Ad Hoc Networks 000 (2016) 1–14

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks

Mahmood Salehi*, Azzedine Boukerche, Amir Darehshoorzadeh

School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Ontario, Canada

ARTICLE INFO

Article history:
Received 15 December 2015
Revised 10 May 2016
Accepted 8 July 2016
Available online xxx

Keywords:
Wireless mesh network
Opportunistic routing
Malicious node
Modeling
Markov

ABSTRACT

In wireless networks, opportunistic routing (OR) protocols are designed to route data packets towards their destination with greater reliability than traditional routing schemes. In addition to reliability, nodes' trustworthiness and willingness to cooperate can also play a significant role in the delivery of packets to their final destinations. More specifically, nodes in the network may be compromised, experience software or hardware failures, or behave maliciously for various reasons. Therefore, it would be beneficial to model the behavior of malicious or uncooperative nodes and study their effects in a wireless network that employs OR for communications. In this paper, the behavior of malicious nodes in a wireless mesh network that utilizes unicast opportunistic routing protocols is modeled using Discrete Time Markov Chain (DTMC). Afterwards, using the proposed model, we introduce a novel approach for the calculation of packet drop ratio, through which the negative effects of uncooperative nodes can be calculated. Furthermore, a customized version of a black-hole attack is introduced as an example of malicious behavior in OR protocols; we apply this routing attack to several well-known OR protocols, with the additional use of network simulation as well as through the proposed analytical technique. Finally, a comprehensive set of performance evaluation scenarios is designed and applied, with the purpose of investigating the effects of different parameters on a wireless mesh network that uses OR as a routing approach in the presence of malicious nodes. Evaluation results indicate that the proposed black-hole attack can significantly downgrade communication performance, and the proposed model can properly model the effects of malicious nodes on OR protocols.

1. Introduction

Ensuring the reliability of end-to-end packet routing is of significant importance in wireless networks. *Opportunistic Routing* (OR) protocols are a set of unicast or multicast routing protocols designed to address such reliability requirements. As discussed in [1], the main purpose of OR protocols is to more effectively use the broadcast nature of packet transmissions in wireless networks. To be more specific, when a packet is transmitted in wireless networks through a specific node, all neighboring nodes that are geographically located in the transmission radius of the sending node may receive it. In contrast to traditional routing schemes such as DSR, AODV, OLSR, etc. [2] which suggested selecting only one node in each hop of the routing process to operate as the actual next-hop forwarder and to assist in transmitting the packet towards its destination, OR methods select a subset of neighbors, known as the *candidate set*, as potential next hop forwarders.

In OR protocols, the candidate set of each node is selected using a candidate selection algorithm, and different aspects are considered to increase the probability of delivering packets to their final destination. Amongst the nodes in the candidate set, however, one node will act as the actual next hop forwarder; this node transmits the packet one hop further on its way towards the destination. This node is determined by performing a *candidate coordination* mechanism between nodes in the candidate set. Upon transmission of the packet, such a candidate should wait to receive an acknowledgment from one of its own candidates to ensure that the packet has been successfully forwarded; otherwise, it tends to retransmit the packet for the maximum number of predetermined repetitions. This process increases the likelihood of delivering each packet to its destination. As mentioned in [1], most of the research in the area of OR paradigms is focused on different candidate selection and coordination methods.

Although a tremendous amount of research has been conducted in the interest of various candidate selection and coordination

* Corresponding author.
E-mail addresses: msalehi@uottawa.ca (M. Salehi), boukerch@site.uottawa.ca (A. Boukerche), adarehsh@uottawa.ca (A. Darehshoorzadeh).

http://dx.doi.org/10.1016/j.adhoc.2016.07.004
1570-8705/

methods for OR protocols [1], the research in this area is still ongoing in terms of security and aspects of trustworthiness. To be more specific, almost all of the well-known proposed OR protocols operate following a strong assumption that all nodes in the network are benign and cooperative nodes. In real world situations, however, the scenario might be completely different, and nodes may not behave as expected when it comes to cooperation in network operations. This adversarial behavior occurs as a result of varying malicious or selfish intentions, and can have devastating effects on the performance of communication in wireless networks. For example, in *black-hole* attack [3], which is categorized as a Denial of Service (DOS) attack, malicious nodes seek selection by other nodes in the network as next-hop forwarders, and attract as many data packets as possible. Instead of forwarding, however, such nodes will tend to discard all of the received packets, and decrease network performance.

To the best of our knowledge, the effects of malicious nodes in OR protocols have not yet been significantly studied and investigated. This lack of research has motivated us to propose a model that demonstrates the behavior of uncooperative nodes in OR-based wireless mesh networks, in which candidate nodes follow *perfect coordination*. As explained in [1], perfect coordination implies a situation in which data packet forwarding through a highest-priority candidate that has received the packet results in notification of this transmission to all other candidates, including the previous-hop; this prevents them from forwarding the same packet again. The proposed model, which is an extended version of our previous work [4], is considered a comprehensive approach for investigating the behavior of adversary nodes in unicast OR protocols, when such nodes probabilistically prevent collaboration with benign nodes. In this extension, the proposed model has been elaborated in greater details. Furthermore, a novel method and model for calculating the packet drop ratio is proposed. This makes it possible to more accurately measure the effects of malicious nodes or node failures on data packet drop rates. In addition, some of the various applications and scenarios that accommodate the proposed model including, but not limited to, highly sensitive networks, underwater sensor networks, and environment monitoring applications are explained and studied. This demonstrates the effectiveness with which the proposed model can be applied to provide an estimation of the network connectivity and performance in real-world applications. Furthermore, in order to investigate the effects of different candidate selection algorithms, the introduced model is applied to four well-known OR protocols. Thus, it becomes possible to investigate the behavior of different protocols using the proposed analytical model in the presence of malicious nodes. Finally, a more comprehensive set of evaluations is performed and studied, creating the possibility of studying the proposed model more extensively under different network conditions.

Some of the most important contributions of this paper can be listed as follows.

- First, a novel model to represent the OR-based wireless mesh network is introduced using Discrete-Time Markov Chain (DTMC) for use where malicious and uncooperative nodes exist in the system and prevent data packet forwarding. A set of scenarios and applications is also provided to indicate how the proposed model can be applied.
- Second, using the proposed model, a new approach for the calculation of *packet drop ratio* parameter is introduced. Drop ratio assists in measuring the effects of uncooperative nodes in an OR-based wireless mesh network.
- Third, a novel version of the black-hole attack is introduced, in which the malicious node receives a data packet from a previous hop, drops the packet, and pretends that it has already forwarded the packet so that other candidates do not repeat the transmission.
- Fourth, the effects of the proposed model are evaluated by performing a comprehensive set of performance evaluation tests that consider different network parameters, using both analytical and simulation results. The evaluation is applied and studied on four well-known OR protocols.

The remainder of this paper is organized as follows. Section 2 consists of the most current research in OR methods and secure routing. Some of the applications of the proposed model in real-world scenarios are discussed in Section 3. In Section 4, the proposed DTMC model is elaborated and discussed in greater detail. An analysis of the proposed model is presented in Section 5, and results are discussed in Section 6. Finally, Section 7 concludes the paper and introduces some areas for future research.

2. Related works

Since the presented paper introduces a novel approach to model the effects of malicious nodes in OR-based wireless networks, this is of significant importance for studying the state of the arts in both areas of OR protocols, as well as in secure routing. In the following sub-sections, some of the most important research findings in the mentioned areas are briefly investigated.

2.1. Opportunistic routing protocols

Routing operations in OR protocols, as mentioned in Section 1, are divided into two major phases, known as candidate selection and candidate coordination. Therefore, most of the research in such an area focuses on various methods of performing candidate selection or coordination. Amongst the two, however, candidate selection methods have received more attention from researchers in recent years. In order to select candidates, some methods require a global knowledge of the entire network topology, whereas other techniques only utilize local information. In addition, various methods use different metrics and parameters in the candidate selection process. The quality of communication links between nodes, geographical location of nodes, and security considerations such as trustworthiness of potential candidates are some of the most important parameters used for candidate selection. [1] presents a comprehensive study on different aspects and protocols of OR protocols.

Extremely Opportunistic Routing (EXOR) [5] is one of the primarily published works in OR protocols; it uses the Expected Transmission Count (ETX) as a metric for candidate selection. More information regarding ETX metric, as well as EXOR protocol, will be discussed in Section 5.1.1. Similar to EXOR, Simple Opportunistic Adaptive Routing Protocol (SOAR) [6] uses the ETX metric for candidate selection. In SOAR, the shortest path between source and destination nodes is first calculated using the ETX metric. The set of candidates is then selected by adding nodes that are close to such a shortest path. Least-Cost Opportunistic Routing (LCOR) [7] is another well-known OR protocol that uses the Expected Any-Path Transmission (EAX) metric for candidate selection. EAX, as will be discussed in Section 5.1.4, has been developed considering the characteristics for OR protocols. The authors of LCOR have proven that this algorithm is capable of finding the optimum set of candidates by performing an analysis on a network topology graph. In Opportunistic Any-Path Forwarding (OAPF) [8], nodes are first forced to select an initial list of candidates using the ETX metric. Afterwards, the primarily selected nodes will choose their candidates. In the end, the source node completes the process of candidate selection using the EAX metric. Similar to LCOR, MTS, which stands for minimum transmission selection [9], proposes an

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004

optimum OR protocol using the EAX metric for candidate selection. More information regarding this protocol will be presented in Section 5.1.4.

Unlike previously described protocols, which consider only the quality of links between nodes for candidate selection, there are a category of other protocols that focus on the geographical location of nodes. In CBF [10], which was originally proposed as a routing algorithm for mobile ad-hoc networks, the source node initiates the routing process by locating its own location information, as well as that of the destination node, inside the data packet. Afterwards, the source node broadcasts such a packet, and neighboring nodes receiving this packet will forward it towards the destination, following the timer-based coordination method according to the distance to the destination as described in [1]. Similarly, POR [11] selects the candidate set by considering the amount of achievable distance progress through each candidate to the destination. However, in DPOR [12], a combination of link delivery probability between nodes and distance progress is used to define a metric for candidate selection. POR and DPOR algorithms will be investigated in greater detail in Sections 5.1.2 and 5.1.3. [13] introduced the concept of selecting and changing candidates according to their trust level in wireless networks. The authors introduced different metrics for candidate selection, considering different application requirements. On the other hand, [14] proposed an energy-efficient OR protocol customized for wireless sensor network environments, and [15] proposed an OR approach that consider quality of service, while routing packets towards their destination.

2.2. Security challenges in routing

Apart from reliability requirements, consideration of security measurements is also of great significance. To be more specific, even the most reliable routing algorithms will not be able to effectively operate in the presence of malicious nodes and attackers in the network. [16] and [17] provided reviews of security challenges in wireless sensor networks and mobile ad-hoc networks. Regarding security problems in a wireless network, plenty of research findings have considered cryptography solutions as a defensive mechanism against malicious nodes. Such techniques can guarantee the safety and integrity of data transmission between nodes. However, a separate category of misbehavior can be introduced when it comes to node collaboration in hop-by-hop routing. For example, some malicious nodes may introduce and inject false information in the network, or prevent collaboration with other nodes at the required time.

[17] indicated that the most detrimental routing attacks include impersonation, black-hole, gray-hole and worm-hole attacks. Impersonation reflects the situation in which the malicious node tries to contaminate the network using false identities [17]. However, in black-hole attack, which is a Denial of Service (DoS) attack, the adversary node tries to attract as many data packets as possible, and tends to discard all of the packets afterwards. In ad-hoc networks, black-hole nodes advertise false routing information, and try to convince other nodes in the network that they deserve to be selected as a next-hop node in routing. In a worm-hole attack, two malicious nodes located in different regions collude with each other and attack the network. Technically, once one of the malicious nodes receives a data packet, it sends such a packet to the other region through a private tunnel. The other malicious node will then replay the packet in the other area. In this simulation, such nodes are neighbors that are directly connected to one another, although in reality they are not [18]. In a gray-hole attack, which is a special variant of black-hole, nodes tend to selectively drop some of the received packets and forward others. In other words, the malicious node sometimes acts maliciously, and sometimes not. This makes it more difficult to recognize gray-hole nodes compared to black-hole ones [17].

2.3. Secure routing enhancements

In order to defend against routing attacks, however, different methods have been proposed in the literature. For example, trust and reputation management protocols have been developed with the purpose of recognizing uncooperative nodes in the network, and isolating them accordingly. CONFIDANT [19], CORE [20], [21], and [22] are some of the most important trust and reputation models that have been proposed that utilize direct/indirect interactions between nodes in a wireless network. Conversely, [23] introduced a trust calculation method for opportunistic networks that operates by sending Positive Feedback Messages (PFM). A PFM message is sent by a receiver node to acknowledge the cooperation of another node in an opportunistic network. Similarly, [24] and [25] proposed security enhancements in order to detect and isolate selfish or malicious nodes in an opportunistic networks. Furthermore, [26] proposed a trust-based algorithm for routing packets to their destination in a more reliable manner, taking into account nodes' energy considerations. [27], [28], and [29] presented surveys in the area of trust management systems in wireless networks.

To the best of our knowledge, there has not been enough work in the literature to investigate the security aspects of OR protocols. For example, it is interesting to study the effects of malicious nodes on an OR-based wireless network, and to evaluate how malicious nodes can affect different performance-related parameters. These considerations have motivated us to propose an analytical approach that models the behavior of malicious nodes in wireless mesh networks.

3. Applications of the proposed model

This section includes some of the most important scenarios in which the proposed model can be applied. To be more specific, the introduced approach is a general and comprehensive analytical model that can be utilized in order to assess the performance of any wireless sensor or mesh network in realistic situations. In fact, although the focus of this paper is to investigate the behavior of malicious nodes in OR protocols, the proposed model can be applied to simulate any hardware and software node failure that can occur in a wireless network. For example, in a WSN, nodes have a limited amount of energy, and will crash once their energy is completely consumed. In this scenario, dead nodes will have a similar role to malicious nodes in the proposed model, due to the fact that such nodes will not be cooperating in the packet forwarding process. On the other hand, as stated in [30] and [31], OR protocols outperform traditional routing protocols when it comes to network performance. Furthermore, traditional routing protocols for wireless networks can be considered as a special case of OR protocols, in which each node selects only one node as its next hop forwarder. Therefore, the introduced model can assist in a realistic study of any wireless network, including malicious behaviors or node failures. Some applications of the proposed model can be summarized as follows.

- **Highly sensitive networks:** As stated in [32] and [33], sensor networks have been widely used in highly sensitive situations such as military applications for detecting noise, light, chemicals, explosions, etc. in the area of interest. Consequently, for such mission critical situations, it is highly important to deploy a network that is effective and operational in hostile environments. For example, there is always a possibility that some of the sensor nodes in the battlefield become compromised or get destroyed. The proposed model in this paper is able to effectively simulate the existence of compromised/broken sensors in

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004

a military sensor network. More precisely, the proposed model can simulate the creation of any number of sensors, when a proportion of them is not functioning properly. This will create the possibility of evaluating the performance of such a network, and in the creation of a network that is tolerant to node failures, or misbehaviors in adversary environments.

- **Underwater networks:** Underwater sensor networks are a promising subsection of WSNs with the purpose of exploring and investigating the world beneath the water's surface [34]. However, due to the highly dynamic environment and unstable physical conditions, a suite of more reliable routing protocols must be designed and developed for underwater sensor networks. [35] indicated that OR protocols can be appropriate solutions for addressing the unreliability of such networks, as they can boost the reliability of communications in noisy and unstable environments. On the other hand, maintaining and providing technical support for underwater sensor networks is a considerably more complex task compared to regular sensor networks. Moreover, sensors are at high risk of getting damaged or lost in such environments. Therefore, investigating and studying the effects of malfunctions in such networks before the actual deployment can assist in a more sophisticated and realistic sensor deployment. The proposed model in this paper can effectively simulate the existence of node failures in underwater sensor networks. It should also be noticed that, using the introduced analytical model, the extraction of network parameters such as packet delivery ratio, drop ratio, hop count, etc. will be less computationally expensive, and more flexible than performing network simulations.
- **Environment monitoring/sensing applications:** As cited in [36] and [37], wireless sensor networks (WSNs) and Internet of Things (IoT) have been or will be widely used in many applications including, but not limited to, intelligent transportation systems, target tracking, manufacturing, wildlife monitoring, data gathering, healthcare systems, and so forth. In each of the mentioned applications, wireless nodes might fail to connect to other peers, or might be compromised. Therefore, considering that the proposed protocol in this paper is a general-purpose model that is applicable in any wireless sensor or mesh network, it can be used to evaluate the performance of such networks in realistic situations. This can not only help in performing risk management, but also in building a more reliable, secure, and fault tolerant network.

4. Modeling routing attacks using DTMC in OR protocols

This section describes the proposed model, in which an OR-based wireless mesh network containing malicious nodes is modeled using DTMC. As explained in [38], the hop-by-hop routing process of OR methods creates the possibility of modeling an OR-based wireless mesh network using DTMC, if the coordination method between candidates is perfect. In the following section, an overview of modeling OR protocols using DTMC is described, as presented in [38]. Afterwards, a complementary model is proposed in Section 4.1 which includes and models the effects of malicious nodes in OR protocols. Section 4.3 includes more details on how to calculate transition probabilities between states of DTMC in the proposed model. Finally, a novel method of calculating packet drop ratio by malicious nodes is proposed and calculated in 4.4.

4.1. Modeling OR using DTMC

As explained in Section 1, according to the link quality between the transmitting node in OR protocols and each of its candidates, some candidates may receive the mentioned packet; otherwise, the sending node tends to retransmit the packet a certain number of times if no candidates receive it. Assuming that a perfect coordination mechanism is applied between candidate nodes, and considering node priority in the candidate set, only one of the candidates will forward the packet, while others discard it. This process continues until the packet successfully reaches its destination, or gets discarded in a node after being retransmitted for the maximum number of times.

Routing operations in OR methods can be accurately modeled using DTMC, according to the characteristics described in the remainder of this section. First of all, DTMC is a memoryless system, meaning that reaching a specific state in DTMC is independent of past states. This situation applies to OR protocols in which packet arrival at any given time is independent of previous hops, and the current hop attempts to forward the packet to the next hop. Second, in DTMC the state of the system changes given probability values between different states. This is also applicable in OR protocols, where a probability value for each node in the candidate set determines whether each candidate will act as the relay node and will progress the packet. Finally, a DTMC with two absorbing states is basically similar to an OR protocol with two absorbing states. Such states can be considered as a *Success* state, which resembles successful delivery of the packet to its final destination, and a *Fail* state, which represents the situation in which a packet is discarded after a maximum number of retransmissions. For the purpose of modeling an OR protocol using DTMC, perfect coordination between candidate nodes should be applied. Furthermore, each state in the DTMC is defined using a tuple, which contains the node identifier and the number of occurred retransmissions in that specific node. The proposed model is valid for an OR containing any number of candidates or retransmissions, any topology, or any candidate selection algorithm, as described in [38].

4.2. A DTMC model for black-hole attack

Although the proposed model in [38] is a general model for assessing the performance of an OR-based mesh network, such a model is unable to represent realistic scenarios in which the network may contain uncooperative or malicious nodes. More specifically, there are numerous situations in which nodes do not participate in routing operations as expected. This may occur due to a hardware or software failure, malicious intentions, and so forth. In this section, we propose a modified model of an OR protocol that uses DTMC in the presence of uncooperative nodes. It should be emphasized that a node is considered uncooperative when, for any reason, it does not collaborate in routing operations according to the specification of an OR protocol. More specifically, it is possible to assign a probability value to a malicious node indicating its ratio of willingness to cooperate. In this paper, however, it is assumed that malicious nodes will always behave maliciously if they are supposed to take any action. Table 1 contains symbols and notations that are used throughout the entire paper.

The main idea of the proposed model in this paper is the existence of M malicious nodes in the network. In fact, the focus of the paper is on modeling black-hole attacks in the network. Similarly, it would be possible to generalize the model, to encompass any uncooperative behavior in which the malicious node is assigned with a probability value regarding its ratio of cooperation. As mentioned in Section 2.3, a black-hole node receives all of the data packets and drops them maliciously. Basically, when a node selects a black-hole node as one of its candidates, it expects the malicious candidate to forward received packets according to its priority in the candidate set. Surprisingly, however, the malicious node drops such packets and, following perfect coordination, sends an acknowledgment message to all other candidates indicating that it has already forwarded every single packet. Therefore, the previous

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004

Table 1
Notation and ymbols.

Symbol	Description
N	Number of nodes in the network
M	Number of malicious nodes
K	Maximum number of allowed retransmissions
C	Maximum number of candidates
$CS_{i,\ dest}$	Candidate set of node i for destination $dest$
S	Number of states in DTMC
P	Transition probability matrix
Q	Transition probability matrix between transient states
R	Transition probability matrix between transient and absorbing states
I	Transition probability matrix between absorbing states
Z	Transition probability matrix between absorbing and transient states
V	DTMC's initial state
F	Fundamental matrix of Markov process
ID	Node identifier
ReTx	Number of retransmissions taken place so far
(ID, ReTx)	A state in the DTMC
$p^{(i,j)}_{(i',j')}$	Transition probability between states (i, j) and (i', j')
c_i	The i_{th} priority candidate
$link_{prob}(x, y)$	Link delivery probability between nodes x and y

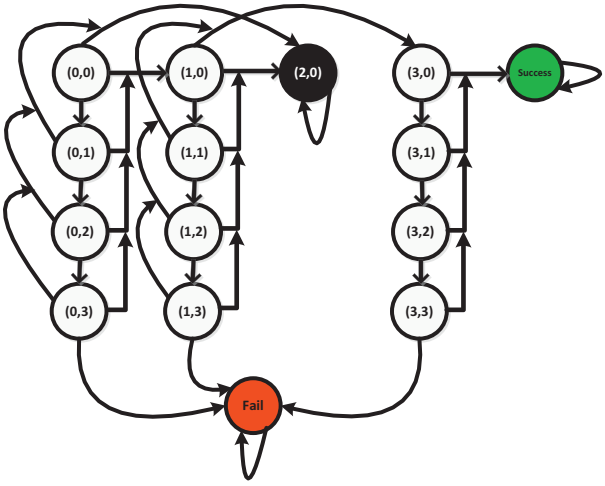

Fig. 1. An example of a DTMC for a linear topology in the presence of a black-hole node ($N = 5,\ M = 1,\ K = 3,\ C = 2$).

hop and all other candidates will prevent the forwarding of such packets, and they will be permanently lost.

In order to simply describe the proposed model, a linear topology is studied in which $N = 5,\ K = 3,\ M = 1,$ and $C = 2$. In this simple model, it is also assumed that the distance between all nodes is equal, and nodes with $(ID = 0)$ and $(ID = 4)$ are the source and the destination, respectively. In this scenario, it is also assumed that a node with $(ID = 2)$ is the only malicious node for following a black-hole attack. This scenario conveys that the malicious node will drop all of the received packets upon receiving them. Such nodes can therefore be modeled as absorbing states in DTMC. More specifically, once the system reaches an absorbing state, it will stay in that state, and no more transitions between states will occur. Therefore, as shown in Fig. 1, since the node with $(ID = 2)$ is a packet dropper, neither an attempt to forward the packet towards the destination nor a retransmission will take place once the system reaches state (2, 0). Considering this, as well as the existence of M malicious nodes, it would be possible to calculate the number of states in the system, say S, using Eq. (1).

$$S = (N - M - 1) \times (K + 1) + M + 2 \tag{1}$$

As shown in Eq. (1), the number of absorbing states will be equal to $M + 2$, corresponding to M number of malicious nodes, one *Fail*, and one *Success* state. Furthermore, the number of transient states in the proposed model would be $(N - M - 1) \times (K + 1)$. Finally, once all of the states in a DTMC are known, it would be possible to create a stochastic matrix containing the transition probabilities between states; using that matrix, we can extract required network parameters such as packet delivery ratio, drop ratio, etc.

The transition probability matrix P is an $S \times S$ matrix in the form of $P = \begin{bmatrix} Q & R \\ Z & I \end{bmatrix}$ which corresponds to the modeled DTMC in the presence of malicious nodes. This matrix is presented in canonical form in Fig. 2. As observed, P is composed of four different sub-matrices. Q, which demonstrates the probability of transitioning between transient states, is a matrix with $[(N - M - 1) \times (K + 1), (N - M - 1) \times (K + 1)]$ dimensions. Matrix R, which shows the probability of the transition from transient states to absorbing states, is a $[(N - M - 1) \times (K + 1), (M + 2)]$ matrix. The bottom-left corner of P, the Z matrix, is a $[(M + 2), (N - M - 1) \times (K + 1)$ matrix, and represents the probability of transitioning between absorbing and transient states. According to DTMC, logically this matrix is filled with all zero elements; the reason is that once the system is in an absorbing state, it remains in that state permanently, and no more transitions occur. Finally, I, which is an identity matrix of $[(M + 2), (M + 2)]$ dimensions, demonstrates transition probabilities between absorbing states.

In some network situations, particularly when the number of malicious nodes is significant and corresponds with the candidate selection algorithm, it is possible that all of the candidates for a specific node will be selected as malicious nodes. In this case, all of the packets being sent by the sending node will be maliciously dropped by all of the candidates. More specifically, the probability of reaching the destination node, represented as *Success* state in DTMC, will be zero. This is due to the fact that no path will exist between the source and the destination nodes. This scenario has been depicted in Fig. 3, in which all candidates of node 0, say nodes 1 and 2, are malicious nodes. In this scenario, regardless of the number of retransmissions by node 0, all of the sent packets will be captured and dropped by its candidates, and no packet will have the chance to arrive at its destination.

4.3. Calculating transition probability matrix

Once all states of the DTMC are recognized and the dimensions of each matrix is known, it should be possible to calculate the probability values of each element in P. As previously stated, the transition probability value between states (i, j) and (i', j') is defined as $p^{(i,j)}_{(i',j')}$ where i and i' represent node identifiers, whereas j and j' stand for the number of occurred retransmissions in each node. To obtain the probability values, different situations should be considered, as inspired by [38]. It should also be mentioned that all of the calculations are independent of any network topology, and are valid for any OR-based wireless mesh network, regardless of the number of candidates or retransmissions.

- **Reaching a state corresponding to the highest-priority candidate:** This case demonstrates the probability of transitioning to a state in DTMC that corresponds to the highest-priority candidate in the candidate set. For example, $p^{(0,0)}_{(2,0)}$ or $p^{(1,0)}_{(3,0)}$ in Fig. 1 is calculated following this rule. This probability value is basically equal to the link delivery probability between node i and its highest-priority candidate, say c_1, in the candidate set, as specified in Eq. (2).

$$p^{i,j}_{c_1,0} = link_{prob}(i, c_1) \tag{2}$$

$$\begin{bmatrix} \begin{bmatrix} p^{(0,0)}_{(0,0)} & \cdots & p^{(0,0)}_{(N-M-1,K)} \\ p^{(1,0)}_{(0,0)} & \cdots & p^{(1,0)}_{(N-M-1,K)} \\ \vdots & \ddots & \vdots \\ p^{(N-M-1,K)}_{(0,0)} & \cdots & p^{(N-M-1,K)}_{(N-M-1,K)} \end{bmatrix} & \begin{bmatrix} p^{(0,0)}_{BH_1} & \cdots & p^{(0,0)}_{BH_M} & p^{(0,0)}_{Fail} & p^{(0,0)}_{Dest} \\ p^{(1,0)}_{BH_1} & \cdots & p^{(1,0)}_{BH_M} & p^{(1,0)}_{Fail} & p^{(1,0)}_{Dest} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ p^{(N-M-1,K)}_{BH_1} & \cdots & p^{(N-M-1,K)}_{BH_M} & p^{(N-M-1,K)}_{Fail} & p^{(N-M-1,K)}_{Dest} \end{bmatrix} \\ \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \end{bmatrix}$$

Fig. 2. The transition probability matrix.

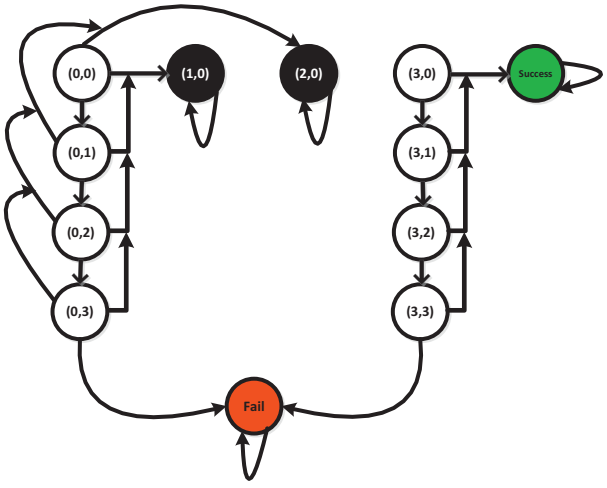

Fig. 3. The DTMC for a linear topology in the presence of two black-hole nodes ($N = 5$, $M = 2$, $K = 3$, $C = 2$).

- **Reaching a state corresponding to other candidates (except for the highest-priority candidate):** In this case, the transition occurs from state (i, j) to state (i', j') where i' is not the highest-priority candidate for node i. This can be calculated using the link delivery probability between nodes i and i', say $link_{prob}(i, i')$, given that none of the higher-priority candidates have already received the packet. The probability of this transition in the state machine can be calculated using Eq. (3).

$$p^{i,j}_{c_x,0} = link_{prob}(i, c_x) \times \prod_{t=1}^{x-1}(1 - link_{prob}(i, c_t)) \tag{3}$$

- **Reaching a state corresponding to a retransmission or the *Fail* state:** As described earlier, if no candidates receive a packet upon transmission, the sending node tends to perform a retransmission. This happens for a maximum of K retransmissions. After that, if no candidate receives the packet, it is permanently discarded from the network. Eq. (4) is designed to address the probability of retransmission or packet failure.

$$p^{i,j}_{i',j'} = 1 - \sum_{t=1}^{C} p^{i,j}_{c_t,0} \tag{4}$$

- **Reaching absorbing states:** Finally, in the process of different transitions, it would be possible for the system to reach one of the absorbing states. This is simulated as a situation in which the packet is discarded after K retransmissions, successfully reaches the final destination, or is grabbed by one of the malicious nodes in the network. All of the demonstrated cases are shown in the state machine using *Fail*, *Success* or $(ID, 0)$ where ID is the identifier of a malicious node. In this scenario, the system will stay in the mentioned state, and no other transition takes place between states. This results in the creation of an identity matrix, represented as I in the transition probability matrix P. Matrix I is created by setting $p^{i,0}_{i,0}$ to 1 where $(i, 0)$ shows an absorbing state.

4.4. Packet drop ratio calculation

After creating states in DTMC and calculating all probability values in transition probability matrix P, it will be possible to obtain different parameters in the network. [38] showed how to calculate different parameters, such as packet delivery ratio, expected number of transmissions, and hop-count. In our paper, a novel method for the calculation of another important parameter, known as *packet drop ratio*, is introduced. Packet drop ratio is defined as the number of packets received by uncooperative nodes and maliciously dropped. More precisely, packet drop ratio can be obtained by calculating the probability that each absorbing state corresponding to malicious nodes can be reached from an initial state, and subsequently combining them. Clearly, the initial state in OR protocols will be related to the source node, which generates data packets. Eq. (5) shows the initial state of an OR-based DTMC. The probability of reaching any state from the initial state V after multiple (h) number of transitions between states can then be calculated using P^h.

$$V = \begin{bmatrix} 1 & 0 & \ldots & 0 \end{bmatrix} \tag{5}$$

If we assume the existence of only one node as a source node in the network, say a node with $ID = 0$, it would be necessary to calculate the probability of reaching each absorbing state related to malicious nodes. For this purpose, considering the initial state of the system in Eq. (5), calculating $V \times P^h$ will result in the first row of the P^h. This can be used to determine the probability of reaching any absorbing state from the source node. More specifically, the element $(0, BH_1)$ in matrix $V \times P^h$ will represent the probability that the malicious node BH_1 will receive and drop the packet. Finally, Eq. (6) is used to calculate the overall ratio of packets being dropped by all of the malicious nodes. Similarly, as demonstrated in [38], it becomes possible to determine the probability of reaching *Success* or *Fail* states. Such values account for the probability of

reaching the destination, or failing a packet, respectively.

$$Drop\ Ratio = \sum_{i=1}^{M} Drop_{BH_i} \tag{6}$$

Alternatively, as shown in [38], required parameters can be obtained using the fundamental matrix F of the Markov process. Eq. (7) shows how to calculate F. In the end, by calculating $F \times R$, it would be possible to calculate the probability of reaching any absorbing state from any transient state.

$$F = (I - Q)^{-1} \tag{7}$$

5. Analysis

The proposed DTMC model, which takes into account the behavior of malicious nodes, must be evaluated. The model is independent of any OR algorithm; however, four well-known OR protocols, EXOR [5], POR [11], DPOR [12], and MTS [9] have been considered as case studies. A brief explanation of the behavior of each algorithm is presented in the following subsections. All of the mentioned algorithms are then evaluated under the effect of different network parameters, using both the proposed analytical model as well as the simulation. The proposed model has been implemented using Java programming language, while all simulations have been performed through Network Simulator 2 (NS 2.35) [39]. Having done so, it would be possible to perform the same set of experiments using the analytical model and simulation, and compare results accordingly.

5.1. OR case studies

As explained earlier, four famous OR protocols have been selected for performance evaluation. Out of these four algorithms, EXOR and MTS select candidates using link delivery probability between nodes, where MTS is proven to select the optimum candidate set in terms of expected number of transmissions (ETX). The other two algorithms, POR and DPOR, take the geographical location of nodes into account for candidate selection. This way, it would be possible to compare both categories of OR protocols.

5.1.1. EXOR algorithm

EXOR [5] uses the ETX metric for candidate selection. More specifically, ETX between nodes i and j is calculated considering the link delivery probability between such nodes following $ETX_{i,j} = \frac{1}{link_{prob}(i,j)}$ equation. First, EXOR tries to establish the shortest path between each node and its destination, then finds the first neighbor of each node as a potential candidate in this shortest path. Afterwards, if the ETX value from such a candidate to the destination is smaller when compared to the current node, this candidate will be added to the candidate set for the current node. This process is repeated until the maximum number of candidates is selected. Algorithm 1 provides greater detail on the method of candidate selection used by EXOR, following the work in [5].

5.1.2. POR algorithm

POR [11] is a simple OR protocol that selects the candidate set for each node by considering only their geographical location. To be more specific, each node in the network selects the neighbor resulting in the highest amount of distance progress towards the destination, and adds this neighbor to its set of candidates. This process continues until the maximum number of candidates has been selected, or the number of neighbors is too small to meet demands. The basic concept behind the POR algorithm is to decrease the number of hops required to send a packet, by selecting the next closest neighbors to the destination from each node. Algorithm 2 provides the pseudocode of the POR protocol, as explained in [11].

Algorithm 1 EXOR Protocol

```
1: procedure SELECT-CANDIDATES(node, dest, C)
2:     cost_node ← ETX_node,dest
3:     CS_node,dest ← ∅
4:     while (|CS_node,dest| < C) and exists(shortestPath(node, dest)) do
5:         path ← shortestPath(node, dest)
6:         cand ← getNeighgour(node, path)
7:         if equals(cand, dest) then
8:             add(CS_node,dest, dest)
9:             cost(dest) ← 0
10:        else
11:            cost(cand) ← ETX_cand,dest
12:            if cost(cand) < cost(node) then
13:                add(CS_node,dest, cand)
14:            end if
15:        end if
16:        removeEdge(node, cand);
17:    end while
18: end procedure
```

Algorithm 2 POR Protocol

```
1: procedure SELECT-CANDIDATES(node, dest, C)
2:     CS_node,dest ← ∅
3:     while (|CS_node,dest| < C) and notEmpty(neighbors(node)) do
4:         cand ← findBestNeighborByDistanceProgress(node)
5:         add(CS_node,dest, cand)
6:         removeEdge(node, cand)
7:     end while
8:     sortByDistanceProgress(CS_node,dest, node, dest)
9: end procedure
```

5.1.3. DPOR algorithm

Similar to POR, DPOR [12] benefits from the geographical location of nodes for its candidate selection. DPOR introduces a metric known as Expected Distance Progress (EDP), and attempts to establish a balance between the amount of achievable distance progress through each neighbor and the link delivery probability between them. In fact, DPOR suggests candidate selection not only on their ability to progress the packet towards the destination, but also on the quality of their links. More details regarding the candidate selection algorithm for DPOR can be found in Algorithm 3, according to [12].

5.1.4. MTS algorithm

MTS [9] is an OR algorithm that guarantees the selection of the optimum set of candidates in the context of the expected number of transmissions between source and destination. MTS uses EAX as a metric for candidate selection. [1] provided additional information on how to calculate the EAX metric. Basically, EAX is calculated recursively, considering multiple possible paths for reaching the destination in an OR-based wireless network. MTS initiates the process of candidate selection from the destination node's neighbors, adds the destination node to the candidate set of all such neighbors, and assigns the cost of each link using the EAX of each candidate to the destination. Subsequently, the algorithm iteratively finds the node with a minimum amount of EAX to the destination, for example bestNode, and adds bestNode and all of its candidates to the initial candidate set of all bestNode's neighbors. Finally, to determine the optimum candidate set, nodes are sorted in an increasing order using EAX value, and an exhaustive search is conducted to obtain the candidate set that includes less than or equal to C candidates. It was proved in [9] that this set contains an

Algorithm 3 DPOR Protocol

```
1: procedure SELECT-CANDIDATES(node, dest, C)
2:     candSetEDP ← −1
3:     neighbors ← getNeighbors(node)
4:     eligibleNeighbors ← ∅
5:     for all neighbor in neighbors do
6:         if distance_{neighbor,dest} < distance_{node,dest} then
7:             add(eligibleNeighbors, neighbor)
8:         end if
9:     end for
10:    sortByDistance(eligibleNeighbors)
11:    while (|CS_{node,dest}| < C) and notEmpty(eligibleNeighbors) do
12:        cand ← findBestNeighborByEDP(node)
13:        thisSet ← (CS_{node,dest} ⋃ cand)
14:        thisSetEDP ← EDP(thisSet)
15:        if thisSetEDP > candSetEDP then
16:            add(CS_{node,dest}, cand)
17:            candSetEDP ← thisSetEDP
18:            removeEdge(node, cand)
19:        end if
20:    end while
21:    sortByDistanceProgress(CS_{node,dest}, node, dest)
22: end procedure
```

optimum combination of candidates with regards to the expected number of transmissions (ETX). More details on the candidate selection method for MTS protocol is presented in Algorithm 4, following [9].

Algorithm 4 MTS Protocol

```
1: procedure SELECT-CANDIDATES(node, dest, C)
2:     cost_{node} ← 0
3:     nodes ← The set of all nodes except dest
4:     for all node in nodes do
5:         if isNeighbor(node, dest) then
6:             add(CS_{node,dest}, dest)
7:             cost(node) ← 1 / link_{prob}(node,dest)
8:         else
9:             CS_{node,dest} ← ∅
10:            cost(node) ← ∞
11:        end if
12:    end for
13:    while notEmpty(nodes) do
14:        currentNode ← minCost(nodes)
15:        removeNode(currentNode, nodes)
16:        neighbors ← getNeighbors(currentNode)
17:        for all neighbor in neighbors do
18:            add(CS_{neighbor,dest}, currentNode)
19:            for all c in CS_{currentNode,dest} do
20:                add(CS_{neighbor,dest}, c)
21:            end for
22:            cost(neighbor) ← EAX(CS_{neighbor,dest}, neighbor, dest)
23:        end for
24:    end while
25:    nodes ← The set of all nodes except dest
26:    sortByCost(nodes)
27:    for all node in nodes do
28:        CS_{node,dest} ← pickBestSetsByMaxSize(CS_{neighbor,dest}, C)
29:        cost(node) ← EAX(CS_{node,dest}, node, dest)
30:    end for
31: end procedure
```

Table 2
Propagation model parameters.

Parameter	Value
P_t	0.28183815 Watt
G_t, G_r, L	1
λ	$\frac{3\times10^8}{914\ MHz}$
RXThresh	3.652×10^{-10} Watt
β	2.7
σ_{dB}	6

5.2. Customized Black-hole attack

As explained in Section 2.2, black-hole nodes try to decrease network performance by attracting and dropping as many data packets as possible. In this section, a variation of the black-hole attack is introduced, after customization for OR protocols. In the proposed version, the malicious node not only tries to drop all of the received packets, but also prevents other candidates from progressing the packet. In fact, in conducted simulations, once the malicious node receives the packet, it informs all other candidates (as well as the previous-hop node) that it has already received and forwarded the packet. Following perfect coordination, other candidates and the previous hop then assume that the packet has already been transmitted, and they abstain from transmitting or retransmitting packets. The malicious node, however, drops the packet and removes it from the network.

5.3. Evaluation settings

Before presenting and exploring evaluation results, it is of significant importance to study network parameters and settings. For instance, in the modeling and simulation of wireless networks, it is important to select a realistic propagation model. In this paper, we have selected the shadowing propagation model, as it is possible to simulate the existence of noise in wireless channels with the use of this model, as explained in [39]. More details on related parameters for this model are presented in the following subsection, followed by a thorough list of network parameters.

5.3.1. Propagation model

As explained in Section 5.3, the shadowing propagation model is used in this paper for wireless communication between nodes, and the standard set of parameters is applied following [39], as shown in Table 2, to simulate communication between nodes in outdoor environments. Having used the shadowing propagation model, for every single transmitted packet it would be possible to calculate the power received from the signal, using Eq. (8) where d represents the distance, $P_r(d)$ shows the power received at distance d, P_t stands for the transmitted power, G_t accounts for the transmission antenna's gain, and G_r demonstrates the reception antenna's gain. Similarly, λ is the signal wavelength, β is the system loss, and X_{dB} stands for a Gaussian random variable with zero mean and standard deviation σ_{dB}. Finally, when a packet is transmitted, if the received power at the receiving node is greater than or equal to a threshold, say *RXThresh*, the node can successfully receive the packet. Therefore, it would be possible to calculate the delivery probability between nodes x and y at distance d using Eq. (9) as discussed in [12,39].

$$P_r(d)|dB = 10.log_{10}\left(\frac{P_t.G_t.G_r.\lambda^2}{L.(4\pi)^2.d^{\beta}}\right) + X_{dB} \tag{8}$$

$$link_{prob}(x,y) = Probability(P_r(d)|dB \geq 10\ log_{10}(RXThresh)) \tag{9}$$

Table 3
Simulation parameters.

Parameter	Value
Propagation model	Shadowing
MAC	802.11
Number of nodes (N)	40
Network field dimension	$500 \times 500\ m^2$
Number of malicious nodes	6
Maximum number of candidates (C)	3
Maximum number of retransmissions (K)	3
Data payload Size	512 bytes
Transmission rate	5 Packets/Second
Coordination delay	15 ms
Simulation time	1800 s

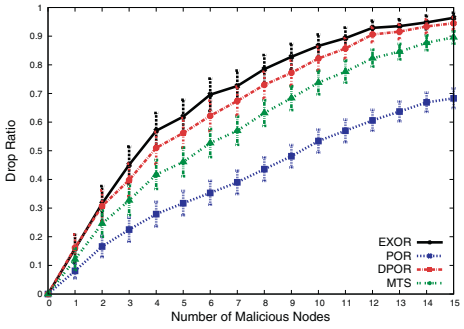

Fig. 4. Drop ratio.

5.3.2. Network parameters

Table 3 shows a list of all parameters being used in both analytical and simulation studies. In order to thoroughly study the effects of various parameters, three different parameters have been chosen for experiments including the number of malicious nodes, node density, and the maximum number of candidates (C). When all parameters are set to their default value, then changed one at a time, four different important network evaluation metrics are calculated and reported. These parameters include drop ratio, packet delivery ratio, expected number of transmissions, and hop count.

6. Results

As mentioned in Section 5.3.2, the results of performance evaluation for three different parameters are reported in this paper. For each parameter, evaluations for both analytical and simulation results have been conducted 100 times by randomly changing the network topology and reporting the average value of all executions, while considering a confidence interval of 95%. In addition, all graphs consist of four curves for EXOR, POR, DPOR, and MTS protocols. Finally, in order to prevent including very similar graphs in the paper, all plotted figures represent only the results of analytical studies, although the figures are significantly similar to simulation results. At the end of each subsection, however, the mean and the standard deviation of difference for each calculated parameter between analytical and simulation results is presented and explained.

6.1. Effect of malicious nodes

This section is presented to investigate the effects of the number of malicious nodes on different parameters. For this purpose, the number of malicious nodes changes from 0 to 15, where all other parameters are set to their default values listed in Table 3. As we will observe through all figures, malicious nodes can have significant and devastating effects on different network parameters.

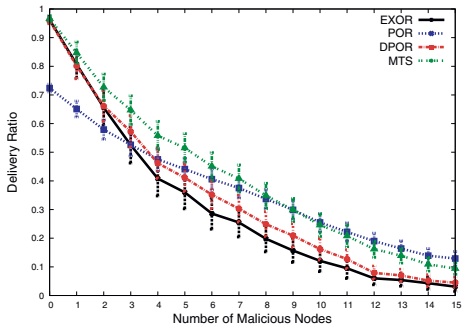

Fig. 5. Packet delivery ratio.

6.1.1. Drop ratio

Fig. 4 shows the packet drop ratio as a function of the number of malicious nodes. Drop ratio in analytical results has been calculated using Eq. (6). For simulation results, however, the drop ratio is calculated by dividing the overall number of dropped packets through malicious nodes by the total number of generated packets. Clearly, as the number of malicious nodes increases, the drop ratio rises as well. This change in ratio occurs because when there are more malicious nodes in the network, the probability of such nodes being selected as candidates in all of the protocols increases and, consequently, more malicious nodes will have the chance to attack the network by capturing data packets and dropping them accordingly. Amongst the four protocols, POR demonstrates the best performance when it comes to exposing packets to malicious nodes. The focus of POR algorithm is to minimize the number of hops for every packet. This indicates a reasonable decrease in the probability of packet receipt by malicious nodes. MTS, which focuses on optimizing the number of transmissions, ranks second. Here too, fewer overall transmissions indicate a smaller chance of capturing packets by malicious nodes, and consequently, a smaller drop ratio. Finally, DPOR outperforms EXOR through its consideration of nodes' geographical locations for candidate selection.

6.1.2. Delivery ratio

The delivery ratio of packets is calculated via the method explained in [38]. Basically, the delivery ratio in the analytical results is calculated as the probability of receiving the success state from the initial state. In simulations, however, the delivery ratio is the percentage of packets being received by the destination node, divided by the total number of generated packets. As observed in Fig. 5, increasing the number of malicious nodes will result in a decrease of the delivery ratio for all protocols. This is reasonable, as an increase in the number of malicious nodes will result in an increase in the number of packets being captured and dropped. This will clearly lead to a lower delivery ratio. When comparing different protocols, it is evident that MTS, which has an optimum candidate selection algorithm, possesses nearly the highest delivery ratio. As shown in the previous subsection, POR seems to be less affected by malicious nodes when compared to other protocols. The reason for its resiliency can be found in its candidate selection algorithm, which attempts to decrease the number of potential hops that can receive packets between the source and the destination. Similarly, DPOR outperforms EXOR in terms of packet delivery ratio.

6.1.3. Expected number of transmissions

Fig. 6 shows how a change in the number of malicious nodes can affect the expected number of transmissions (ETX). As observed, the ETX for MTS is reasonably the lowest value, when compared to other protocols. This behavior is predictable, because MTS has been proven to minimize ETX value. In contrast, EXOR has the

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004

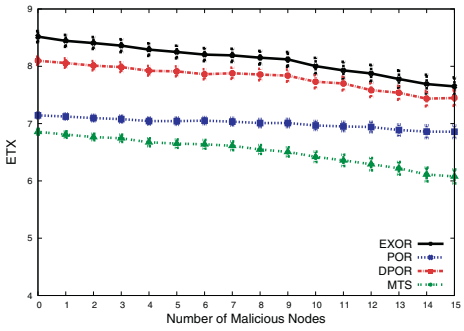

Fig. 6. Expected number of transmissions.

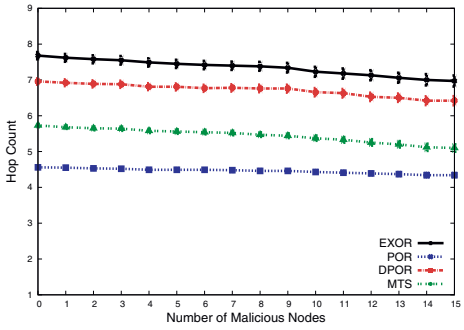

Fig. 7. Hop count.

worst ETX between all four protocols. POR, with its focus on minimizing hop count, outperforms DPOR. For all protocols, however, ETX value slightly decreases as the number of malicious nodes increases. The reason for this observation is that with the presence of a large number of malicious nodes in the network, a negligible proportion of packets will have an opportunity to arrive at their destination. Such packets demonstrate a rare situation, in that the route between the source and the destination is most likely clear of malicious nodes and, as shown later in this section, fewer hops are required to route such packets to their destination. A smaller hop count will result in fewer overall transmissions and retransmissions and, as a result, a lower value for ETX.

6.1.4. Hop count

Fig. 7 shows the effect of changing the number of malicious nodes in the hop count. As observed, by increasing the number of malicious nodes, the hop count decreases slightly for all protocols. As previously explained, this is because an increase in the number of attackers corresponds with a greater probability that such nodes may receive and drop data packets. In this scenario, a smaller number of hops between the source and the destination indicates a higher probability that packets will reach their destination, because the probability of having a malicious node in the path also decreases. When different algorithms are compared, POR displays the best hop count by considering the closest node to the destination as the best candidate, even though POR is incapable of delivering a large number of packets to their destination. MTS ranks second, with an optimal algorithm for candidate selection. DPOR is the third best algorithm, whereas EXOR ranks as the worst protocol in terms of the number of hops between source and destination.

6.1.5. Comparison of analytical and simulation results

This section is allocated for the comparison of conducted analytical results with simulation results. As observed in Table 4, two values have been reported for each evaluated parameter, which represent not only the average of the difference between all points

Table 4
Comparison of results for changing malicious nodes

Evaluated parameter	Measurement	EXOR	POR	DPOR	MTS
Drop ratio (%)	Average	0.0121	0.0175	0.0141	0.0286
	Deviation	0.0086	0.0097	0.0109	0.0125
Delivery ratio (%)	Average	0.0759	0.0025	0.0710	0.0026
	Deviation	0.0360	0.0021	0.0266	0.0020
ETX	Average	0.1809	0.0233	0.2192	0.0289
	Deviation	0.0323	0.0092	0.0339	0.0140
Hop count	Average	0.2643	0.0043	0.2512	0.0156
	Deviation	0.0467	0.0051	0.0398	0.0072

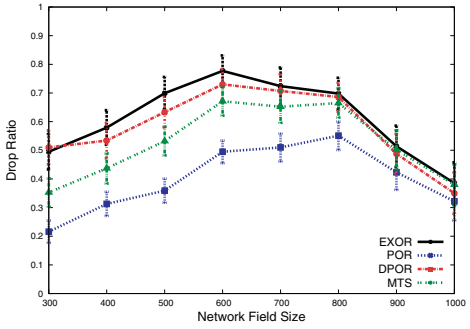

Fig. 8. Drop ratio.

in analytical and simulation results, but also their standard deviation. In fact, for drop ratio and delivery ratio, reported values demonstrate a percentage value, whereas absolute values are reported for ETX and hop count. As observed in Table 4, simulation results are, overall, very close to analytical results, which can be assumed as a verification for provided analytical results.

6.2. Effect of node density

This subsection studies the effects of changes in node density on different network parameters. For this evaluation, the dimensions of the network area will change from 300 × 300 to 1000 × 1000 m^2, while the number of malicious nodes is set to 6 nodes.

6.2.1. Drop ratio

Fig. 8 demonstrates the effect of changes in network size on packet drop ratio. As observed, by enlarging the field size, the drop ratio for all protocols increases to a certain level, and starts to decrease afterwards. This behavior is reasonable, since with a smaller network, say 300 × 300 m^2, the path between source and destination is shorter, and packets are not required to travel from many different hops to reach the destination. This decreases the probability that malicious nodes may receive data packets. In contrast, by enlarging the field size, more nodes will become involved in routing packets towards their destination. This offers greater opportunities for malicious nodes to capture more packets. However, when the network size is too large, say 1000 × 1000 m^2, the average distance between nodes will be reflective of that size; therefore, a great deal of packets will become lost in the network as a result of obstructions in the wireless channel. Therefore, although malicious nodes may still be selected as potential candidates by other nodes, fewer packets will successfully reach them, so they can discard less. A comparison of different protocols shows that POR is the most resistant protocol against malicious nodes, and EXOR ranks as the worst.

6.2.2. Delivery ratio

Fig. 9 shows packet delivery ratio as a function of changing the network field size. Reasonably, by increasing the network size,

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004

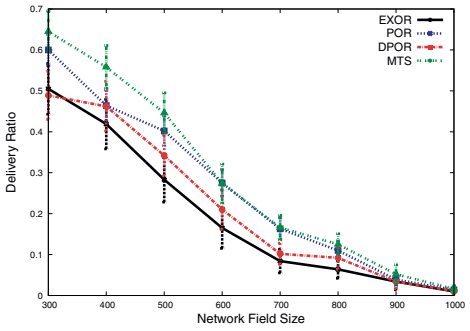

Fig. 9. Packet delivery ratio.

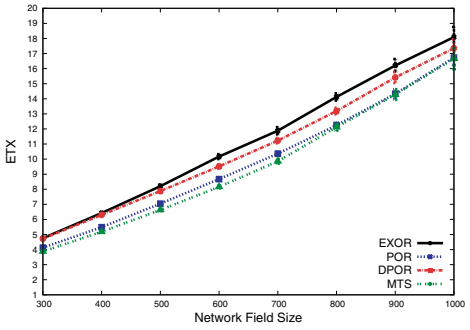

Fig. 10. Expected number of transmissions.

delivery ratio decreases. This occurs because, first of all, malicious nodes will be able to capture and drop some of the received data packets. Second, as the network size extends, the distance between nodes increases, and the probability of packet loss escalates for all different protocols. Therefore, fewer packets will have the opportunity to successfully reach the destination. A comparison of different protocols indicates that MTS acts as the best algorithm for packet delivery to the destination, whereas EXOR shows the worst delivery ratio. Interestingly, however, POR almost outperforms both EXOR and DPOR. The reason, as stated in the previous subsection, is that POR will try to decrease the number of necessary hops between the source and the destination. This results in a smaller probability of receiving packets to malicious nodes compared to DPOR and EXOR and, as a result, a higher delivery ratio. DPOR still outperforms EXOR by incorporating both link delivery probability between nodes, and their geographical information for candidate selection.

6.2.3. Expected number of transmissions

Fig. 10 shows the expected number of transmissions for all different protocols as a function of network field size. In all protocols, enlarging the network size results in an increase in distance between source and destination; as a result, packets will need to travel longer paths to reach their destination. Having longer paths means that packets must be transmitted or retransmitted more frequently in larger networks, compared to smaller ones. In this scenario, MTS, as expected, performs the best due to its optimum candidate selection scheme, and POR ranks second. DPOR and EXOR rank third and fourth, respectively.

6.2.4. Hop count

The hop count of packets sent between the source and the destination is shown in Fig. 11. As previously explained, a larger network area requires longer paths. Therefore, it is reasonable to have a higher hop count for larger networks. Taking the POR algorithm as an example, in a 300×300 m^2 field, packets must travel for less than 3 nodes to reach their destination, whereas in a 600×600 m^2

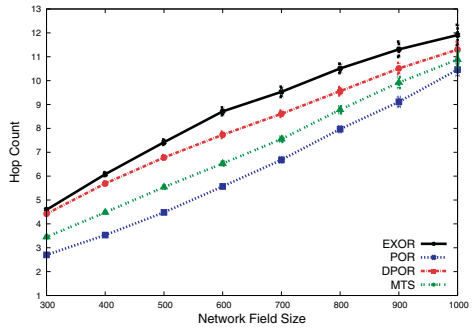

Fig. 11. Hop count.

Table 5
Comparison of results for changing node density.

Evaluated parameter	Measurement	EXOR	POR	DPOR	MTS
Drop ratio (%)	Average	0.0732	0.0686	0.0650	0.0808
	Deviation	0.0484	0.0602	0.0632	0.0615
Delivery ratio (%)	Average	0.0640	0.0018	0.0582	0.0025
	Deviation	0.0504	0.0012	0.0445	0.0017
ETX	Average	0.3535	0.0215	0.3084	0.0245
	Deviation	0.2344	0.0146	0.1550	0.0154
Hop count	Average	0.3812	0.0187	0.3137	0.0287
	Deviation	0.1872	0.0172	0.1147	0.0195

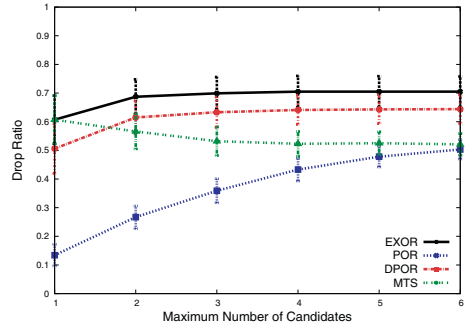

Fig. 12. Drop ratio.

field, the hop count is less than 6; and in a network with an area of 1000×1000 m^2, the value is less than 11. Comparing different protocols also represents a reasonable behavior in which POR has the lowest hop count, and EXOR has the highest. Similarly, MTS outperforms DPOR due to its candidate selection algorithm.

6.2.5. Comparison of analytical and simulation results

A comparison of simulation and analytical results following changes to node density is shown in Table 5. As observed, the average and standard deviation of changes show that simulation results are close to analytical ones. This conveys that changes to different network parameters follow the same trends for both sets of conducted results.

6.3. Effect of candidates

This subsection investigates the effect of the number of candidates on different network parameters. In this scenario, the maximum number of candidates changes from one to six nodes, while other parameters are set to their default values, as shown in Table 3.

6.3.1. Drop ratio

Fig. 12 shows the effect of candidate changes on the packet drop ratio. The change in the drop ratio for EXOR and DPOR

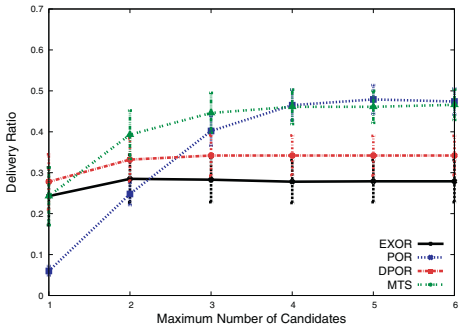

Fig. 13. Packet delivery ratio

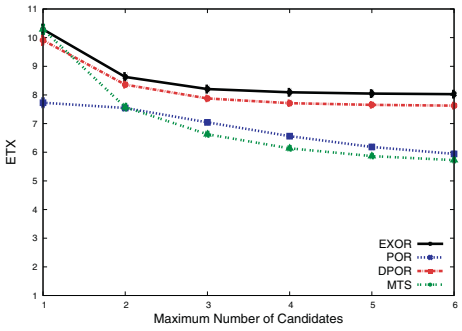

Fig. 14. Expected number of transmissions.

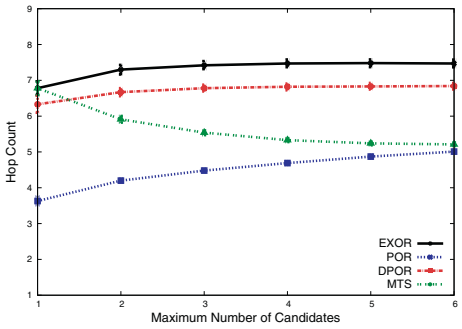

Fig. 15. Hop count.

appears insignificant when the number of candidates is more than two. More specifically, although the probability of a packet reaching its destination increases with the presence of more nodes in a candidate set, the probability also increases of a malicious node being included in the candidate set. POR, however, shows an interesting behavior; an increase in the number of malicious nodes leads to an increase in packet drop ratio for this protocol. This is because a small number of candidates, say one node, results in losing a large number of packets due to packet loss and fading in the propagation model. In fact, increasing the number of nodes in the candidate set decreases the chance of packet loss, while at the same time, increases the likelihood of selecting higher number of malicious candidates. This will lead to an increase in drop ratio. MTS reasonably shows results identical to EXOR when there is only one node in the candidate set. However, with more candidates, MTS' focus on best candidate selection shows a slight reduction until the number of candidates is 3, and the trend becomes almost constant thereafter. Overall, it can be concluded that EXOR has the highest drop ratio, whereas POR has the lowest value. Similarly, in MTS fewer packets can be captured by malicious nodes compared to DPOR.

6.3.2. Delivery ratio

Packet delivery ratio is shown in Fig. 13. In POR, as discussed earlier, the probability of packet loss decreases as the number of candidates is increased, while the algorithm still attempts to reduce the hop count by selecting nodes closest to the destination. Therefore, the reliability of sending packets to their destination increases, resulting in an increase in packet delivery ratio. MTS also shows a considerable rise in delivery ratio until the number of candidates is 3 nodes. After that, the trend of packet delivery ratio becomes almost constant, similar to EXOR and DPOR algorithms. Finally, effects of the candidate selection algorithm can be clearly compared between all protocols. Overall, MTS has been proven to function as the best algorithm. POR shows a poor delivery ratio when the maximum number of candidates is less than 3 nodes, and its performance increases with more nodes in the candidate set. Finally, DPOR has a higher delivery ratio compared to EXOR, which is achieved by incorporating geographical information with link delivery probability between nodes.

6.3.3. Expected number of transmissions

Fig. 14 shows the expected number of transmissions when the number of candidates is variable. For all protocols, the expected number of transmissions decreases as the number of candidates increases. This is reasonable because, as previously explained, having more candidates in the candidate set means that the probability of packet loss will decrease. Thus, packets will most likely either be captured and dropped by malicious nodes, or successfully sent to the next hop. In either case, the probability of retransmission decreases, and packets may experience fewer transmissions.

Table 6
Comparison of results for changing candidates.

Evaluated parameter	Measurement	EXOR	POR	DPOR	MTS
Drop ratio (%)	Average	0.0150	0.0180	0.0181	0.0233
	Deviation	0.0060	0.0133	0.0076	0.0147
Delivery ratio (%)	Average	0.1011	0.0040	0.0840	0.0051
	Deviation	0.0555	0.0036	0.0416	0.0078
ETX	Average	0.2132	0.0552	0.1819	0.0668
	Deviation	0.1314	0.0995	0.0958	0.1072
Hop count	Average	0.2833	0.0266	0.2350	0.0516
	Deviation	0.1676	0.0557	0.1275	0.0884

Here too, MTS shows the best ETX when more than one node exists in the candidate set whereas EXOR shows the worst value. Finally, DPOR demonstrates better performance than EXOR.

6.3.4. Hop count

The hop count of packets is represented in Fig. 15. As observed in POR, an increase in the number of candidates results in a slight corresponding increase in hop count. This is due to the fact that a smaller number of candidates leads to greater packet loss in POR; if some packets reach the destination, they have traveled from a very short path. As the number of candidates increases, however, more packets will reach the destination, but packets may need to travel from more hops. Nevertheless, POR still has the lowest hop count compared to other protocols, and EXOR shows the worst hop count. MTS reasonably ranks second, while DPOR operates better than EXOR but worse than MTS.

6.3.5. Comparison of analytical and simulation results

Finally, Table 6 shows the average and standard deviation of gaps between simulations as well as analytical results. The values on the table demonstrate that simulation results are very close to analytical results, which verifies the correctness of the proposed model and reported results.

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004

7. Conclusion

In this paper, the effects of malicious and uncooperative nodes were studied on opportunistic routing protocols in wireless mesh networks. More specifically, assuming that nodes in the candidate set follow perfect coordination, a new analytical model was designed and implemented using Discrete-Time Markov Chain (DTMC) to demonstrate the existence of malicious nodes. Additionally, in order to measure the effect of malicious nodes on the network, a new approach of calculating drop ratio was introduced. As an example of a malicious behavior, an implementation of a black-hole attack was introduced, after customization for opportunistic routing protocols. Finally, a comprehensive set of performance evaluation scenarios was designed and conducted, using both simulation and analytical studies on four well-known opportunistic routing protocols known as EXOR, POR, DPOR, and MTS. To summarize, evaluation results demonstrated that malicious nodes can significantly decrease the performance of wireless networks by preventing packets from reaching their destinations. Finally, by comparing results of simulations and analyses, we conclude that the proposed model is capable of demonstrating the effects of malicious nodes on opportunistic routing protocols. A possible direction for future works involves extending the proposed analytical model to include a defensive mechanism against malicious nodes, using a variation of trust and reputation systems.

Acknowledgment

This work is partially supported by NSERC, the Canada Research Chair program, ORF funds, and EAR Research Award.

References

[1] A. Boukerche, A. Darehshoorzadeh, Opportunistic routing in wireless networks: Models, algorithms, and classifications, ACM Comput. Surv. (CSUR) 47 (2) (2014) 22.
[2] A. Boukerche, B. Turgut, N. Aydin, M.Z. Ahmad, L. Bölöni, D. Turgut, Routing protocols in ad hoc networks: a survey, Comput. Netw. 55 (13) (2011) 3032–3080.
[3] F.-H. Tseng, L.-D. Chou, H.-C. Chao, A survey of black hole attacks in wireless mobile ad hoc networks, Human-centric Comput. Inform. Sci. 1 (1) (2011) 1–16.
[4] M. Salehi, A. Darehshoorzadeh, A. Boukerche, On the effect of black-hole attack on opportunistic routing protocols, in: Proceedings of the 12th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, PE-WASUN '15, ACM, New York, NY, USA, 2015, pp. 93–100.
[5] S. Biswas, R. Morris, Opportunistic routing in multi-hop wireless networks, ACM SIGCOMM Comput. Commun. Rev. 34 (1) (2004) 69–74.
[6] E. Rozner, J. Seshadri, Y. Mehta, L. Qiu, Soar: Simple opportunistic adaptive routing protocol for wireless mesh networks, Mob. Comput., IEEE Trans. 8 (12) (2009) 1622–1635.
[7] H. Dubois-Ferrière, M. Grossglauser, M. Vetterli, Valuable detours: Least-cost anypath routing, Netw., IEEE/ACM Trans. 19 (2) (2011) 333–346.
[8] Z. Zhong, J. Wang, S. Nelakuditi, G.-H. Lu, On selection of candidates for opportunistic anypath forwarding, ACM SIGMOBILE Mob. Comput. Commun. Rev. 10 (4) (2006) 1–2.
[9] Y. Li, W. Chen, Z.-L. Zhang, Optimal forwarder list selection in opportunistic routing, in: Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on, IEEE, 2009, pp. 670–675.
[10] H. Füßler, J. Widmer, M. Käsemann, M. Mauve, H. Hartenstein, Contention-based forwarding for mobile ad hoc networks, Ad Hoc Netw. 1 (4) (2003) 351–369.
[11] S. Yang, F. Zhong, C.K. Yeo, B.S. Lee, J. Boleng, Position based opportunistic routing for robust data delivery in manets, in: Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, IEEE, 2009, pp. 1–6.
[12] A. Darehshoorzadeh, L. Cerda-Alabern, Distance progress based opportunistic routing for wireless mesh networks, in: Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, IEEE, 2012, pp. 179–184.
[13] M. Salehi, A. Boukerche, A. Darehshoorzadeh, A. Mammeri, Towards a novel trust-based opportunistic routing protocol for wireless networks, Wirel. Netw. (2015) 1–17.
[14] E. Ghadimi, O. Landsiedel, P. Soldati, S. Duquennoy, M. Johansson, Opportunistic routing in low duty-cycle wireless sensor networks, ACM Trans. Sen. Netw. 10 (4) (2014) 67:1–67:39.
[15] L. Cheng, J. Niu, J. Cao, S.K. Das, Y. Gu, Qos aware geographic opportunistic routing in wireless sensor networks, Parallel and Distributed Systems, IEEE Transactions on 25 (7) (2014) 1864–1875.
[16] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, Security in wireless sensor networks, in: Handbook of Information and Communication Security, Springer, 2010, pp. 513–552.
[17] S. Agrawal, S. Jain, S. Sharma, A survey of routing attacks and security measures in mobile ad-hoc networks (2011). arXiv preprint arXiv:1105.5623.
[18] S. Ji, T. Chen, S. Zhong, Wormhole attack detection algorithms in wireless network coding systems, Mob. Comput., IEEE Trans. 14 (3) (2015) 660–674.
[19] S. Buchegger, J.-Y. Le Boudec, Performance analysis of the confidant protocol, in: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, ACM, 2002, pp. 226–236.
[20] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in: Advanced Communications and Multimedia Security, Springer, 2002, pp. 107–121.
[21] T. Ghosh, N. Pissinou, K. Makki, Towards designing a trusted routing solution in mobile ad hoc networks, Mob. Netw. Appl. 10 (6) (2005) 985–995.
[22] A. Boukerche, Y. Ren, R.W.N. Pazzi, An adaptive computational trust model for mobile ad hoc networks, in: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, ACM, 2009, pp. 191–195.
[23] N. Li, S.K. Das, A trust-based framework for data forwarding in opportunistic networks, Ad Hoc Netw. 11 (4) (2013) 1497–1509.
[24] R. Chen, F. Bao, M. Chang, J.-H. Cho, Dynamic trust management for delay tolerant networks and its application to secure routing, Parallel Distrib. Syst., IEEE Trans. 25 (5) (2014) 1200–1210.
[25] S. Gupta, S.K. Dhurandher, I. Woungang, A. Kumar, M.S. Obaidat, Trust-based security protocol against blackhole attacks in opportunistic networks, in: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2013, pp. 724–729.
[26] M.M. Mahmoud, X. Lin, X. Shen, et al., Secure and reliable routing protocols for heterogeneous multihop wireless networks, Parallel Distrib., IEEE Trans. 26 (4) (2015) 1140–1153.
[27] J.-H. Cho, A. Swami, R. Chen, A survey on trust management for mobile ad hoc networks, Commun. Surv. Tutorials, IEEE 13 (4) (2011) 562–583.
[28] H. Yu, Z. Shen, C. Miao, C. Leung, D. Niyato, A survey of trust and reputation management systems in wireless communications, Proc. IEEE 98 (10) (2010) 1755–1772.
[29] G. Han, J. Jiang, L. Shu, J. Niu, H.-C. Chao, Management and applications of trust in wireless sensor networks: a survey, J. Comput. Syst. Sci. 80 (3) (2014) 602–617.
[30] S. Biswas, R. Morris, Exor: opportunistic multi-hop routing for wireless networks, in: ACM SIGCOMM Computer Communication Review, vol. 35, ACM, 2005, pp. 133–144.
[31] Z. Zhao, B. Mosler, T. Braun, Performance evaluation of opportunistic routing protocols: A framework-based approach using omnet++, in: Proceedings of the 7th Latin American Networking Conference, ACM, 2012, pp. 28–35.
[32] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Comput. Netw. 38 (4) (2002) 393–422.
[33] M.P. Đurišić, Z. Tafa, G. Dimić, V. Milutinović, A survey of military applications of wireless sensor networks, in: Embedded Computing (MECO), 2012 Mediterranean Conference on, IEEE, 2012, pp. 196–199.
[34] I.F. Akyildiz, D. Pompili, T. Melodia, Underwater acoustic sensor networks: research challenges, Ad hoc netw. 3 (3) (2005) 257–279.
[35] L.F.M. Vieira, Performance and trade-offs of opportunistic routing in underwater networks, in: Wireless Communications and Networking Conference (WCNC), 2012 IEEE, IEEE, 2012, pp. 2911–2915.
[36] J.K. Hart, K. Martinez, Environmental sensor networks: a revolution in the earth system science? Earth-Sci. Rev. 78 (3) (2006) 177–191.
[37] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[38] A. Darehshoorzadeh, R. De Grande, A. Boukerche, Towards a comprehensive model for performance analysis of opportunistic routing in wireless mesh networks, Trans. Veh. Technol. PP (99) (2015) 1–15.
[39] K. Fall, K. Varadhan, The ns manual (formerly ns notes and documentation), VINT Project (2011) 1–193.

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004

Mr. Mahmood Salehi obtained his B.Sc. and M.Sc. degree in Computer Engineering (Software) in 2003 and 2006, respectively. After that, he served as a part-time lecturer at the Department of Computer Engineering, Islamic Azad University of Shahrekord, Iran from 2006 to 2009 and as a faculty member at Sama Department, Islamic Azad University of Karaj, Iran from 2009 through 2012. He is currently a Ph.D. candidate at the School of Electrical Engineering and Computer Science, University of Ottawa, Canada and studies under the supervision of Professor Azzedine Boukerche as a member of PARADISE research group. His main areas of research interest consist of opportunistic routing, trust management, security, and data gathering in wireless sensor/mesh networks and mobile/vehicular ad hoc networks.

Azzedine Boukerche (FIEEE, FEiC, FCAE, FAAAS) is a full professor and holds a Canada Research Chair position at the University of Ottawa (Ottawa). He is the founding director of the PARADISE Research Laboratory, School of Information Technology and Engineering (SITE), Ottawa. Prior to this, he held a faculty position at the University of North Texas, and he was a senior scientist at the Simulation Sciences Division, Metron Corp., San Diego. He was also employed as a faculty member in the School of Computer Science, McGill University, and taught at the Polytechnic of Montreal. He spent a year at the JPL/NASA-California Institute of Technology, where he contributed to a project centered about the specification and verification of the software used to control interplanetary spacecraft operated by JPL/NASA Laboratory. His current research interests include wireless ad hoc, vehicular, and sensor networks, mobile and pervasive computing, wireless multimedia, QoS service provisioning, performance evaluation and modeling of large-scale distributed systems, distributed computing, large-scale distributed interactive simulation, and parallel discrete-event simulation. He has published several research papers in these areas. He served as a guest editor for the Journal of Parallel and Distributed Computing (special issue for routing for mobile ad hoc, special issue for wireless communication and mobile computing, and special issue for mobile ad hoc networking and computing), ACM/Kluwer Wireless Networks, ACM/Kluwer Mobile Networks Applications, and Journal of Wireless Communication and Mobile Computing. He has been serving as an Associate Editor of ACM Computing Surveys, IEEE Transactions on Parallel and Distributed systems, IEEE Transactions on Vehicular Technology, Elsevier Ad Hoc Networks, Wiley International Journal of Wireless Communication and Mobile Computing, Wiley's Security and Communication Network Journal, Elsevier Pervasive and Mobile Computing Journal, IEEE Wireless Communication Magazine, Elsevier's Journal of Parallel and Distributed Computing, and SCS Transactions on Simulation. He was the recipient of the Best Research Paper Award at IEEE/ACM PADS 1997, ACM MobiWac 2006, ICC 2008, ICC 2009 and IWCMC 2009, and the recipient of the Third National Award for Telecommunication Software in 1999 for his work on a distributed security systems on mobile phone operations. He has been nominated for the Best Paper Award at the IEEE/ACM PADS 1999 and ACM MSWiM 2001. He is a recipient of an Ontario Early Research Excellence Award (previously known as Premier of Ontario Research Excellence Award), Ontario Distinguished Researcher Award, Glinski Research Excellence Award, IEEE CS Golden Core Award, IEEE Canada Gotlieb Medal Award, IEEE ComSoc Expectional Leadership Award, IEEE TCPP Exceptional Leadership Award. He is a co-founder of the QShine International Conference on Quality of Service for Wireless/Wired Heterogeneous Networks (QShine 2004). He served as the general chair for the Eighth ACM/IEEE Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, and the Ninth ACM/IEEE Symposium on Distributed Simulation and Real-Time Application (DS–RT), the program chair for the ACM Workshop on QoS and Security for Wireless and Mobile Networks, ACM/IFIPS Europar 2002 Conference, IEEE/SCS Annual Simulation Symposium (ANNS 2002), ACM WWW 2002, IEEE MWCN 2002, IEEE/ACM MASCOTS 2002, IEEE Wireless Local Networks WLN 03–04; IEEE WMAN 04–05, and ACM MSWiM 98–99, and a TPC member of numerous IEEE and ACM sponsored conferences. He served as the vice general chair for the Third IEEE Distributed Computing for Sensor Networks (DCOSS) Conference in 2007, as the program co-chair for GLOBECOM 2007–2008 Symposium on Wireless Ad Hoc and Sensor Networks, and for the 14th IEEE ISCC 2009 Symposium on Computer and Communication Symposium, and as the finance chair for ACM Multimedia 2008. He also serves as a Steering Committee chair for the ACM Modeling, Analysis and Simulation for Wireless and Mobile Systems Conference, the ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, and IEEE/ACM DS–RT.

Dr. Amir Darehshoorzadeh is a Research Scientist at the PARADISE Lab at University of Ottawa. He received his Ph.D. in 2012 with Prof. Cum Laude from the Technical University of Catalonia (UPC), Barcelona, Spain. He received his M.Sc. Degree from Iran University of Science and Technology (IUST), Tehran, Iran in 2006. His main current research areas are Opportunistic Routing, Modeling and Network optimization, Wireless Networks including VANETs, MANETs, WSNs, Multicast protocols and QoS provision. He has extensively published research papers in international conferences and journals and presented several lectures in mentioned areas.

Please cite this article as: M. Salehi et al., Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.07.004