Defenses Against Packet Dropping Attacks in Wireless Multihop Ad Hoc Networks

L. Sánchez-Casado, R. Magán-Carrión, P. García-Teodoro, J.E. Díaz-Verdejo
Dpt. of Signal Theory, Telematics and Communications
Faculty of Computer Science and Telecommunications - CITIC
University of Granada, 18071- Granada, Spain
{sancale,rmagan,pgteodor,jedv}@ugr.es

***Abstract*:** Wireless multihop ad hoc networks are vulnerable to several specific security threats. In particular, a number of papers exist in the literature where *sinkhole, blackhole, grayhole* and *selfish* attacks are studied for this kind of networks. All of these malicious behaviors can be grouped into a general class known as *packet dropping* attacks and constitute a serious risk for communications, services and users. This paper provides a complete overview on the abovementioned packet discarding related security threats for multihop ad hoc networks, the most known security approaches being organized and discussed according to the defense line they are intended to cover: prevention, detection or response. Additionally, to clarify the efforts and proposals made until now by the community, open challenges and new trends in this field are also pointed out. In summary, the present paper constitutes a relevant contribution for interested researchers to better understand packet dropping related defenses in wireless multihop ad hoc networks.

***Keywords*:** Ad hoc networks; Defense line; Malicious behavior; Multihop transmission; Packet dropping; Security attack/threat.

1. Introduction

Ad hoc networks constitute a technology of increasing use in certain areas, such as environmental and military applications, disaster management, etc. This fact is mainly motivated by some particular characteristics of these networks, which are among others: geographical distribution without a fixed infrastructure, self-configuration capability, and wireless-based communications. It is also remarkable for these environments that the nodes in the network with no direct communication among them can communicate each other through other nodes. This is the so-called *multihop* transmission strategy.

As wireless multihop ad hoc networks proliferate, many security issues associated with this communication paradigm become more relevant and thus need to be conveniently addressed. In this line, Table 1 shows some principal security threats reported for this kind of environments [1] [2] [3]. Among them, there are several attacks where a malicious node, after introducing itself in some way in the origin-destination routes (multihop path), controls communications and alters transmissions by discarding packets. This kind of well-known attacks generally includes *sinkhole*, *blackhole*, *grayhole* and *selfish*.

Sinkhole attacks are usually referred to misbehaving nodes that try to introduce themselves in the routing/forwarding path to seize communications. To do so, a malicious node modifies routing messages either by publishing that it has the shortest path to the destination or by spoofing the destination address to guarantee that the sender chooses it as an intermediate hop. Blackhole and grayhole attacks are two of the most popular attacks in multihop ad hoc networks. Both are related with the packet forwarding process carried out by intermediate nodes. When the node completely drops all the received packets, the attack is considered a blackhole attack. Instead, the grayhole attack is caused by a node dropping packets in a selective way, *e.g.*, one out of N packets received, one packet every certain time, only packets corresponding to specific flows, etc. On the other hand, selfish nodes evade their responsibility on forwarding packets in the network with the principal aim of preserving or economizing its energetic resources.

All of the abovementioned attacks can be grouped into a generic type named *packet dropping attack*, which constitutes a major security concern in current wireless multihop ad hoc networks [4] [5]. As mentioned, nodes exhibiting this behavior maliciously drop received data or routing messages instead of

Attack	Description
Physical layer	
Eavesdropping	Listening to private communications, *i.e.*, intercepting data
Jamming (random, periodic, …)	Generating signal interferences, which provokes communication disruption
Link layer	
Collision	Generating selective interferences to disrupt MAC mechanisms, which affects the capture of a channel for legitimate transmissions
Exhaustion	Repeated collisions and/or continuous retransmissions to occupy the channel
Sleep deprivation, *a.k.a.* Resource consumption	Repeated collisions that induce the node to continuous retransmissions, thus causing its death
Network layer	
Blackhole	Sending fake routing information that claims an optimum route to make other nodes relay data packets through the malicious node. In a second step, this node could drop or discard traffic
Delay	Introducing time delays in the retransmission of control packets, thus disrupting the normal routing operations
Grayhole, *a.k.a.* Selective forwarding	Blackhole attack where the node drops packets selectively, *e.g.*, with a certain probability, one packet every certain time, or only packets corresponding to specific flows
HELLO flooding	Massive sending of HELLO packets to overwhelm neighbors
Link spoofing	Advertising fake links with non-neighbors, thus disrupting routing operations
Link withholding	Ignoring a link advertisement, which can result in node isolation
Link-broken error	Sending fake control messages, which gives rise to connectivity loss
Routing cache poisoning	Faking routing table information, thus disrupting the routing function
Routing table overflow	Advertising an excessive number of routes to non-existing nodes, which prevents neighbors from creating new legitimate routes
Rushing	Artificial quick retransmission of routing packets, which can result in building fake routes
Selfish	Bypassing certain protocols rules to save resources (*e.g.*, battery), which decreases network performance
Sinkhole	Sending fake routing information that claims an optimum route to make other nodes route data packets through the malicious node to inspect and filter the traffic in some way
Wormhole	Two colluding attackers record packets at one location and replay them at another using a private high speed link
Other layers or any of them	
Jellyfish	Introducing time delays to TCP retransmissions, which decreases end-to-end performance
Sybil	Adopting multiple identities, *e.g.*, becoming a legitimate part of the network
Tampering	Physically manipulating a node to affect some functionality or compromise it

Table 1. Some principal attacks reported in the literature for wireless multihop ad hoc networks.

forwarding them, which in fact disrupt the normal operation of the network [6]. Though the specific damage caused by packet dropping attacks depends on the discarding level implemented in each case (*e.g.*, indiscriminate *vs.* selective dropping, or actual malicious behavior *vs.* "just" saving resources-related selfish behavior), its potential impact and relevance in communications is unquestionable. This way, huge efforts are carried out by the research community to address this problem, the number of proposals in the specialized literature in this line being continuously increasing.

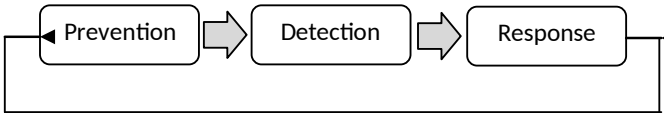

Figure 1. Defenses lines in a traditional defense in-depth approach.

However, some limitations can be checked for almost the totality of the contributions in the field. First, most of the published papers deal with only a partial aspect of the problem. On the one hand, some of them are limited to a particular type of data discarding (*i.e.*, blackhole or sinkhole or grayhole or selfish) instead of studying all of them as a global typology. On the other hand, the majority of the papers are only focused either on preventing or detecting or reacting against these malicious behaviors, while they avoid the rest of possible defense lines.

Another relevant shortcoming that usually affects works on multihop ad hoc security is the existence of bit confusion in specifications. Thus, both the definition and scope of each particular attack and the type of defense lines specifically developed in each case are wrong or at least mixed up, in occasions.

In summary, the great majority of current proposals are interesting but partial and, conversely, incomplete, when not slightly confusing. This paper tries to solve these limitations by presenting a general survey on defenses against packet dropping attacks with the following main characteristics:

1. As previously stated in the previous paragraphs and through Table 1, each specific attack (sinkhole/blackhole/grayhole/selfish) is clearly defined and differentiated from the rest.
2. Despite this difference, especially regarding the research works we can find in the literature, we propose to group all of them as belonging to a common class, *packet dropping*, with similar final consequences on network performance.
3. A detailed state-of-the-art covering the most relevant proposals existent in the literature to fight against this kind of attacks is afterwards presented. Aimed at providing an organized vision of the subject, the study is carried out based on the specific defense line considered in each case. Despite some other organizations can be alternatively performed for that (*e.g.*, network layer or protocol affected), we consider the traditional defense in-depth approach a good option (see Figure 1).
4. Finally, new trends and open challenges in the field of wireless multihop ad hoc security are discussed with the aim of completing as much as possible the information about the topic.

According to these principal contributions, and once the motivation of the paper has been clarified along this first section, the rest of the paper is structured as follows. Section 2 presents the main works related with the development of prevention techniques against packet dropping attacks. Among others, cryptographic and credit-based algorithms are the most widely used prevention schemes at present [7]. In Section 3 current detection proposals are discussed, which usually rely on observing the occurrence of misbehaviors and intrusion events in the monitored environment. Section 4 is devoted to analyze response/reaction related security approaches, which are basically oriented to isolate the malicious nodes to preserve the operation of the network and services. In some cases, the reaction schemes are aimed at serving as a feedback mechanism to strengthen the network by adapting the considered security mechanisms to the particular conditions observed, as shown in Figure 1. After that, Section 5 brings new trends and open challenges in the topic of multihop ad hoc security in general, and for packet dropping attacks in particular. Finally, the paper concludes with a summary of the main aspects contributed.

2. Preventing packet dropping related attacks

A first concern quickly arises regarding the prevention of packet dropping attacks when reviewing the literature. It is directly related to the concept of prevention itself. In a strict sense, only mechanisms or

methods avoiding the potential attacks should be considered preventive. But there are many authors that label their approach as preventive despite they are based on a detection phase. In this sense, these algorithms should be included either in the detection or the reaction category. Therefore, all these methods will be described later in Section 3 or 4. On the other hand, there exist approaches which explicitly encourage the nodes not to misbehave, although they do not neglect the possibility of dropping attacks. We will consider these approaches as preventive, as there is no detection or reaction mechanism involved. Anyway, it is a difficult task to label many of the approaches that will be described later as belonging to a single category, as they can mix various techniques from different categories.

According to [8], a wireless multihop ad hoc network should "*1) provide an effective security mechanism to deal with misbehaving nodes in the network, 2) encourage co-operation among nodes in the network …*". Therefore, for the purposes of this paper, we will consider as preventive mechanisms those not allowing or discouraging misbehaving nodes. In this context, four main categories of mechanisms can be identified according to the main method used for the prevention scheme: authentication-based, based on changes in the routing protocol, reputation-based and credit-based systems. They are described in the next.

2.1. Authentication-based prevention schemes

The methods in this category usually provide for preventive schemes to protect the routing procedure, that is, to guarantee the correctness of the announced routes, mainly based on key management or encryption techniques, by checking the identity of the nodes involved in communications. Therefore, they are primarily targeted at the prevention of unauthorized nodes from joining the network, which constitutes a defense against external attacks.

Most of the techniques in this category are based on authenticated routing. Some examples of this kind of methods are Ariadne [9] and ARAN [10]. Ariadne uses an end-to-end authentication based on shared key pairs, while ARAN uses a hop-by-hop authentication.

These techniques are suitable to prevent foreigner nodes from being able to disrupt the network operation through fake route announcements and, consequently, are able to avoid subsequent packet dropping attacks. However, most of them fail in its preventive behavior if the attacker is an insider. On the other hand, the use of ciphering constitutes a drawback from the point of view of energy saving and performance, even if a trusted authority is not required.

2.2. Prevention based on routing protocol modification

Most of the routing protocols for multihop ad hoc networks, especially in the case of MANETs (Mobile Ad hoc NETworks), have not been designed with security requirements in mind. Therefore, a method for the prevention of dropping attacks is the introduction of changes in the used protocol to fix the vulnerabilities that make the attacks possible. In this sense, multipath routing can be considered as a first kind of prevention, as the objective is to support a secure and reliable communication in case a route is compromised. Nevertheless, other approaches which use additional exchanges of information among nodes are described in the literature.

Although in some cases the changes include the use of ciphering, it is worth to mention that the primary goal is not to guarantee the identity of the nodes involved in the communication, but to guarantee the freshness and correctness of the communication routes between nodes. This way, there exist many proposals in the literature based on the cross-checking of the routes by comparison with the neighbors' ones or by explicitly requesting the final or intermediate nodes to confirm them or to send additional information about the routes. An example of the later is the case of SAODV [11] [12], which is an extension of AODV to counter for dropping attacks. It is based on the use of new SRREQ and SRREP packets with a secret code each time a RREP packet is received. When the source node receives at least two SRREP packets, it chooses the shortest path as a secure path to the destination. Another similar procedure is that introduced in [13], which verifies the security of the path after receiving a RREP packet by sending back the next hop information within the RREP. Alternatively, the proposal in [14], also aimed at preventing the blackhole attack, uses CREQ and CREP packets to confirm the route validity by explicit comparison with neighbors' routes.

An alternative approach is based on somehow enforcing the cooperation of the nodes through the introduction of new mechanisms in the protocol. This way, OMH (One More Hop) [15] uses asymmetric keys to cipher the packets in such a way that only the next node to a node in the route knows whether the destination of the packet is the previous node or not. Thus, every node receiving a packet needs to forward it in order to be informed by the next node about the keys required to decipher the content, in case it is the final node.

The main disadvantage of this family of solutions is the increased cost in terms of the number of packets required and the higher number of nodes involved in the communication. On the other hand, some of them use encryption, which is an additional drawback.

2.3. Reputation-based prevention schemes

Reputation-based prevention methods monitor the nodes' behavior during the operation of the network in order to assign them a reputation or trust level. Only nodes with an adequate level of reputation will be considered during the routing of packets. According to [16], "*Reputation of an agent is a perception regarding its behavior norms, which is held by other agents, based on experiences and observation of its past actions*". Therefore, in order to assign the reputation level, two main components are required: a model for the normal or proper behavior of the nodes when forwarding packets, and a way to observe, measure and store the reputation value.

An additional question arises for this kind of procedures. Although in many of them there is no explicit detection of misbehaving nodes, the reputation level of a node can be used as an indicator of its proper behavior and, therefore, it would be straight to label them as attackers. And, having into account that the un-trusted nodes will be avoided during the forwarding process of the packets, the procedure can also be somehow considered as a response scheme. Nevertheless, we have included this category in the prevention phase as some of the proposed systems limit their operation to only include proven trustable nodes in route selection algorithms, which does not imply the other nodes to be misbehaving.

Thus, one of the first proposals using reputation was the Pathrater algorithm [17], which encourages nodes to forward packets to increase its rating. Nevertheless, it is clearly based upon detecting misbehaving nodes by using the Watchdog method. Therefore it will be detailed in next sections.

Some solutions make use of a trusted authority for storing the reputation of each other, while others adopt a decentralized management approach and introduce a recommendation protocol to exchange trust related information. As an example, in CORE [18] each node keeps track a reputation table through the observation of neighbors' behavior and the exchange of information with the nodes involved in each operation. When a request to relay a packet arrives at a node, it is forwarded only if the requester has a positive reputation value. A similar approach is the so-called Friend and Foes proposed in [19], which is based on the society principle stating that people agree to cooperate in a duty as long as they notice there is a fair tasks distribution in the group. To build an opinion for a node, each participating node advertises its set of friends and foes, that is, the set of nodes to whom it is / it is not willing to forward packets. Another decentralized approach is SORI [20], where the nodes exchange reputation information only with their neighbors.

A hybrid approach using reputation is that in [21], where a routing protocol is proposed to combat the blackhole attack that includes a trust-based method where the sender takes opinion of the neighbors which replied with a RREP packet.

2.4. Credit-based prevention schemes

In credit-based approaches each node receives a micro-payment for its cooperation in forwarding network messages, while it also pays those nodes retransmitting its messages [22]. Two models can be applied: the message purse model and the message trade model [23]. In the message purse case it is the source node who pays the intermediate nodes for their service in forwarding packets. Therefore, a node should have enough

credits to start a new transmission. On the contrary, in the message trade case, the messages are considered as merchandise and, consequently, it is the receiver who pays the sender and the intermediate nodes. Both approaches suffer from the same problem, which is related with handling credits. Thus, to avoid cheating, secure payments have to be deployed and a proof of the effective forwarding of the packets is required. This usually involves a central trusted authority, which is usually impractical in multihop ad hoc networks.

The simplest credit-based method is TFT (Tit-for-tat) [24], in which two neighbor nodes exchange the same amount of messages. This method distinguishes between two types of messages: primary and secondary. Primary messages are those in which the node is directly interested, that is, the node is the origin or the destination of the message. Secondary messages are those in which the node is not interested. The key idea is to involve the nodes in the forwarding of the secondary messages in order to earn credits for the transmission or reception of primary messages. This method does not require any credit accounting or trusted authority, but it is only valid in delay tolerant networks, as the messages should wait in the queue till the nodes have enough credits.

Sprite [25] is a cheat-proof credit-based proposal that uses digital signatures for any single transaction. There exists a central trusted authority, the Credit Clearance Service, which is responsible for the accounting of the credits. Apart from the need of this central authority, the main limitation is the use of signatures, as they are costly operations and had to be done by every forwarding node.

An improvement over Sprite, named Express, is described in [22]. It is based on the substitution of the signatures by hash chains, which reduces the processing costs for the nodes.

Mobicent [26] is a more recent typical credit-based solution in which a virtual bank performs the charging and rewarding processes. The credit charged to a node for sending a packet is equally distributed to the intermediate nodes.

The credit-based systems do really incentive the cooperation of nodes in the forwarding process in order to earn credits for their own transmissions, which is especially relevant to avoid selfish behaviors. But they require a trusted party to avoid cheating on the credits and can be unfair if not all the nodes send a similar amount of information.

3. Detection of dropping attacks in wireless multihop ad hoc networks

Despite the great efforts carried out by the research community to propose preventive solutions for the dropping problem, it is still necessary to perform a subsequent detection procedure, as shown in Figure 1. Thus, a big number of approaches have been proposed in the literature to handle packet dropping in wireless multihop ad hoc networks [4]. In the next, we classify them into two main categories according to their basic operation: ACK-based and intrusion detection related.

3.1. ACK-based schemes

In this category, nodes request an explicit acknowledgment from their neighbors to confirm the success on the reception of the packets they send.

A two-hop ACK-based scheme is proposed in [27], where each node asks its two-hop neighbors for an ACK packet to detect misbehaving nodes. As the next hop is able to send a forged ACK packet back on behalf of the intended two-hop neighbor, an authentication mechanism is used. In order to reduce the overhead involved, the authors propose in [28] each node to ask its two-hop neighbors randomly instead of continuously. However, these two schemes fail when any two-hop neighbor refuses to send back an ACK. In such a situation, the requester node is unable to determine who the malicious node is.

To overcome the previous ambiguity in detecting malicious nodes, Liu et al. [29] propose TWOACK to detect malicious links instead. The main idea is to send two-hop acknowledgment packets in the opposite

direction of the routing path. In this scheme, each sender maintains a list of data packets sent out but not yet acknowledged, a counter of the forwarded data packets and a counter of the missed packets. Also, to reduce the incurred routing overhead, authors in [30] present an improvement of their scheme by proposing 2ACK, where only a fraction of the packets are acknowledged according to the value of an *acknowledgement ratio*.

In [31] a modification of the AODV protocol is introduced to detect multiple blackholes in the group. The scheme uses a table which provides a given fidelity level to every participating node. When the destination correctly receives a data packet, it will send an acknowledgement to the source and, therefore, the fidelity level of the intermediate nodes will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented. If the fidelity value of a given node reaches zero value, it will be labeled as malicious. The main drawback of this solution is the processing delay introduced in the network.

The authors in [32] complete their previous works in [27] and [28] by suggesting a modular solution which employs two-hop cryptographic acknowledgments for unicast packets, while a passive feedback mechanism to monitor broadcast packets is also employed. The gathered information is afterwards used as the basis for an accusation-based collaborative mechanism to detect dropping attacks.

The main idea of [33] is using Merkle tree, a binary tree in which each leaf carries a given value and the value of an interior leaf (including the root) is a one-way hash function of the leaf's children values. For detecting single and cooperative blackhole attacks, each node contains a hash which is a combination of its own identity and a secret value that only the node knows. Then, each node in the path acknowledges the reception of the message to the source, which constructs a Merkle tree whose leaves are the acknowledgments and calculates the root value y^r. Thereafter, y^r is compared with a pre-computed value y^p, obtained during an initialization process generally corresponding to the route discovery mechanism. If they are equal, the path is secure against droppers. Because of the huge overhead implied, authors propose two versions: Total Acknowledgment (TA), acceptable if we are dealing with important data; and Random Acknowledgment (RA), which generates a relatively small overhead but providing no guarantee, and which may be used with less important data.

3.2. Intrusion detection related schemes

Intrusion detection techniques have been recurrently used in the literature to deal with the potential occurrence of non-legitimate events in a communication environment (either host or network related) [34]. Consequently, several intrusion detection systems have been proposed to determine the potential existence of droppers in wireless multihop ad hoc environments. Based on the approach followed to perform the intrusion detection process, the next works are grouped into different classes.

Some techniques simply monitor the target environment, comparing the value of the collected features with a given threshold, which could be adaptive or not. As previously discussed, Marti et al. [17] presented in their pioneering work Watchdog and Pathrather. Watchdog uses a monitor node which saves the recently sent packets by itself and compares them with the overheard packets forwarded by the next hop. If a sent packet does not match longer than a timeout, a failure tally is incremented for the next hop. If the tally exceeds a given threshold, the node is determined to be malicious. In [35] Kurosawa et al. deal with blackhole attacks in MANETs by introducing an anomaly detection scheme which makes use of a dynamic training method. They consider the number of RREQ packets sent and RREP packets received, as well as the average of the differences between the destination sequence numbers sent in RREQ packets and the ones received in RREP packets, to express the state of the network. Thus, this training set of features is employed to calculate the detection threshold based on the normal state of the network, which is dynamically updated at regular time intervals to improve the detection accuracy. For the detection process, every sample in the data set is compared with the threshold to detect deviations from the normal network state. In [36] the authors propose a solution called DPRAODV to counter blackhole attacks, in which the node receiving a RREP message from an intermediate node checks whether the sequence number value exceeds a given threshold. To reduce inaccuracies which can lead to false alarms, this threshold value is dynamically updated at every time interval. If the sequence number is higher than the threshold, the intermediate node is suspected to be malicious and is added to a blacklist.

Other approaches carry out some sort of matching techniques. For instance, IDAD (Intrusion Detection based on Anomaly Detection) [37] is a host-based IDS solution to detect both single and multiple blackholes. This scheme compares every activity of a host with a pre-collected set of anomaly and attack activities, called *audit data*. The parameters used as audit data are a set of entries obtained from each anomaly RREP packet: destination sequence number, hop count, route lifetime, destination IP address and timestamp. This way, the IDAD system is able to differentiate normal from abnormal RREP packets just by checking if the received RREP resembles one of those listed in the audit data. In such a case, the given node will be concluded to be malicious.

Supervised/unsupervised machine learning approaches are applied in many proposals to perform the detection process. Zhang et al., in [38], introduce a local and cooperative scheme in which each mobile node runs a SVM-based IDS agent that monitors local traces, collecting data like user and system activities or communications within the radio range. Also, each agent is responsible for detecting, locally and independently, signs of intrusions. However, if an anomaly is detected among the local data, or if an evidence is inconclusive and needs further investigation, neighboring IDS agents will collaboratively investigate in a broader range, participating in the cooperative and global detection procedure which is launched. A cross-feature method is described in [39], where a total of 141 traffic and topology related features are defined. This method also executes a data mining analysis to extract correlations and interrelations between features, in order to reduce this space of features. Then, a classifier like C4.5, RIPPER or Naïve-Bayes is used to carry out the anomaly detection procedure. The authors in [40] introduce a multi-layer approach composed of three different subsystems that use a Bayesian classifier, Markov chains and an association rule algorithm for intrusion detection in MAC, routing and application layers, respectively. The results from the three layers are integrated into a local module, and the final result is sent to a global module. CRADS [41] combines the use of a nonlinear SVM-based detector and some data reduction techniques to decrease the size of the feature set, thus minimizing the learning overhead. In a similar line, the authors in [42] use a linear classification algorithm, namely Fisher Discriminant Analysis (FDA), to remove data with low-information content, making the SVM classifier feasible for ad hoc nodes.

Additionally, some schemes make use of reputation methods to establish, in a cooperative way, a confidence level for each node which allows the detection process. In [43], the CONFIDANT protocol tries to detect malicious nodes. A *monitor module* supervises, through a passive-feedback technique, the behavior of its first-hop neighbors. If a suspicious event is detected, details are passed to a *reputation module*, which manages a table containing the rating for all the known nodes. Depending on how significant and how frequent the event is, the rating can be updated and the node labeled as malicious. The use of a *trust manager* and a *path manager* modules will be lately discussed in the response section. In the aforementioned Friend and Foes approach [19], each node performs the detection through a passive-feedback technique and by maintaining *credits* for each other, indicating the number of packets forwarded by other nodes. Then, the node classifies the rest in three categories periodically updated: friends, for which the node accepts to relay packets; foes, for which no service is provided; and selfish, corresponding to those that consider the node as a foe. The concept of *inner-circle consistence* was adopted in [44] to identify and detect forged route replies. The idea is to let each node discover its *k*-hop neighborhood. All its neighbors form its inner-circle, responsible for voting malicious outgoing data from the node. Specifically, route replies need to get approval from its inner-circle, which verifies the validity of the messages. If a reply contains false routing information to attract packets, an attack is detected through a voting process performed by each inner-circle node.

Finally, some works extract an analytical model for representing the dynamics of a given protocol, detecting inconsistencies during its operation. In [6], the authors obtain the Extended Finite State Automaton (EFSA) for the AODV routing protocol, modeling its normal state and proposing both specification-based and statistical-based detection. The first approach detects anomalous events which are direct violations of the specifications defined by EFSA. Thus, the attackers can be detected by monitoring some particular transitions. In anomaly detection, a set of statistical features based on anomalous events associated with different attacks is defined, as well as another set which defines the normal state. Then, a rule-based classifier (RIPPER) is used to process these sets and to generate a collection of detection rules useful to detect these attacks. The authors in [45] propose a theoretical model for the different causes of packet loss, detecting dropping attacks in DSR-based networks and distinguishing these attacks from other legitimate circumstances, like collisions or channel errors. However, a very limited topology is studied there, and no mobility aspects are considered.

This needs more investigation indeed. In [5], a heuristic is proposed to complete the model in [45] to properly deal with mobility scenarios which cause legitimate packet drops when a node moves out of the communication range. These reasons can cause a large number of false positives if not properly treated. For that, some features from MAC and routing layers are considered. As a result of such multi-layer approach, much better detection efficiency is obtained than that raised in the referred paper.

4. Response schemes against packet dropping attacks

As commented before, a large amount of proposals exist in the literature which deal with packet dropping attacks. They are mainly related to prevention and detection security defense lines. Although these security lines are needed, they are not sufficient to avoid the consequences due to the potential apparition of attack events. Therefore, a reaction defense line is recommended to mitigate such undesired consequences (Figure 1). Prevention (resistance), detection (recognition) and response (recovery) defense lines strengthen thus the target system and contribute to its *survivability*, which is defined as *"the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures or accidents"* [46].

Most of the ad hoc networks security solutions are focused on prevention and detection techniques, while others response-based mechanisms are less often. The current reaction related approaches are generally intended to isolate or elude misbehaving nodes in order to preserve the network operation and performance [47].

Even though it is not an easy task to provide a definitive classification for response mechanisms, we tentatively propose the following types, groups or classes: node exclusion, node exclusion and announcement, and node isolation.

4.1. Node exclusion

This type of reaction techniques are aimed at eluding the misbehaving node in such a way that it is avoided as an intermediate node in multihop origin-destination routes. These reaction schemes present two main features. First, only the nodes that belong to the malicious node neighborhood are aware of the misbehavior occurrence. Second, and as a subsequent action of the previous fact, the neighbors will try to elude those routes to which the malicious node belongs.

Although trust-based management systems are widely used as prevention and detection techniques, they are also considered as response mechanisms. Thus, a security extension of DSR routing protocol is introduced in [48]. A Hidden Markov Model (HMM) for each node is in charge of computing the node's trustworthiness, which can be considered *"a quantitative value of trust that indicates the probability that a node will behave as expected"* [49]. Trust-based secure MANET routing using HMMs (TSR) acts against selfish behaviors by the selection of the route whose nodes have higher trustworthiness values. This way, the misbehaving node will be eluded. In [50] the DSR MANET routing protocol is modified by attaching two agents to each network node: a MOnitoring Agent (MOA) and a ROuting Agent (ROA). The first one monitors the network node behavior to assign a trust value. When a malicious node is detected its assigned trust value is decreased. Afterwards, the ROA agent selects a trustworthy route discarding nodes with less trust level.

Other existing mechanisms use the information provided by a reputation system to trigger the response.. The authors in [20] introduce SORI, a secure and objective reputation-based incentive scheme. SORI discourages selfish behaviors by discarding, with a certain probability, the packets generated by a selfish node. This way, a smaller reputation value causes a higher discarding probability, which limits over the time the transmission capability of the selfish node. More recently, in [51] a reputation-based routing algorithm is proposed as a response mechanism. In this case the future trustworthiness of each node is evaluated by means of a dynamic prediction algorithm that takes into account its historical behavior. Similarly to [48], when a node begins its malicious activities the system reduces the associated trustworthiness, so that no more packets are sent to or from this node when a fixed threshold is surpassed. This proposal has a particularity: the malicious node can be recovered as a benign node. Hence, the system is acting now as a tolerance method as

it tries to maintain the node in the network to avoid disconnections that would negatively affect the network performance.

Other systems make use of simpler thresholds to execute the response procedure are also proposed in the literature. For example, in [52] the malicious node is blocked at the source node routing table when the RREP sequence number has a high value. In [53], during the route establishment phase, each node creates a legitimacy table whose entries, one per node in the network, are calculated using two factors: the number of times that the entry node has been chosen as an intermediate node, and the number of times the destination node has been really reached through such intermediate node. When a malicious behavior is detected the legitimacy value for the corresponding node is decreased. Afterwards, the nodes with higher legitimacy value will be chosen as intermediate nodes in the route, which in fact results in confining the malign node.

4.2. Node exclusion and announcement

These response mechanisms improve the previous ones by notifying the existence of the malicious node/s to the rest of the network by means of different messages. Then, any node is able to discard the misbehaving node as a routing intermediary, making the response action more global than in the previous case.

A reputation-based trust management is described in [54] (an ulterior work to [43]). Here, the response action is carried out cooperatively between a reputation manager module, a trust manager module and a path manager module. Once a suspected event is detected for a node, it is passed to the reputation manager in order to evaluate the historical behavior of the node. If a threshold is exceeded, a notification is passed to the path manager, which will remove this node from the route. Additionally, an ALARM message is sent by the trust manager to the neighborhood. Every ALARM message received in a node is passed to the trust manager module to determinate if the associated node has been evaluated in the same way by other trusted nodes. If so, that is, if there exist sufficient evidences about the malignity of the node, it is notified to the reputation module for the malicious node be discarded as a routing alternative.

In [55] a response mechanism is taken in one of two ways: directly or indirectly. In the first case, each node is in charge of removing a detected malicious node from its routing table. On the contrary, in the second case a monitor node will send an alarm message to the neighborhood. Depending of the amount of alarm messages received at a given node, this will remove the misbehaving node from its routing table.

The authors in [56] introduce a blocking related response mechanism. There exists a set of agents monitoring the network with communication capabilities with each other. This way, when a malicious node is detected, the subsequent response action is launched. First, a blocking message in sent to the associated nodes of the agent who discovered the attack. Moreover, this blocking message is disseminated among the rest of the agents for the misbehaving node being eluded from the network.

In [57] a modified DSR routing protocol is presented. A blackhole node is eluded by means of the creation of a blacklist of nodes and its dissemination throughout the network. Therefore, all nodes know who is a blackhole and they won't process any packet from it. In the Friend and Foes algorithm introduced in [19] two lists of nodes are broadcasted by each node. The first one is the set of nodes to whom we are willing to forward packets and the second one is the set of nodes which we are not willing to forward packets. Thus, a benign node will refuse a control packet from a selfish node, which will force to the establishment of an alternative path.

In [58] the intermediate nodes react by discarding RREP packets from a given node if the sequence number exceeds a fixed threshold. This value is calculated with the sequence number stored in the routing table of the intermediate node, the sequence number of the incoming RREP packet and the number of RREPs received. Also, the malicious node identification is disseminated to the others nodes by adding the malicious node information into the RREP message.

4.3. Node isolation

Schemes intended to actively isolate the misbehaving node are introduced here. In this class of response mechanisms, a misbehaving node is besieged or surrounded by others which are in charge of blocking the incoming and outgoing communications of the former. Therefore, not a mere "passive" exclusion of the node out of the routing paths is performed.

A cross-layer mechanism is provided in [59] for that purpose. Although the attack occurs at the routing layer, the reaction is performed at the physical layer by means of the creation of a radio quarantine zone around the attacker. Nodes into the quarantine zone won't be able to send or receive packets. This is aided by a positioning system, which provides the locations of the nodes over the time.

Reaction techniques based on the inclusion of autonomous agents, are now described. In [60] the authors introduce a scheme imitating the human immune system. There exists an Immune Agent (IA) distributed along the network. The IA is in charge of detecting, classifying, isolating, and recovering the system from the attack (the last action is only performed if needed). A given node is isolated from the rest of the network when it has carried out a certain number of attacks. Moreover, the isolated node can be recovered as a benign node when it is not longer a threat for the environment. A similar scheme is proposed in [61], where there exist two types of agents in the system: detection agents and counterattack agents. When a threat is detected, an activation message is first broadcasted to the counterattack agents. Only the counterattack agents belonging to the neighborhood of the attacker node are going to be activated. Afterwards, they will block any packet from and to the misbehaving node. In [62] an ad hoc network is partitioned in clusters, where a Cluster Head (CH) supervises the corresponding nodes in each cluster. When the CH detects a malicious node, an Action Agent (AA) is created, cloned and positioned in each neighbor. Afterwards, each AA checks if the malicious node is one-hop located. If it is so, the AA remains in the neighbor node; otherwise, it is auto-cloned and positioned in the neighborhood. This operation is repeated until the misbehaving node is surrounded. The next step can be diverse: to isolate the malicious node from the network, to remove the node from the routing tables, to block traffic from and towards the malicious node, to reduce the trust level of this node to avoid its incorporation in valid routes, etc.

5. New trends and open challenges in wireless multihop ad hoc networks security

We have shown the existence of a vast literature and a number of associated proposals on wireless multihop ad hoc networks security. However, despite such big efforts, it is still necessary to empower current technologies and boost new approaches if we want to improve system performance and users' confidence in this kind of environments. New trends and several challenges should be remarked in this line in the following. They all are beyond the trivial recommendation of improving both current prevention, detection and response schemes.

Some authors defend the necessity of designing new protocols and procedures to reinforce traditional security aspects such as that of authentication. This way, more robust routing protocols and collaborative procedures to strengthen reliability are being developed, *e.g.*, [63] [64] [65]. Although these mechanisms can be used in a dynamic way in a number of tasks (access control, trust and reputation, etc.), they all are usually related with a prevention perspective of security. In other words, the continuous apparition of new attacks concludes to the evident necessity of improving the initial security conditions considered for a target network.

Moreover, as new types of attacks and variants appear, it is also required to have more powerful and reliable detection schemes at our disposal. The usual response given by the community for this is the development of more specialized detection approaches. This diversification or specialization in detection gives way to two main consequences. On the one hand, it provides a better performance in terms of detection figures. On the other hand, however, this leads to a significant increase in detection cost as the number of attacks and variants we want to be able to detect is broadened. To avoid this inconvenient while not affecting the detection accuracy, we defend the convenience of developing holistic detection schemes. This way, the construction of semantic models will help us implementing novel detection paradigms that surpass attack particularities to provide with more global detection capabilities.

Also, as new attacks and variants appear, it is also recommended to devise new reaction schemes for guaranteeing the continuity and survivability of the monitored communications system. Opposite to current response schemes, which are generally performed locally, novel global reaction schemes based on the collaboration of the whole network are desirable. Otherwise, the response could be useless. For example, if a packet dropper is isolated and prohibited to participate in communications by a group of neighbor nodes, the malicious node could avoid the restriction by simply moving to a different area of the network.

Another challenge and recommendation from our point of view is to design and implement integral defense mechanisms. That is, to mix together prevention, detection and reaction mechanisms in such a dynamic way that the security system acts as a whole instead of the mere sum of the parts. In other words, it is desirable the dynamic unsupervised adaptation of the system. This global adaptation must converge to stable and optimal solutions, which in fact have to be carefully controlled by the defense system itself. In other words, every functional element must be conveniently interrelated with the rest to provide with global solutions. For example, as a new attack instance is detected, it is evaluated in terms of its risk before triggering the adequate response/s and, if necessary, new prevention schemes may be carried out to protect our environment. Additionally, the model used in the detection process can be dynamically re-estimated and thus, adapted to the conditions of the network over the time.

One of the main consequences of the abovementioned research lines is the necessity of intra- as well as inter-node collaboration. However, this implies a new level of complexity and, as a consequence, a higher consumption of physical and logical resources. Since the disposal of such resources (*i.e.*, battery and disk space) is restricted in some new devices, environments and applications, a trade-off between security and cost is mandatory. In this line, the deployment of holistic approaches for resource consumption saving when dealing with the different security mechanisms is highly recommended. This trade-off between security and cost is also relevant from the point of view of the impact on the quality of service (QoS) of the communications. In consequence, some of the current proposals existing in the literature are not valid from a practical perspective because they obviate resource consumption and/or their real impact on network performance. This, in fact, implies developing alternative schemes and methods.

6. Summary

This work constitutes a global survey on packet dropping security threats for wireless multihop ad hoc networks. Beginning with the existence of several attacks reported in the literature with a similar objective of dropping packets, and sometimes a bit confusing in their final purposes, the paper provides a detailed state-of-the-art on different approaches based on the defense lines deployed to fight against this kind of attacks. Thus, both prevention, detection and reaction schemes developed in the literature during the last years are subsequently described here to organize the knowledge existing in the field. Moreover, new trends and open challenges are also highlighted in order to point out what would constitute the near future in the target topic.

In summary, the paper contributes a complete study of the packet discarding behavior problem in wireless multihop ad hoc networks, which is of high interest for the research community to improve security, and thus service providing, in this kind of (more and more accepted) environments. This work will actively help researchers to better understand packet dropping related security attacks in multihop ad hoc networks.

Acknowledgment

This work has been partially supported by the Spanish MICINN through project TEC2011-22579.

References

[1] D. Martins, H. Guyenne, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey," *Proc. 13th International Conference on Network-Based Information Systems (NBiS)*, pp. 313–320, 2010.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," *IEEE Wireless Communications*, vol. 14, n. 5, pp. 85–91, 2007.

[3] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," *Chapter 12 in "Wireless/Mobile Nerwork Security"*, *Springer*, 2006.

[4] S. Djahel, F. Nait-Abdesselam, Z. Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 13, n. 4, pp. 658–672, 2011.

[5] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, "An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs," *Proc. 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), pp. 231–238, 2012.

[6] Y. Huang, W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," *Proc. 7th International Symposium on Recent Advances in Intrusion Detection 2004 (RAID)*, pp. 125–145, 2004.

[7] A. El-Mousa, A. Suyyagh, "Ad Hoc Networks Security Challenges," *Proc. 7th International Multi-Conference on Systems, Signals and Devices (SSD)*, pp. 1–6, 2010.

[8] R. Raghuvanshi, R. Kaushik, J. Singhai, "A Review of Misbehaviour Detection and Avoidance Scheme in Adhoc Network," *Proc. International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, pp. 301–306, 2011.

[9] Y. Hu, A. Perrig, B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proc. 8th Annual International Conference on Mobile Computing and Networking (MOBICOM)*, pp. 12–23, 2002.

[10] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," *Proc. 10th IEEE International Conference on Network Protocol (ICNP)*, pp. 1–10, 2002.

[11] S. Lu, L. Li, K. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," *Proc. 5th International Conference on Computational Intelligence and Security (CIS)*, pp. 421–425, 2009.

[12] D. Cerri, A. Ghioni, "Securing AODV: the A-SAODV Secure Routing Protocol," *IEEE Communications Magazine*, vol. 46, n. 2, pp. 120–125, 2008.

[13] H. Deng, W. Li, D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," *IEEE Communication Magazin*e, vol. 40, n. 10, pp. 70–75, 2002.

[14] S. Lee, B. Han, M. Shin, "Robust Routing in Wireless Ad-Hoc Networks," *Proc. 31st International Conference on Parallel Processing Workshops (ICPPW)*, pp. 73–78, 2002.

[15] C. Song, Q. Zhang, "OMH-Suppressing Selfish Behavior in Ad hoc Networks with One More Hop," *Mobile Network Applications*, vol. 14, n. 2, pp. 178–187, 2009.

[16] J. Liu, V. Issarny, "Enhanced Reputation Mechanism for Mobile Ad Hoc Networks," *Trust Management, Lecture Notes in Computer Science*, vol. 2995, pp. 48–62, 2004.

[17] S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. 6th Annual International Conference on Mobile Computing and Networking (MOBICOM)*, pp. 255–265, 2000.

[18] P. Michiardi, R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-Hoc Networks," *Proc. 6th IFIP Conference on Communication and Multimedia Security (CMS)*, pp. 107–121, 2002.

[19] H. Miranda, L. Rodrigues, "Friends and Foes: Preventing Selfishness in Open Mobile Ad hoc Networks," *Proc. 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 440–445, 2003.

[20] Q. He, D. Wu, P. Khosla, "SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad-Hoc Networks," *Proc. IEEE Conference on Wireless Communications and Networking (WCNC)*, vol. 2, pp. 825–830, 2004.

[21] M. Medadian, M. H. Yektaie, A. M. Rahmani, “Combat with Black Hole Attack in AODV Routing Protocol in MANET,” *Proc. 1st Asian Himalayas International Conference on Internet (AH-ICI)*, pp. 1–5, 2009.

[22] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, M. S. Fallah, “A Secure Credit-Based Cooperation Stimulating Mechanism for MANETs Using Hash Chains,” *Future Generation Computer Systems*, vol. 25, pp. 926–934, 2009.

[23] J. Miao, O. Hasan, S. Ben Mokhtar, L. Brunie, K. Yim, “An Analysis of Strategies for Preventing Selfish Behavior in Mobile Delay Tolerant Networks,” *Proc. 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, pp. 208–215, 2012.

[24] L. Buttyan, L. Dora, M. Felegyhazi, I. Vajda, “Barter Trade Improves Message Delivery in Opportunistic Networks,” *Ad Hoc Networks*, vol. 8, n. 1, pp. 1–14, 2010.

[25] S. Zhong, J. Chen, Y.R. Yang, “Sprite: A Simple, Cheatproof Credit Based System for Mobile Ad Hoc Networks,” *Proc. 22nd IEEE Conference on Computer Communications (INFOCOM)*, pp. 1987–1997, 2003.

[26] B.B. Chen, M.C. Chan, “Mobicent: A Credit-Based Incentive System for Disruption Tolerant Network,” *Proc. 29nd IEEE Conference on Computer Communications (INFOCOM)*, pp. 1–9, 2010.

[27] D. Djenouri, N. Badache, “New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks,” *Proc. Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecurComm)*, pp. 288–294, 2005.

[28] D. Djenouri, N. Ouali, A. Mahmoudi, N. Badache, “Random Feedbacks for Selfish Nodes Detection in Mobile Ad Hoc Networks,” *Proc. 5th IEEE International Workshop on IP Operations and Management (IPOM)*, pp. 68–75, 2005.

[29] K. Balakrishnan, J. Deng, P.K. Varshney, “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks,” *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2137–2142, 2005.

[30] K. Liu, J. Deng, P.K. Varshney, K. Balakrishnan, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs,” *IEEE Trans. Mobile Computing*, vol. 6, no. 5, pp. 536–550, 2007.

[31] L. Tamilselvan, V. Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET,” *Journal of Networks*, vol. 3, n. 5, pp. 13–20, 2008.

[32] D. Djenouri, N. Badache, “On Eliminating Packet Droppers in MANET: A Modular Solution,” *Ad Hoc Networks*, vol. 7, n. 6, pp. 1243–1258, 2009.

[33] A. Baadache, A.Belmehdi, “Fighting Against Packet Dropping Misbehavior in Multi-hop Wireless Ad Hoc Networks,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1130–1139, 2012.

[34] P. García-Teodoro, J.E. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez, “Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges,” *Computer & Security*, vol. 28, pp. 18–28, 2009.

[35] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, Y. Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method,” *International Journal of Network Security*, vol. 5, n. 3, pp. 338–346, 2007.

[36] P.N. Raj, P.B. Swadas, “DPRAODV, A Dynamic Learning System against Blackhole Attack in AODV based MANET,” *International Journal of Computer Science Issues*, vol. 2, pp. 54–59, 2009.

[37] Y.F. Alem, Z.C. Xuan, “Preventing Black Hole Attack in Mobile Ad-Hoc Networks using Anomaly Detection,” *Proc. 2nd International Conference on Future Computer and Communication (ICFCC)*, vol. 3, pp.672–676, 2010.

[38] Y. Zhang, W. Lee, Y.A. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks,” *Wireless Networks*, vol. 9, n.5, pp. 545–556, 2003.

[39] Y. Huang, W. Fan, W. Lee, P.S. Yu, “Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies,” *Proc. 23rd IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp. 478–487, 2003.

[40] S. Bose, S. Bharathimurugan, A. Kannan, "Multi-Layer Integrated Anomaly Intrusion Detection System for Mobile Adhoc Networks," *Proc. IEEE International Conference on Signal Processing and Networking (ICSCN)*, pp. 360–365, 2007.

[41] J.F.C. Joseph, A. Das, B.C. Seet, B.S. Lee, "CRADS: Integrated Cross Layer Approach for Detecting Routing Attacks in MANETs," *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1525–1530, 2008.

[42] J.F.C. Joseph, B.S. Lee, A. Das, B.C. Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks using SVM and FDA," *IEEE Trans. on Dependable and Secure Computing*, vol. 8, n. 2, pp. 233–245, 2011.

[43] A.S. Buchegger, J.Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol," *Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking & computing (MOBIHOC)*, pp. 226–236, 2002.

[44] C. Basile, Z. Kalbarczyk, R.K. Iyer, "Inner-Circle Consistency for Wireless Ad Hoc Networks," *IEEE Trans. Mobile Computing*, vol. 6, n. 1, pp. 39–55, 2007.

[45] T. Hayajneh, P. Krishnamurthy, D. Tipper, K. Taehoon, "Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad Hoc Networks," *Proc. IEEE International Conference on Communications (ICC)*, pp. 1–6, 2009.

[46] M. Lima, A. dos Santos, G. Pujolle, "A Survey of Survivability in Mobile Ad-Hoc Networks", *IEEE Communications Surveys & Tutorials*, vol. 11, pp. 66–77, 2009.

[47] R. H. Jhaveri, S. J. Patel, D. C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," *Proc. 2nd International Conference on Advanced Computing Communication Technologies (ACCT)*, pp. 535–541, 2012.

[48] M.E.G. Moe, B.E. Helvik, S.J. Knapskog, "TSR: trust-based secure MANET routing using HMMs," *Proc. 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*, pp. 83–90, 2008.

[49] J.H. Cho, A. Swami, I.R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 13, n. 4, pp. 562–583, 2011.

[50] I.T.A. Halim, H.M.A. Fahmy, A.M. Bahaa El-Din, M.H. El-Shafey, "Agent-Based Trusted On-Demand Routing Protocol for Mobile Ad Hoc Networks," *Proc. 4th International Conference on Network and System Security (NSS)*, pp. 255–262, 2010.

[51] H. Xia, Z. Jia, X. Li, L. Ju, E.H.M. Sha, "Trust Prediction and Trust-Based Source Routing in Mobile Ad Hoc Networks," *Ad Hoc Networks, in press*, pp. 1–19, 2012.

[52] N. Sreenath, A. Amuthan, P. Selvigirija, "Countermeasures Against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs," *Proc. 2nd International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–7, 2012.

[53] S. Gupta, S. Kar, S. Dharmaraja, "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network," *Proc. 2nd International Conference on Computer and Communication Technology (ICCCT)*, pp. 468–473, 2011.

[54] S. Buchegger, J.Y. Le Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," *Proc. 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing (PDP)*, pp. 403–410, 2002.

[55] I. Khalil, S. Bagchi, C.N. Rotaru, N.B. Shroff, "UnMask: Utilizing Neighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks," *Ad Hoc Networks*, vol. 8, n. 2, pp. 148–164, 2010.

[56] M.-Y. Su, K.-L. Chiang, W.-C. Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," *Proc. 8th International Symposium on Parallel and Distributed Processing with Applications (ISPA)*, pp. 162–167, 2010.

[57] P.C. Tsou, J.M. Chang, Y.H. Lin, H.C. Chao, J.L. Chen, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs," *Proc. 13th International Conference on Advanced Communication Technology (ICACT)*, pp. 755–760, 2011.

[58] R.H. Jhaveri, S.J. Patel, D.C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad Hoc Networks," *Proc. 2nd International Conference on Advanced Computing Communication Technologies (ACCT)*, pp. 556–560, 2012.

[59] A. Konig, M. Hollick, R. Steinmetz, "On the Implications of Adaptive Transmission Power for Assisting MANET Security," *Proc. 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS)*, pp. 537–544, 2009.

[60] Y.A. Mohamed, A.B. Abdullah, "Immune-Inspired Framework for Securing Hybrid MANET," *Proc. IEEE Symposium on Industrial Electronics Applications (ISIEA)*, vol. 1, pp. 301–306, 2009.

[61] X. Ye, J. Li, "A Security Architecture Based on Immune Agents for MANET," *Proc. International Conference on Wireless Communication and Sensor Computing (ICWCSC)*, pp. 1–5, 2010.

[62] X. Ye, J. Li, R. Luo, "Hide Markov Model Based Intrusion Detection and Response for MANETs," *Proc. 2nd International Conference on Information Technology and Computer Science (ITCS)*, pp. 142–145, 2010.

[63] P.L.R. Chze, W.K.W. Yan, Kan Siew Leong, "A User-Controllable Multi-Layer Secure Algorithm for MANET," *Proc. 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1080–1084, 2012.

[64] A. Nabet, R. Khatoun, L. Khoukhi, J. Dromard, D. Gaiti, "Towards Secure Route Discovery Protocol in MANET," *Proc. 3rd Global Information Infrastructure Symposium (GIIS)*, pp. 1–8, 2011.

[65] C.A. Melchor, B.A. Salem, P. Gaborit, K. Tamine, "AntTrust: A Novel Ant Routing Protocol for Wireless Ad-hoc Network Based on Trust between Nodes," *Proc. 3rd International Conference on Availability, Reliability and Security (AReS)*, pp. 1052–1059, 2008.