications as well as an overview on the security approaches available for opportunistic routing protocols.

**Keywords:** wireless networks; security; opportunistic routing.

**Reference** to this paper should be made as follows: Saidi, H., Gretete, D. and Adnane, A. (2019) 'Survey: secure opportunistic routing protocols in wireless networks', *Int. J. Information Privacy, Security and Integrity*, Vol. 4, No. 1, pp.30–48.

**Biographical notes:** Hanane Saidi received her Network and Telecoms Engineering degree from the National School of Applied Sciences. She is also a PhD student at the same school and works on wireless sensors networks.

Driss Gretete is a Professor at the National School of Applied Sciences ENSA of the University Ibn Tofail of Kenitra, Associate of Mathematics Promotion 1993, obtained his DEA of the University Paul Sabatier of Toulouse and Doctorate of the University of Provence Aix Marseille I under the theme: Probability of returning random walks to locally compact groups. He started at the preparatory classes where he taught graduate mathematics classes from 1993 to 1996 and special mathematics classes from 1996 to 2009.

Addaim Adnane is a Professor at the National School of Applied Sciences of Kenitra, University Ibn Tofail. He holds a PhD in Applied Sciences from the Mohammadia School of Engineering in Electronics, Networks and Telecoms and a Postgraduate Diploma in 'Aerospace Science and Technology'.

This paper is a revised and expanded version of a paper entitled 'Survey: secure opportunistic routing protocols in wireless networks' presented at NISS2018, Tangier, 28 April 2018.

## 1 Introduction

The progress made in recent decades in the fields of microelectronics, and wireless communication technologies have produced reasonable components of a few cubic meters of volume. As a result, a new domain of research has been created to offer solutions economically attractive and easily deployable to remote monitoring and data processing even in complex and distributed environments this domain is wireless sensor networks. WSNs are made up of number of nodes deployed in order to collect and transmit environmental data to one or multiple nodes in autonomous way. These networks have an interest particularly for military, environmental, home automation, medical purposes and of course applications related to critical infrastructure monitoring. These applications often need a high level of security.

However because of their characteristics (lack of infrastructure, energy constraint, dynamic topology, large number of sensors, limited physical safety, reduced capacity of the nodes, …) the security of the sensor networks, today, of many scientific and technical challenges.

The routing techniques used in wired networks try to select the best nodes to forward and receive packets, these data can be then sent through one path like in traditional routing or broadcasted through multiple paths in a probabilistic way and this is the basic idea of opportunistic routing protocols. So, one of the important research fields in WSNs is the routing of packets, due to the limited resources of energy, it is one of the major design prerequisite for routing protocols. To save lot of energy, the transmission range of every sensor is restricted. Therefore, information packets, that ought to be transmitted across the network, have to be forwarded through many hops. Furthermore, the routing should be adaptable to topology changes and environmental influences by using small energy.

Even if the routing of packets in wireless sensor networks is important to ensure the communications between nodes, the security side should not be ignored, routing does not have to be limited in metrics like reliability, energy saving or robustness, and the non-consideration of security problems can be an opportunity for attackers to access to the network.

## 2 Traditional routing

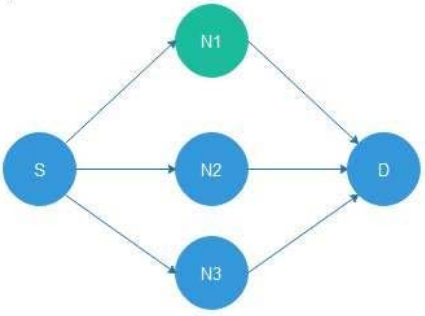
TR selects a path according to some metrics for a node and sends the packets to an intermediate relay to forward them to the destination.

TR ignores the wireless medium broadcast nature. Which however leads to packet loss, Figure 1 shows that the source has selected N1 to forward a packet N2 and N3 overheard it, N1 may face some hardware problems or may fail to receive the packets, the information is then lost so is the energy, the reliability decreases as well.

**Table 1** Comparison between OR and TR

| | *Broadcast nature* | *Number of relays* | *Relay selection* | *Packet overheard* | *Time of candidate selection* | *Type of transmission* |
|---|---|---|---|---|---|---|
| TR | Ignores | One | Fix | No | Before | Unicast |
| OR | Uses it | Multiple | Dynamically | Yes | After | Broadcast |

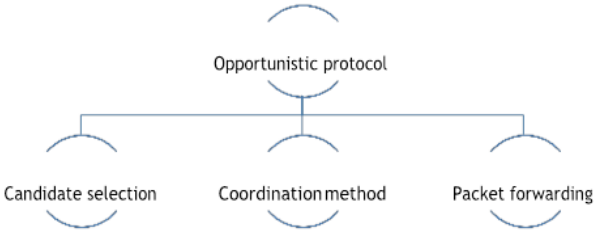
**Figure 1** Traditional routing transmission (see online version for colours)




## 3 Opportunistic routing

Most of traditional routing protocols such as dynamic source routing (DSR), Ad hoc on-demand vector (AODV), optimised link state routing (OLSR), select a short path between the source and the destination and send the traffic according to a specific path. OR in the other hand differs from TR by exploiting the broadcast nature of the wireless medium and changes the route after transmission. Basically, OR operates in three main steps first a packet is broadcasted to a group of nodes (set) that have fully received the packet, this set run a coordination protocol to choose the best node to forward the packet to the destination

**Figure 2** Opportunistic routing coordination methods (see online version for colours)




### *3.1 CRS*

In some opportunistic routing protocols like simple opportunistic adaptive routing (SOAR) (Rozner et al., 2009), the source selects using traditional routing a default candidates (set) each relay choose dynamically other neighbouring nodes to avoid duplication and this is what we call candidate relay set (CRS), another characteristic of OR is that it uses TR metrics such as expected transmission count (ETX) and expected transmission time (ETT). Which makes OR always relaying on TR, 90% of the packets are transferred using OR and 10% is sent using TR. When a CRS receive a packet, only

one node is in charge of forwarding, this selection is made by a coordination method whether based on a timer, token or network coding or contention. When a node is selected among a CRS the others cancel the overheard packet to avoid duplication transmission we will discuss the coordination methods in the next paragraph. An example of set selection in a wireless sensor environment under water is proposed by Menon (2016) that shows through a comparative analysis between OR protocols underwater for wireless sensors networks and divide them into location-based protocols such as VBF and geographic and opportunistic routing with depth adjustment-based topology control for communication Recovery (GeDAR). Moreover, a pressure based such as depth-based routing (DBR) protocol and void aware pressure routing (VAPR). The main characteristic of the first category is to use the location of the nodes to select the candidates, however, one of the disadvantages is the constraint of the bandwidth, but the second category uses depth and water pressure to select the relays.

### *3.2 Coordination phase*

The coordination method helps to know which node is best to forward the data packet, the nodes that should cancel it, this mechanism must choose the best relay with low energy time, and duplication cost. Researchers have divides the coordination methods into: timer-based, token-based and network coding-based coordination.

#### *3.2.1 Timer*

This type of coordination is the easiest to implement, but one of its weakness is it allows duplication. To select the best relay from the network, the source send the packet to all the nodes and then they are ranked by order of responding, the first to respond is the relay, this mechanism could also occur in a set of nodes to choose one of the CRS. Opportunistic wakeup MAC (OPWUM) (Aoudia et al., 2016) is a timer-based contention protocol for wireless sensors networks that allows selecting a relay with low cost of energy and preventing transmission duplication by allowing the relay to choose nodes from the neighbouring.

#### *3.2.2 Token*

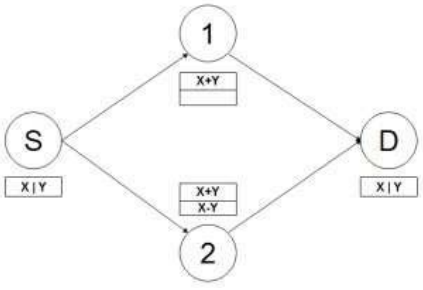
This method has been proposed by Hsu et al. (2009). A token sweep all the nodes of the network starting by the destination (higher priority) if a relay is selected an acknowledgement is injected in the token to avoid other nodes from transferring and thus avoid packet duplication, and this is the main advantage if this solution coped to timer-based coordination but the cost in terms of control packets and energy is high. Token-distributed coordination function (DCF) is a distributed MAC protocol that uses an overhearing technique to rank network stations for transmission on the wireless medium. The design goal of Token-DCF is to decrease idle and collision time, which significantly improves the performance in terms of system throughput and access delay. O-ACK is an efficient MAC protocol, which improves the channel utilisation by employing packet overhearing and eliminating explicit ACK frames. This protocol adjusts itself based on the surrounding environment. This protocol outperforms the DCF and Token-DCF protocol.

### *3.2.3 Network coding*

Network coding is a technique in which data is encoded at the source and decoded at the destination, to minimise the number of candidates and maximise the throughput. There is no coordination overheard when an opportunistic routing is network coding based which makes the wireless network duplication free.

Figure 3 shows that the packet is broadcasted into a linear combination. If we want to transmit the packets x and y to the destination through 1 and 2, the source codes the packet by engendering linear combination. In this example, 1 missed one packet but 2 received the mail. 1 and 2 code the packets again and forward them to the destination. With absence of coordination, the destination decodes and restores the initial packets.

**Figure 3** Network coding-based transmission




PlayNcool (Pahlevani et al., 2013), cooperative opportunistic alert diffusion (COPE) (Katti et al., 2008), BEND (Zhang et al., 2013) and MAC-independent opportunistic routing protocol (MORE) (Chachulski et al., 2007) are opportunistic routing protocols that use this type of coordination. Network encoding makes the network more robust and optimises the bandwidth. However, there are some issues concerning this technique such as:

- *Attacks vulnerabilities*

  A malicious node in a network can quickly spread the attack pollution to all the nodes by corrupting the packets even though they are encrypted by forging signatures. To avoid this, Charles et al. (2009) designed a homomorphic encryption signature to prevent attacks in network code-based wireless schemes, this technique allows nodes to sign any linear combination with no need of the agreement of the signing authority.

- *Packet redundancy*

  Redundancy is different than duplication. The latest generates an identical copy of the packet, redundancy adds superfluous information. Some network coding-based protocols such as MORE does not have redundancy problems it is a MAC-independent opportunistic protocol that randomly combine the packets before sending them which prevent the other nodes from forwarding the same packet. MORE is more utilised for stationary wireless schemes. We are not sure yet if it can be adaptable to dynamic scenarios with high mobility.

- *Time cost*

  In a vast wireless network, the time spent in coding and decoding may cost an important amount of time.

**Table 2** OR protocols classification

| *Timer-based* | *Token-based* | *Network coding-based* |
|---|---|---|
| OPWUM (Aoudia et al., 2016) | Token-DCF (Hosseinabadi and Vaidya, 2012) | MORE (Chachulski et al., 2007) |
| ExOR (Biswas and Morris, 2005) | O-ACK (Ahsan and Vaidya, 2015) | PlayNcool (Pahlevani et al., 2013) |
| SOAR (Rozner et al., 2009) | ECONOMY (Hsu et al., 2009) | COPE (Katti et al., 2008) |
| | | BEND (Zhang et al., 2013) |
| | | CodeOR (Lin et al., 2008) |
| | | slideOR (Lin et al., 2010) |
| | | XCOR (Koutsonikolas et al., 2008) |
| | | CCACK (Koutsonikolas et al., 2011) |

### *3.3 Transmission*

Opportunistic networks are unstable for the current opportunistic routing protocols. These networks may experience packet losses depending on the strength of the routing links. When a packet does not reach a destination, the source node resend it which decrease the performance of the network, the packet is definitely dropped when a maximum number of retransmissions is reached.

### *3.4 Current opportunistic routing protocols*

Many researches focused on creating protocols to improve the performances of opportunistic routing in wireless sensors networks. Let us cite the main ones:

a *Extremely opportunistic routing (ExOR)*

ExOR is the first OR protocol implemented in 2005 focusing on showing that opportunistic routing out performs traditional routing (Biswas and Morris, 2005). ExOR is based on batches each batch had its own ID a batch contains a number of packets, one batch is transferred when the transmission if the first one is fully completed. ExOR is timer-based which induced supplication.

Moreover, the main metrics used in this protocol are ETX and ETT. These metrics may degrade the performance of OR since they consider only one path which led to the idea of creating OR metrics such as expected any path transmission (EAX) and expected any path transmission time (EATT).

b *SOAR*

SOAR is a timer-based protocol. In it, the source used traditional routing to choose a candidate that dynamically adds other relays. SOAR out performs EXOR and prevent packet duplication (Rozner et al., 2009).

c *MORE*

MORE is a network coding protocol implemented in 2007 (Katti et al., 2008), it does not need any coordination for packet transmission but present some problems such as redundancy and batch limits. To overcome these issues, CodeOR (opportunistic routing in wireless mesh networks with segmented network coding) (Lin et al., 2008) deals with batch limits and cumulative coded acknowledgement (CCACK) gives an update of their neighbours status to prevent redundancy.

d *Geographic opportunistic routing (GOR)*

GOR is a geographic timer-based protocol and an improvement of CBF (Chakchouk, 2015) by reducing nodes overhead. OR chooses the closest relays to destination by EOT metric to prevent duplicate transmission. Multirate geographic opportunistic protocol (MGOR) is proposed as an improvement of GOR based on OEOT metric. This extension provides high throughput and low delay.

e *GeDAR*

GeDAR is a geographic opportunistic routing location-based protocol, which uses greedy forwarding when a packet reaches a relay to choose another candidate sensor (Coutinho et al., 2014).

f *LCOR*

Least cost opportunistic routing protocol based on EAX metrics. The algorithm computes all the possible neighbouring node combinations to choose the best path with the least cost (Dubois-Ferriere et al., 2010).

## 4 Security issues of OR protocols

We have noticed above that opportunistic routing face many problems such packet duplication, high-energy costs and some researchers have found solutions to these issues to add robustness and save energy in wireless networks. However, the security issues as important as the previous problems and we unfortunately notice a few work done to cope with the attacks threatening wireless sensors networks in general.

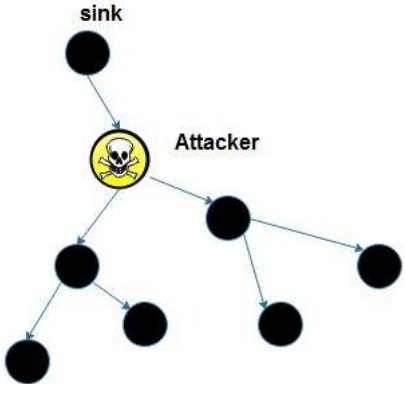
### *4.1 Attacks on wireless sensors networks*

Attacks against wireless sensor networks could be on the hardware or on the routing protocols. We can notice less damage in network coding-based protocols due to the fact that they involve coding and decoding mechanism but still both opportunistic routing and traditional routing are vulnerable to the same threats equally. Here the major attacks in wireless sensors network schemes:

### *4.1.1 Black hole attack*

Figure 4 shows that in a sinkhole or black hole attack, a malicious node collects all the traffic in the sensor network and instead of sending them to the destination, it drops them. In other scenarios, the attacker may spread false information between the nodes to make the illusion that the packets are correctly forwarded.

**Figure 4** Blackhole attack (see online version for colours)




### *4.1.2 Sybil attacks*

In the Sybil attack, a malicious node illegitimately takes multiple identities. The aim of this attack is to degrade the routing, data integrity, security and energy. The peer to peer is more vulnerable to Sybil whereas in wireless sensors networks it could be avoided by using correct protocols. Known targets of Sybil are the distributed storage, routing protocols, voting, data aggregation, resource allocation and misbehaviour detection (Newsome et al., 2004) has developed a probability equation to detect the existence of Sybil malicious nodes:

$$\Pr(detection) = 1 - \left( \sum_{S,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G} S-(m-M)}{\binom{n}{c} c} \right)^{r}$$

$n$ is the number of nodes in the network

$s$ infected nodes

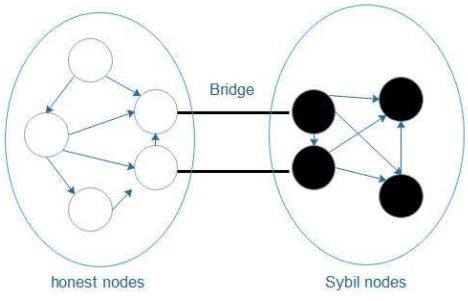
$m$ malicious nodes

$g$ safe nodes

$c$ number of tested nodes at a time

$r$ the number of rounds.

**Figure 5** Sybil attack mechanism (see online version for colours)

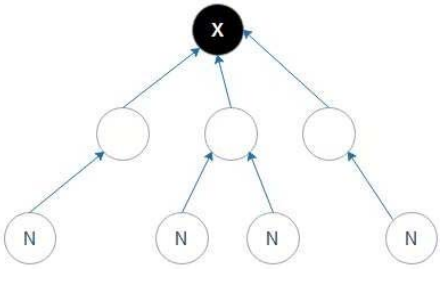



### *4.1.3 Hello flood attack*

Discovery protocols in wireless schemes use HELLO messages to discover neighbouring nodes. In a HELLO flood attack, the attacker uses these packets to saturate the network and consume its energy.

The malicious node X in Figure 6 has a powerful connection that allows it to send HELLO messages to a large number of nodes in a continuous manner. The neighbouring nodes N will then try to answer it, even if they are located at far distances from the malicious node. By dint of trying to answer these messages, they will gradually consume all of their energy.

**Figure 6** Hello flood attack (see online version for colours)




### *4.1.4 Denial of service*

A so-called denial of service attack in a computer network is an attack carried out in order to harm the normal operation of this network.

There are many ways to proceed, and there is there for a multitude of existing denial of service attacks. The state of the art in this field has the particularity that it includes two points of view: one from the attacker and the other from the 'defender'. It is essential to be able to define the model of an attack to be able to propose adequate counter measures. In addition, more or less reciprocally, the protective mechanisms put in place over time push attackers (or researchers) to develop new attacks to circumvent them.

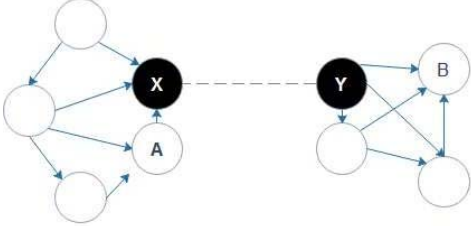
Sensor networks are unfortunately very exposed to attacks as denial of service, due to:

- their extremely limited resources, and mainly in terms of energy
- their weak capabilities, which can introduce delays (latency in communications or processing time)
- their exposure to physical attacks
- the low reliability of the transmission medium, about confidentiality or collisions
- their remote management
- the lack of centralised management (and the impossibility of knowing precisely the status of other nodes).

### *4.1.5 Wormhole attack*

The attack of the wormhole requires the insertion of at least two malicious nodes. These two nodes are connected by a powerful connection such as a wired link. The purpose of this attack is to mislead neighbouring nodes over distances. Generally, the routing protocol looks for the shortest path in hop count, in the case of a wormhole attack; the two malicious nodes make it possible to reach a distant place with a single jump. This possibility will mislead the other nodes on the real distances that separate the two nodes, but will especially force the neighbouring nodes to pass by the malicious nodes to transfer the information. Thus, the malignant nodes that form the wormhole will be in a privileged position that will allow them to have priority over information flowing through their near nodes. This attack is shown in Figure 7 where two malicious nodes X and Y, form a wormhole. The nodes A and B will prioritise the fastest route formed by the wormhole, and thus the attacker can retrieve the information (Ji et al., 2014).

**Figure 7** Wormhole attack mechanism (see online version for colours)




### *4.1.6 Selective forwarding*

Selective forwarding is harder to detect. A malicious node may drop the packets from some selected nodes and forward those from other nodes. A more subtle way is to drop packets intermittently so that it behaves like an unstable channel. Most routing protocols require that each sensor node periodically broadcast routing information to maintain the network topology.

#### 4.1.7 Acknowledgement spoofing

Numerous sensor network routing protocols depend on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgements for 'overheard' packets broadcasted to neighbouring nodes. The purpose is to convince the sender that a weak link is strong or that a damaged node is active. For example, a routing algorithm may select the next candidate in a route using link reliability. Artificially reinforcing a weak link is a subtle way of manipulating such a scheme. Since that packets sent along weak links are lost, an attacker can effectively place a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

## 5 Secure OR protocols

We have noticed previously that wireless networks can be threatened by external and internal attacks, which make the security as serious matter to take into consideration. Opportunistic routing is also concerned, and the steps made to improve the integrity of data on OR are little most of researchers focus on energy saving and robustness, but we cannot deny that some work has been done to secure OR new security protocols had been implemented, or some existing protocols are improved to add security to the network that we have now security protocols based on cryptography, trust-based OR protocols, and game theory category. In this section, we will discuss all the proposed protocols or combination of these techniques.

### 5.1 Cryptographic-based OR protocols

#### 5.1.1 SecEXOR

SecEXOR is an improvement of EXOR. It adds a digital signature and Lagrange Polynomial Group (LPG) for key distribution to ensure the security of OR protocol for wireless networks. SecExOR generates a public and a private key for each node in the network to establish authentication before sending packets to the destination. A digital signature and a hash protocol is used to guarantee the integrity of data. Private keys are generated based on Lagrange polynomial group and the keys are pre-shared to ensure the confidentiality of the transmission and data packets. Generating keys and pre sharing them requires a considerable amount of energy and processing time as well, which makes this protocol quite hard to apply on real networks especially wireless sensors networks that have limited storage and processing memory (Zhou et al., 2010).

#### 5.1.2 INPAC

INPAC is a combination of cryptographic and game theory techniques. It is an improvement of MORE protocol for wireless mesh schemes. It implements an incentive algorithm for routing to enforce nodes to accurately communicate the status of their links, to know approximately the number of transmissions a node can make. This mechanism is based on payment formula of node reports true information, false reported information nodes are not paid and punished. The author suggests solutions as well to prevent false reports and problems that may face this approach. Moreover nodes watch each other's

forwarding activities and communicate their neighbours' behaviours. INPAC supervise the timing of transferring and receiving activity for each node, if a relay takes more time than usual and another candidate repays it, the latest get paid for preventing the packets delay (Chen and Zhong, 2014).

#### *5.1.3 Privo*

Privacy preserving opportunistic routing (Privo) for delay tolerant networks ensures privacy by protecting nodes sensitive information. Nodes compare their routing metrics in a private manner using homomorphic encryption. The main metric on which this protocol relies is pweight (Privo weight) which is a time metric based on nodes encounter history to know the behaviour of nodes. The privacy aspect of this protocol allows relays to know each other's metrics without disclosing them (Magaia et al., 2017).

### *5.2 Trust-based OR protocols*

#### *5.2.1 SGOR*

Scalable geographic opportunistic routing (SGOR) implements an ambient sensitive direct and indirect (that depend on the cooperation of sensor nodes in verifying locations) trust-based model to secure geographic opportunistic routing in wireless sensors networks without costly public key infrastructures. It can prevent a many serious attacks such as location spoofing, which is detected by cooperated sensor nodes using received signal strength (RSS) in physical layer. In a network, nodes watch the transferring behaviour of the neighbours, and depending on the degree of cooperation of each node, a trust value is given to them. Lyu et al. (2015) show the efficiency of SGOR against Sybil attacks by using location and RSS because these values are the same between two benign nodes, when a candidate starts to drop packets the trust value given to it decreases and will not be chosen for next transmission. This mechanism can be deployed in rushing attacks replay attacks and wormhole attacks (Lyu et al., 2015).

#### *5.2.2 MCOR*

Minimum cost routing algorithm (MCOR) is a trust-based opportunistic forwarding model. In this protocol, each node can check the close relays transmitting conduct accurately, and chose the best candidate from the trusted forwarding list to attenuate node misbehaviour. Moreover, each node can also select the minimum cost path to minimise the number of packet retransmissions during the packet transmission phase. The authors defined a trust level for each node as well conforming to the previous cooperation behaviours that is divided into two parts: the direct trust level of each node and recommendation trust level based its similar recommendation capacity. In addition to that, Jie et al. (2012) give extended formulas on opportunistic routing trust-based real cost, which also contains two components: fore link cost and remaining path cost. Then, we define a simple effective forwarder selection mechanism and propose a trusted opportunistic forwarding model to select the least cost trusted opportunistic routing among all the potential trusted routes. They also designed a trusted minimum cost routing algorithm and use trust degree of next-hops to make an optimal routing choice by

choosing an effective forwarder from each trusted neighbour forwarding list, to improve the packet transmission efficiency and alleviate the malicious attacks (Jie et al., 2012).

### *5.2.3 TRP*

Smita and Patel (2017) propose a trust-based routing protocol to diminish the impact of attacks in opportunistic routing schemes. The proposed protocol evaluates the capacity of a relay node to diminish the impact of a malicious node. TRP is based on the following components; scenario assumption where packets are transmitted among the candidates using the store-carry-forward technique. Each node tries to send a message using it maximum capacity of transmission to detect the misbehaviours in an opportunistic network no duplication of the packets is allowed this method allows to determine the malicious nodes in the network. To guarantee data integrity and confidentiality each node has it private and public key to encode and decode the messages delivered by a public key infrastructure. In addition to this module, the authors have proposed an observer element that collects direct and indirect samples to study the nodes behaviours to attribute rewards using a trust management module (Smita and Patel, 2017).

## *5.3 Game theory OR protocol*

Game theory is a technique used first in the economic field to predict the effect of a phenomenon when different parts are competing for the same resources. This scheme is used to secure opportunistic routing. Nodes are players in a routing game. Benign and malicious nodes are both parts of the game. The mathematical design of the game theory fixes the conflict between players aiming for the same goal. In opportunistic routing, scheme for example, benign nodes tend to find efficient and best path to transfer the packets whereas malicious nodes tend to drop messages, the evolution of Game theory has settled a new mathematical model that nodes will follow when malicious appear in the network. In this section, we are going to list the existing game theory-based opportunistic routing protocols.

### *5.3.1 COMO*

Cooperation-optimal protocol for multirate opportunistic routing (COMO) is a game theory-based that stands for cooperation optimal protocol for multirate opportunistic routing and forwarding. This protocol mainly aim to prevent selfish nodes to ensure fidelity of the players and reach maximised end to end throughput by using Nash equilibrium (Wu et al., 2014).

When the nodes obey the protocol, the network is optimised and the nodes get paid. The protocol measures link loss probabilities to include probe message. COMO uses cryptographic elements to defend the probed messages from casting. The payment scheme ensures that nodes do not take advantage from link loss probabilities. COMO main metric is EATT (time metric). In a real network, a source node pays the relays for transmitting packets. By using the strongly Pareto, the relays cannot expand their utility if the other nodes utility does not decrease.

Wu et al. (2014) have experimented COMO on ORBIT wireless scheme and could prevent nodes misbehaviours, because nodes report the activity of their neighbours using traditional routing to compute the link loss probabilities. Moreover, when a node reports, it gets paid and thus prevents selfish relays. Authors provided an extended amount of simulation to show the efficiency to prevent selfish behaviours.

### *5.3.2 GISSO*

The aim of game theoretic incentive scheme for social aware routing (GISSO) is to stimulate social selfish relays to maximise the performance of MSNs networks (Jedari et al., 2017). GISSO architecture is based on these main components:

- *Social utility calculator*

  The social utility calculator has a function that uses social information, space and table characteristics of their lays to measure the social benefit of a non-local message to a relay node. Jedari et al. (2017) created two elements in this composing, particularly social tie measurement and message appraisal. The first module calculates the tie capacity between two mobile relays according to social analogy approach. Let us suppose that the nodes can have many social characteristics, a statistical technique to recognise the import of the characteristics of the relays. The Message Appraisal computes the cost of each message to a relay node according to their importance of the message content. The candidate social service is utilised by message handler and selfish-aware message delivery elements to hold the message forwarding.

- *Message handler*

  The message handler determines the forwarding order of the messages and administers the buffer of each node in GISSO. Two elements are created for this component; the authors have designed two features priority manager and buffer manager. The first determine the transmission priority of packets. The problem is the order of the packets is affected by the link duration between two candidates is finite and delays may happen. The authors divided the transmission of the messages into two phases. When two nodes establish a link to transmit a packet, the packets are first forwarded to another relay where messages are ranked in priority order according to their TTL. The packet in this first phase could add the local or non-local messages or both. In the second phase, the saved packets are forwarded to the area where they are ranked in an ascending order of their social utility to the destination. The buffer manager deletes the copies of the packets because non-local messages cannot be stored for a long duration to have enough space for other messages and also they might slow down the process. Otherwise an over flow problem will be caused. GISSO uses replicas of the packets some of these may still be saved in the nodes which may slow the computing and saturates the network due to the lack of space. The authors overcome this issue by creating garbage where non-local messages are collected or ask the nodes to put their useless packets in the garbage.

- *Incentive scheme*

  The purpose of this component is to motivate the nodes to transmit less useful information from other relays. For this, Jedari et al. (2017) created two elements in this component, the bargaining mechanism and the reputation mechanism. The first uses a bargaining game way where the source (buyer) bargains with another relay (seller) to perform a transmission aid in some cases. By using virtual money as negotiation between the nodes. When an arrangement is settled the sender pays an amount of money to the destination candidate, the node can transmit the message. The reputation mechanism in the other hand shows the degree of cooperation of the relays to transmit the message. The purpose of the reputation mechanism is to motivate a node to bargain over non-local packets. If a node has a good reputation, they get a discount on the amount of money they should normally pay for forwarding non-local. The reputation may increase or decrease depending on the amount of reputation a node achieves by forwarding the message that has an inversely proportional to her social tie strength and the appraisal of the message to her. Meanwhile, the reputation of a node is decreased proportionally to the period between her last and current message forwarding.

- *Selfish aware message delivery*

  This element is the main purpose of GISSO protocol that administers the traffic between the nodes. In an opportunistic routing scheme, the paths dynamically change depending on the best-chosen path to send a packet; the link between relays is thus changes as well. Therefore, the amount of exchanged packets between the nodes may change to lead to an unbalance of charges for every node. To overcome this problem, the authors suggested TFT technique that makes a node send a message and wait until it receives another.

### *5.3.3 AIM*

Auction incentive mechanism in wireless networks with opportunistic routing (AIM) is a game theory-based protocol, it prevent selfish nodes behaviours in opportunistic routing protocol SOAR (time-based coordination) (Zhang et al., 2013), and make the energy consumption even equal between the nodes. The source node uses a payment technique to make the relays transmit the packet to the destination. The forwarding nodes send the bids. Zhang et al. (2013) designed a forwarding auction game. First the source chooses an amount of forwarding nodes, these relays determine the price that a node deserve to get to forward the packet. The aim of the auction game is to settle a pricing plan in order to optimise the transmission. AIM achieves The Bayesian Nash equilibrium solution to maximise the benefit of the nodes. This process requires an important amount of energy. The authors did not forget this detail by including it in the auction game process.

**Table 3** Comparison of secured OR protocols

| *Securing technique* | *Secured opportunistic protocol* | *Original OR* | *Metrics* | *Coordination* | *Main advantage* | *Problems* | *Wireless topology* |
|---|---|---|---|---|---|---|---|
| Cryptography | SecExOR | ExOR | ETX | Time-based | Secure transmission thanks to private/public key | Important energy cost due to coding and encoding key generation | WSN |
| | INPAC (Wu et al., 2013) | MORE | ETX | Network coding | Isolate and punish malicious nodes | Does not solve dynamic link loss probability | Wireless topology |
| | PRIVO (Magaia et al., 2017) | DTN protocols | MTTE | Network coding | Reduce the cryptography energy consumption | Does not overcome all attacks | DTN |
| Trust-based | SGOR (Lyu et al., 2015) | Geographic OR protocols | Distance | Timer-based | High performance against location attacks | Does not prevent all attacks | WSN |
| | MCOR (Bo et al., 2011) | LCOR | EAX | Timer-based | Tend to minimise energy consumption | No trust-based metric | Wireless topology |
| | TRP (Smita and Patel, 2017) | PROPHET | ONE | Network coding | Promote the cooperation between nodes to avoid selfish behaviours | Not applied on community-based networks | DTN |
| | Salehi and Boukerche (2015) | GEOTOR | | Timer-based | Isolate malicious nodes | Does not prevent collision attacks | WSN |
| Game theory | COMO (Wu et al., 2014) | MORE | EATT | Network coding | Overcome selfish behaviours | Energy consumption | Wireless topology |
| | GISSO (Jedari et al., 2016) | SCORP | SS | Timer-based | Introduce a buffer technique to save and drop packets | Does not consider trust aging metric | MSN |
| | AIM (Zhang et al., 2010) | SOAR | ETX | Timer-based | Reduce energy consumption during routing | Does not control malicious nodes | WSN |

## 6 Discussion

This paper has presented the existing security protocols in opportunistic routing protocols. We have compared the OR protocols to traditional routing and concluded that the main feature was that OR consider the broadcast medium nature. Table 3 presents a classification according to trust theory cryptography and trust-based opportunistic routing protocols approaches. It makes also a comparison between their performances and the wireless topologies they fit in. The metric section shows the main criteria on which the OR protocols rely onto forward packets. All the previous cited protocols are summarised in that table to give a clear idea about the researchers work to improve the performances of opportunistic routing protocols. The protocols do not perfectly solve the wireless networks problems as long as the combination of security and routing cost an important amount of energy and computing compared to the small capacity of the nodes. Each protocol has their pros and cons cited in Table 3.

## 7 Conclusions

The main concern of wireless networks is routing and we noticed that most of developed routing protocols are mainly focusing on metrics like energy saving and robustness while security measures are being ignored knowing that sensors are deployed in sensitive areas and environments that need to be watched and secured. For this purpose, this paper presented several existing security solutions in opportunistic routing networks and the main related areas for secure routing were discussed such as cryptography key establishment trust and reputation systems.

Opportunistic routing is now the main way to optimise the network performance because it depends on the broadcast nature of the network, so researchers have proposed some solutions to protect it against malicious nodes and adversaries but the work in this field has been insufficient and still need more studies. It has given us the motivation to develop a new security concept based on a famous OR protocol ExOR that will be the project of our next paper.

## References

Ahsan, S.B. and Vaidya, N.H. (2015) 'O-ACK: an adaptive wireless MAC protocol exploiting opportunistic token-passing and ack piggybacking', in Kanhere, S., Tolle, J. and Cherkaoui, S. (Eds.): *Proceedings of the 40th Annual IEEE Conference on Local Computer Networks, LCN 2015, [7366340] (Proceedings – Conference on Local Computer Networks, LCN)*, 26–29 October, pp.410–413, IEEE Computer Society.

Aoudia, F.A., Gautier, M. and Berder, O. (2016) 'OPWUM: opportunistic MAC protocol leveraging wake-up receivers in WSNs', *Journal of Sensors*, Vol. 2016, Article ID 6263719, 9pp, https://doi.org/10.1155/2016/6263719.

Biswas, S. and Morris, R. (2005) 'ExOR: opportunistic multi-hop routing for wireless networks', *ACM SIGCOMM Comput. Commun. Rev.*, Vol. 35, No. 4, p.133.

Bo, W., Chuanhe, H., Layuan, L. and Wenzhong, Y. (2011) 'Trust-based minimum cost opportunistic routing for ad hoc networks', *Journal of Systems and Software*, Vol. 84, No. 12, pp.2107–2122.

Chachulski, S., Jennings, M., Katti, S. and Katabi, D. (2007) 'Trading structure for randomness in wireless opportunistic routing', *ACM SIGCOMM Computer Communication Review*, October, Vol. 37, No. 4, pp.169–180.

Chakchouk, N. (2015) 'A survey on opportunistic routing in wireless communication networks', *IEEE Communications Surveys & Tutorials*, Vol. 17, pp.2214–2241.

Charles, D., Jain, K. and Lauter, K. (2009) 'Signatures for network coding', Vol. 1, No. 1, pp.3–14.

Chen, T. and Zhong, S. (2014) 'An enforceable scheme for packet forwarding cooperation in network-coding wireless networks with opportunistic routing', *IEEE Transactions on Vehicular Technology*, Vol. 63, pp.4476–4491, 10.1109/TVT.2014.2312171.

Coutinho, R.W.L., Boukerche, A., Vieira, L.F.M. and Loureiro, A.A.F. (2014) 'GEDAR: geographic and opportunistic routing protocol with depth adjustment for mobile underwater sensor networks', in *2014 IEEE International Conference on communications (ICC)*, IEEE, pp.251–256.

Dubois-Ferriere, H., Grossglauser, M. and Vetterli, M. (2010) *Least-Cost Opportunistic Routing*.

Hosseinabadi, G. and Vaidya, N, (2012) *Token-DCF: An Opportunistic MAC Protocol for Wireless Networks*, arXiv February, ID 1202.0582, p.1202.0582.

Hsu, C-J., Liu, H-I. and Seah, W. (2009) *Economy: A Duplicate Free Opportunistic Routing*, 10.1145/1710035.1710052.

Jedari, B., Liu, L., Qiu, T., Rahim, A. and Xia, F. (2017) 'A game-theoretic incentive scheme for social-aware routing in selfish mobile social networks', *Future Generation Computer Systems*, Vol. 70, pp.178–190, ISSN: 0167-739X.

Ji, S., Chen, T. and Zhong, S. (2014) 'Wormhole attack detection algorithms in wireless networkcoding systems', *IEEE Transactions on Mobile Computing*, Vol. 1233, No. C, pp.1–14.

Jie, Z., Huang, C., Xu, L., Wang, B., Xi, C. and Fan, X. (2012) 'A trusted opportunistic routing algorithm for VANET', *Proceedings of the International Conference on Networking and Distributed Computing, ICNDC*, pp.86–90, 10.1109/ICNDC.2012.28.

Katti, S. et al. (2008) 'XORs in the air: practical wireless network coding', *IEEE/ACM Trans. Netw*., Vol. 16, No. 3, pp.497–510.

Koutsonikolas, D., Hu, Y.C. and Wang, C-C. (2008) 'XCOR: synergistic interflow network coding and opportunistic routing', in *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking (MobiCom)*, September, pp.1–3.

Koutsonikolas, D., Wang, C. and Hu, Y.C. (2011) 'Efficient network-coding-based opportunistic routing through cumulative coded acknowledgments', *IEEE/ACM Transactions on Networking*, Vol. 19, No. 5, pp.1368–1381.

Lin, Y., Li, B. and Liang, B. (2008) 'CodeOR: opportunistic routing in wireless mesh networks with segmented network coding', in *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, IEEE, Orlando, FL, pp.13–22.

Lin, Y., Li, B. and Liang, B. (2010) 'SlideOR: online opportunistic coding in wireless mesh networks', in *Proceeding of IEEE conference on Computer Communications (INFOCOM)*, San Diego, CA, IEEE.10.1109/INFCOM.2010.5462249, pp.171–175.

Lyu, C., Gu, D., Zhang, X., Sun, S., Zhang, Y. and Pande, A. (2015) 'SGOR: secure and scalable geographic opportunistic routing with received signal strength in WSNs', *Comput. Commun*., March, Vol. 59, No. C, pp.37–51.

Magaia, N., Borrego, C., Pereira, P.R. and Correia, M.P. (2017) 'PRIVO: a privacy-preserving opportunistic routing protocol for delay tolerant networks', in *IFIP Networking*, pp.1–9 [online] http://dl.ifip.org/db/conf/ networking/networking2017/1570333245.pdf.

Menon, V.G. (2016) 'Comparative analysis of opportunistic routing protocols for underwater acoustic sensor networks department of information technology', *2016 Int. Conf. Emerg. Technol. Trends*.

Newsome, J., Shi, E., Song, D. and Perrig, A. (2004) *The Sybil Attack in Sensor Networks: Analysis & Defenses*, pp.259–268, ACM Press.

Pahlevani, P., Lucani, D.E., Pedersen, M.V. and Fitzek, F.H.P. (2013) 'PlayNCool: opportunistic network coding for local optimization of routing in wireless mesh networks', in *Proceedings of the 2013 IEEE Globecom Workshops (GC Wkshps)*, Atlanta, GA, USA, 9–13 December, Vol. 1.

Rozner, E., Seshadri, J., Mehta, Y. and Qiu, L. (2009) 'SOAR: simple opportunistic adaptive routing protocol for wireless mesh networks', *IEEE Trans. Mob. Comput.*, Vol. 8, No. 12, pp.1622–1635.

Salehi, M. and Boukerche, A. (2015) 'A comprehensive reputation system to improve the security of opportunistic routing protocols in wireless networks', *Wireless Networks archive Journal*, Vol. 25, No. 2, pp.559–571

Smita, P. and Patel, S. (2017) 'Trust based opportunistic routing scheme', *International Journal of Applied Engineering Research*, Vol. 12, No. 10, pp.2123–2126, ISSN: 0973-4562.

Wu, F., Chen, T., Zhong, S., Qiao, C. and Chen, G. (2013) 'A game-theoretic approach to stimulate cooperation for probabilistic routing in opportunistic networks', Vol. 12, No. 4, pp.1573–1583.

Wu, F., Gong, K., Zhang, T. and Chen, G. (2014) 'COMO: a game-theoretic approach for joint multirate opportunistic routing and forwarding in non-cooperative wireless networks', *IEEE Transactions on Wireless Communications*, Vol. 14, No. 2, pp.948–959; Vol. 1276, No. C, pp.1–12.

Zhang, J., Peter, Y. and Marsic, I. (2010) 'MAC-layer proactive mixing for network coding in multi-hop wireless networks', *Comput. Networks*, Vol. 54, No. 2, pp.196–207.

Zhang, Y., Lee, C., Niyato, D. and Wang, P. (2013) 'Auction approaches for resource allocation in wireless systems: a survey', *Communications Surveys & Tutorials*, IEEE. 15.1020-1041.10.1109/SURV.2012.110112.00125.

Zhou, Y., Tan, X., He, X., Qin, G. and Xi, H. (2010) 'Secure opportunistic routing for wireless multi-hop networks using LPG and digital signature', *Information Assurance and Security Letters*, Vol. 1, pp.18–23.