Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges

Soufiene Djahel, Farid Naït-abdesselam and Zonghua Zhang

***Abstract*—Nodes in mobile ad hoc networks (MANETs) usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments some nodes may refuse to do so for either saving their resources or intentionally disrupting regular communications. This type of misbehavior is generally referred as *packet dropping* attack or *black hole* attack, which is considered as one of the most destructive attacks that leads to the deterioration of network performance.**

The special network characteristics, such as limited battery power and mobility of nodes, make prevention techniques based on cryptographic primitives ineffective to cope with such attack. Rather, a more proactive alternative is required to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Once such scheme fails, some economic-based approaches can be adopted to alleviate the attack consequences by motivating the nodes cooperation. As backup, detection and reaction schemes remain as the final defense line to identify the misbehaving nodes and punish them.

In this survey, we make a comprehensive investigation on state-of-the-art countermeasures to packet dropping attack. Furthermore, we examine the challenges that must be tackled for constructing an in-depth defense against such sophisticated attack.

***Index Terms*—Ad Hoc Networks, Routing Protocols Security, Packet Dropping Attack, Black Hole Attack**

I. Introduction

MOBILE ad hoc networks (MANETs) are usually formed by a group of mobile nodes, interconnected via wireless links, which agree to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative. That means, if a node claims it can reach another node by a certain path or distance, the claim is trusted/true; similarly, if a node reports a link break, the link will no longer be used. While this assumption can fundamentally facilitate the design and implementation of routing protocols, it meanwhile introduces a vulnerability to several types of denial of service (DoS) attacks [41], particularly packet dropping attack. To launch such attack, a malicious node can stealthily drop some or all data or routing packets passing through it.

Due to the lack of physical protection and reliable medium access mechanism, packet dropping attack represents a serious threat to the routing function in MANETs. A foe can easily join the network and compromise a legitimate node then subsequently start dropping packets that are expected to be relayed in order to disrupt the regular communications. Consequently, all the routes passing through this node fail to establish a correct routing path between the source and destination nodes.

Although upper layer acknowledgment, such as TCP ACK (Transmission Control Protocol ACKnowledgment) can detect end-to-end communication break, it is unable to identify accurately the node which contributes to that. Moreover, such mechanism is unavailable in connectionless transport layer protocols like UDP (User Datagram Protocol). Therefore, securing the basic operation of the network becomes one of the primary concerns in hostile environments in the presence of packets droppers. The challenge lies in securing communication meanwhile maintaining connectivity between nodes despite of the attacks launched by the foes and the frequently changing topology. It is thus obvious that both phases of the communication, mainly route discovery and data transmission phase, should be protected, calling for comprehensive security studies.

While a number of surveys [21], [26], [29] and [42], dealing with security threats against routing protocols in MANETs, have provided some insightful overviews on different threats and countermeasures, none of them focuses on a specific attack and examines all its characteristics in different routing techniques. To complement those efforts, this work studies the packet dropping attack, which is known as one of the most destructive threats in MANETs, and illustrates in depth the different schemes used by adversaries targeting on both reactive and proactive protocols. Furthermore, we conduct an up-to-date survey of the most valuable contributions aiming to avoid the packet droppers. The careful examination and analysis has allowed us to carry out a comparative study of the existing security schemes in terms of specific design rationale and objectives. The ultimate goal is to identify the strengths and weaknesses of each scheme in order to devise a more effective and practical solution which can achieve a better trade-off between security and network performance.

The remainder of the paper is structured as follows. In next section, we discuss the root causes of dropping packets in MANETs. Section III describes the Black hole attack in both reactive and proactive routing protocols. An overview of the proposed security schemes for defending against this attack is given in section IV. In section V, some open challenges related to the herein presented attack and solutions are highlighted. Finally, section VI concludes the paper and points out future research directions.

Soufiene Djahel and Farid Naït-abdesselam are with the Department of Computer Science, University of Lille1, France.

Zonghua Zhang is with Institut TELECOM/TELECOM Lille1, France.

Manuscript received February 2010.

II. Root causes of packet dropping in MANETs

Before analyzing the packet dropping attack in details, let us first summarize the different motives that incite some nodes to drop a packet rather than sending or relaying it. In general, a packet can be dropped at either MAC or network layers due to the following reasons:

- The size of packets' transmission buffer at MAC level is limited; therefore whenever the buffer is full any new packet arriving from higher layers will be dropped (buffer overflow).
- IEEE 802.11 protocol's [4] rules: a data packet is dropped if its retransmission attempts or the one of its corresponding RTS (Request To Send) frame has reached the maximum allowed number, owing to node's movement or collision (a lot of contending nodes).
- A data packet may be dropped or lost if it is corrupted during transmission due to some phenomenon specific to radio transmissions such as interference, hidden nodes and high bit error rate.

In addition to these causes, a selfish node may refuse to relay a packet aiming to economize its energetic resources in order to extend its lifetime or simply because its battery power is drained. Moreover a malicious node involved in a routing path may intentionally drop the packets at network layer in order to provoke a collapse in network performances. Furthermore, it can modify the IEEE 802.11 MAC protocol's parameters to provoke packet dropping. According to this analysis, packet dropping problem still open the door to new challenges in MANETs. For example, how can we recognize the reason leading a node to drop others' packets? In other words, how can we know the intention of a node to accuse it as malicious, selfish or legitimate?

III. Black hole attack in MANETs

The black hole attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack. In particular the malicious node can intentionally drop all the forwarded packets going through it (black hole), or it can selectively drop the packets originated from or destined to certain nodes that it dislikes. Furthermore, a special case of black hole attack dubbed *gray hole* attack is introduced in [23]. In this attack, the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed.

In order to launch a black hole attack, the first step for a malicious node is to find a way that allows it to get involved in the routing/forwarding path of data/control packets. To do so, it exploits the vulnerabilities of the underlying routing protocols which are generally designed with strong assumption of trustworthiness of all the nodes participating in the network. Thus, any node can easily misbehave and provoke a severe harm to the network by targeting both data and control packets.

Dropping data packets leads to suspend the ongoing communication between the source and the destination node. More seriously, an attacker capturing the incoming control packets can prevent the associated nodes from establishing routes between them. To facilitate understanding, we illustrate them using two representative routing protocols in MANETs, OLSR (Optimized Link State Routing) [16] and AODV (Ad hoc On Demand Distance Vector) [14], which are table-driven and on-demand respectively.

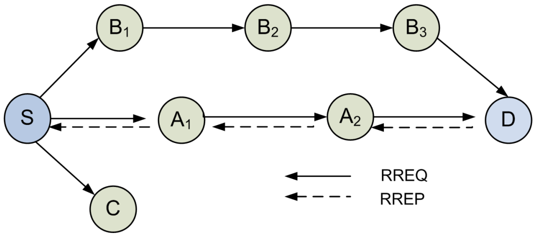


Fig. 1: Route discovery in AODV

A. Routing protocol-specific attack

We first address black hole problem in the two routing protocols cited above.

1) Black hole attack in AODV: In order to discover a new path towards a faraway destination, the source node broadcasts a RREQ (Route REQuest) message with unique identifier to all its neighbors. Each receiver rebroadcasts this RREQ to all its neighbors until reaching the intended destination as depicted in Fig. 1. On receiving the RREQ message, the destination node updates the sequence number of the source node and sends a RREP (Route REPly) message back to its neighbor which has relayed the RREQ. On the other hand, an intermediate node having a route to the destination with destination sequence number greater or equal to the one in RREQ can send back a RREP packet to the source node without relaying the RREQ to the destination. Notice that the links between nodes may be lost due to nodes' mobility, so a RERR (Route ERRor) message is generated and forwarded back to the source node to report the link failure. Thus, the source node initiates a new route discovery to replace the failed path.

The DSR (Dynamic Source Routing) [5] protocol uses the same mechanism as AODV to discover new routes, however the complete path to the destination is chosen by the source node and loaded in the packet header. All the intermediate nodes have to relay the packets with respect to the route specified in the packet header. This feature is important in some cases in order to satisfy QoS (Quality of Service) [47] requirements by performing load balancing between the relay nodes. In this case, the source node sends the packets through different paths to avoid overloading any node in the network.

In on-demand routing protocols, dropping control packets might be the greatly benefit for both selfish and malicious nodes. Specifically, once dropping the RREQ packets, a selfish node prevents the established routes from passing through it and consequently it saves its energy for transmitting its own packets. Likewise, a malicious node can drop the RERR packets in order to prolong the duration of use of the broken routes. As a result, the network throughput collapses sharply since no packet reaches its destination.

A prerequisite for a node to launch a black hole attack is to be involved at least in one routing path. To this end, the

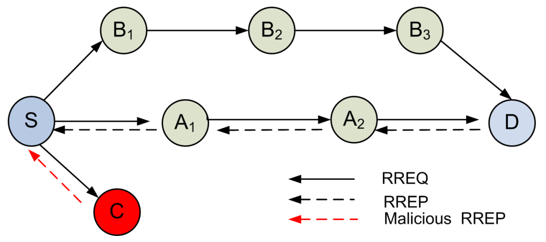


Fig. 2: Black hole attack in AODV

TABLE I: The values of the different fields of RREQ and RREP packets sent or forwarded by both legitimate and malicious nodes: (i) the nodes A_1 and A_2 forward correctly the RREQ and RREP packets (ii) the node C spoofs the destination node's address (D) and augments illegitimately the Dst-Seq-Num

	RREQ			**RREP**			
Sender	S	A_1	A_2	D	A_2	A_1	**C**
IP-src	S	A_1	A_2	D	A_2	A_1	**D**
Dst-adr	D			S			S
Dst-Seq-Num	40			41			**55**

malicious node applies the strategies illustrated below.

- As shown in Fig. 2, C is a malicious node whereas S and D are the source and destination nodes, respectively. First, the node S broadcasts RREQ packet to its one hop neighbors. Then, upon receiving this packet each neighbor node is supposed to rebroadcast it if a route cache towards the destination is unavailable. However, the node C disobeys this rule and claims that it has the shortest path to the destination and sends a RREP packet back to node S. Consequently, if the RREP packet sent by node D or any honest intermediate node, which has a fresh route to D, reaches the node S before the C's RREP then everything works well. Otherwise, the source node S deems that the route passing through the node C is the shortest path, and thus it starts transmitting data packets towards C which in its turn drops them.
- Another strategy to launch the attack can be described as follows: an intermediate node C spoofs the IP address of the destination D, inciting the source node S to establish the path towards C, instead of D. To illustrate that let us consider the network topology depicted in Fig. 2, when the attacker node C receives a RREQ packet it transmits a RREP packet to reply back to S claiming that it is the intended destination. Moreover, it increases the Destination Sequence Number (Dst-Seq-Num) received in RREQ packet by a value larger than one as shown in Table I, where the node C sets Dst-Seq-Num to 55 rather than 41 to guarantee that the source node S chooses it as the actual destination. The consequences of this attack strategy are similar to the previous one.

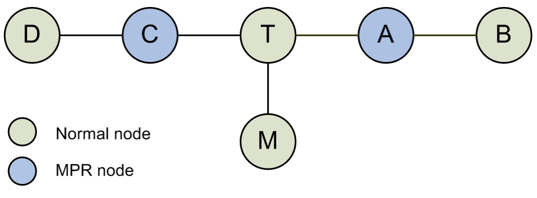


Fig. 3: The MPR set of node T before launching the attack

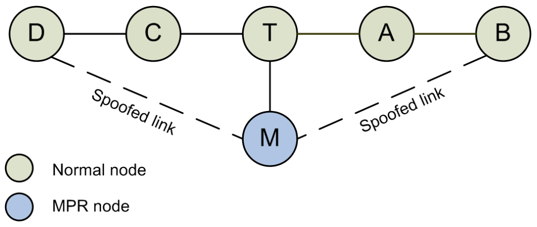


Fig. 4: The new MPR set of node T after the spoofing link attack is launched

2) Black hole attack in OLSR: The Optimized Link State Routing protocol (OLSR) is a proactive routing protocol designed for large and dense networks. The main optimization of this protocol is achieved through the use of MPRs (MultiPoint Relays) which are a set of neighbor nodes that represent the unique responsible for spreading the local link state information to the whole network, thereby reducing the induced overhead. Notice that the local link state information is periodically advertised by the MPR nodes via the transmission of TC (Topology Control) messages. In OLSR, each node selects its MPR set from its one hop neighbors set such that it can easily reach all its two hop neighbors with minimum number of retransmissions. The MPR selection function depends on the number of two hop neighbors reachable through the candidate node and its 'Willingness' value obtained from Hello message. This value indicates the readiness of a node, according to its own resources, to forward the packets of its neighbors. Nodes with higher willingness value are given higher priority to be selected as MPR.

The main functionality of OLSR is neighbor sensing and topology dissemination. Neighbor sensing is accomplished through the periodic exchange of Hello messages, in which every node advertises its neighbor set along with the state of the link connecting it to each neighbor. In addition to that, it indicates whether a given neighbor has been chosen as MPR or not. To disseminate the topological information, each MPR node broadcasts periodically a TC message that contains its MPR selectors set. Using this information, each node constructs a partial topology graph of the network which allows it to establish routes to non-neighboring nodes.

Since TC messages are flooded across the whole network, the attack can occur either at the origin or forwarding point. The damage resulted from targeting a TC message is more severe than that caused by misusing Hello messages as the TC messages are used globally by the whole network for routes calculation. A malicious node may simply send a TC message claiming to be the MPR of nodes although it is not. Therefore, as the network depends on the MPRs for routing services, a malicious node that manages to become an MPR can easily launch a black hole attack on the network. In what follows, we present the strategy adopted by a node to launch a black hole attack.

TABLE II: Example of Hello message sent by node M

Originator-adr	**1-hop neighbors**
M	T, **B**, **D**

- **Gain an MPR position in the network**: a simple way for a malicious node to be an MPR is to set constantly its willingness field to the highest allowed value regardless of its available resources. Thus it compels all its neighbors to elect it as MPR. Besides, it may force a target node to select it as the only MPR by spoofing links with all its 2-hop neighbors as described below. To illustrate this scenario, let us consider the network topology depicted in Fig. 3, where the nodes A and C constitute the MPR set of the node T. The malicious node M generates its Hello message in which it advertises the non-neighboring nodes B and D as its neighbors, as illustrated in Table II. According to the MPR computation heuristic [16], the node T must choose M as the only MPR node, as shown in Fig. 4, since it has connections to the whole set of its two hop neighbors (B, D). Notice that the node M can learn the T's two hop neighbors set by analyzing the received TC messages along with the T's Hello message.
- **Drop all control or data packets supposed to be relayed**: as an MPR, a node can carry out the following disruptions:
  - Correctly participates to TC message forwarding function but fails to deliver data packets for other nodes.
  - Drops all TC messages sent or relayed by its MPR selector nodes. For example, in the network topology depicted in Fig. 5 the malicious node M refuses to relay the TC messages generated by the node T. Thus this makes the routes towards the MPR selectors of node T unknown for the rest of the network. The Fig. 6 illustrates that, where the nodes A_1, A_2 and A_3 are hidden from the nodes B and C because the T's TC message has not been received.
  - Colludes with another neighbor MPR node to make the previous attack harder to be detected as illustrated in [50].

In heterogeneous networks such as MANETs the status of asymmetric links is more likely to be observed. As an example, the topology depicted in Fig. 7 shows two asymmetric links connecting T_1 with T_2 and T_2 with M. Malicious nodes (such as node M in Fig. 7) may get benefits from that and exploit it to launch a black hole attack. To do so, the node M tries to create a false symmetric link between T_1 and T_2. The establishment of this fake symmetric link requires five steps as follows:

msg1: $T_1 \longrightarrow * : Hello, \{\emptyset\}.$

During neighbor discovery phase, the node T_1 broadcasts an empty Hello message that reaches both nodes T_2 and M.

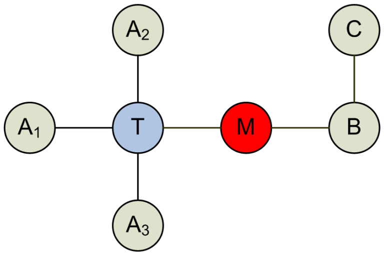


Fig. 5: The network topology held by the nodes B and C before the attack, where they are able to communicate with the T's MPR selectors nodes.

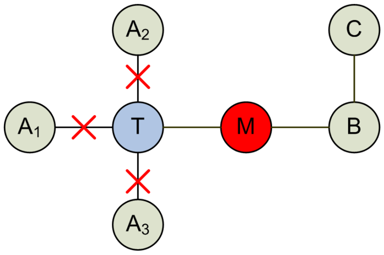


Fig. 6: The network topology held by the nodes B and C after the attack, where the nodes A_1, A_2 and A_3 are unknown for them.

msg2: $T_2 \longrightarrow * : Hello, \{T_1, ASYM\}.$

Next, the node T_2 advertises, in its Hello message, that the node T_1 is an asymmetric neighbor.

msg3: $M \longrightarrow T_1 : Hello, \{T_1, ASYM\}.$

Upon receiving the message msg2, the node M maliciously forwards it to the node T_1 albeit it is not supposed to do.

msg4: $T_1 \longrightarrow * : Hello, \{T_2, SYM\}.$

When the message msg3 reaches the node T_1, it finds its identity included in the advertised neighborhood list and consequently it concludes that it is a symmetric neighbor of T_2. Hence, it advertises this new link status in its Hello message.

msg5: $T_2 \longrightarrow * : Hello, \{T_1, SYM\}.$

On receiving the Hello message msg4, the node T_2 changes its link status with T_1 to symmetric.

As a result, the victim nodes T_1 and T_2 infer that they are connected through a symmetric link while it is not. So, all control packets, such as TC messages, generated by the MPR selectors of node T_2 will not reach the whole network. As a result, the network may be partitioned.

Notice that $*$ denotes the dissemination of a message and {*Id, link*} refers to the content of Hello message, where *Id* is the neighbor identity and *link* is the status of the link connecting the sender of the message and the node *Id*.

B. Inter-layer attack

In this attack, the malicious node modifies the default configuration of IEEE 802.11 MAC protocol, for example it denies the response to the RTS packet sent by its neighbors

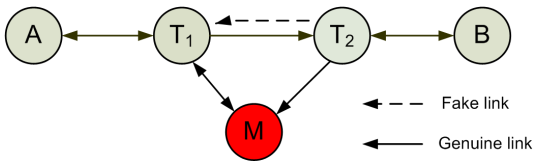


Fig. 7: Fake symmetric link created between nodes T_1 and T_2

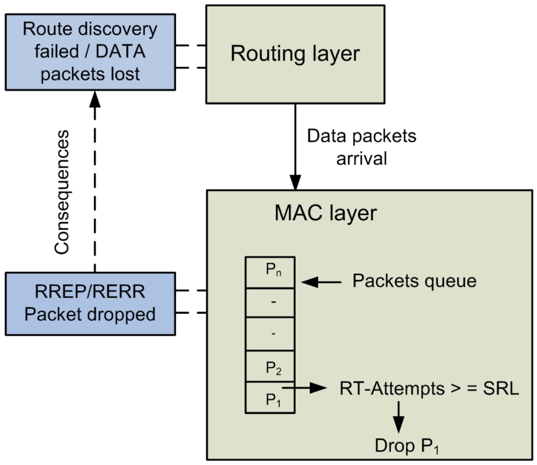


Fig. 8: Inter-layer attack description

rather than sending a CTS (Clear To Send) packet after the SIFS (Short Inter Frame Space) period. When the CTS timeout expires, the sender of RTS infers that the malicious node didn't receive it correctly (i.e, a collision is occurred), as stated in [4]. Thus it retransmits the RTS after waiting for a new backoff time. After several retransmission attempts (RT-attempts), the sender of RTS abandons the transmission of the corresponding data frame whenever the number of attempts reaches the SRL (Short Retry Limit) as depicted in Fig. 8. This attack may disrupt the route discovery process in reactive routing protocols, such as AODV, when the malicious node drops the RTS of the RREP packet, which leads to initiating a new route discovery. Moreover, this misbehavior can trigger a route maintenance process since the sender node will conclude that the link with the malicious node is broken. Consequently, the network performance degrades sharply.

IV. Secure MANETs against Black hole attack

Recently, many investigations have been done in order to improve the security in MANETs, most of which are relied on cryptographic based techniques in order to guarantee some properties such as data integrity and availability. In what follows, we give a snapshot of the mostly used cryptographic primitives in MANETs.

A. *Overview of the cryptographic primitives*

As MANETs become more ubiquitous, the need for providing adequate security tools gets to be more obvious. The existing security schemes in such networks use generally one or more of the following cryptographic technologies: symmetric-key cryptography [15], digital signature [3], threshold cryptography [1] and one way hash chain [2]. Each of these cryptographic primitives has its specific advantages and drawbacks. For example, the security schemes based on digital signature and threshold cryptography generate much more computational overhead than those based on symmetric cryptography. However, the security approaches that are solely based on symmetric-key cryptography are less robust and offer less security than asymmetric key cryptography, due to the higher probability that the shared keys being compromised. As one way chains are known to be very efficient for verification, they became increasingly popular for designing security protocols for hand-held devices. This is due to the fact that the low-powered processors are able to compute a one way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature [8], [22]. Consequently, recent wireless ad hoc network's security protocols extensively use one way chains to design protocols that scale down to resources constrained devices.

These cryptographic schemes are known to be efficient to ensure several properties such as confidentiality, data integrity and non repudiation. However, they cannot be adopted in MANETs since a Certificate Authority (CA) or a Key Distribution Center (KDC) are not always available. Moreover, these techniques cannot prevent a malicious node from dropping packets supposed to be relayed, which is our focus in this survey. In Table III, we point out the main advantages and drawbacks of the cryptographic primitives presented above.

B. *Taxonomy of the proposed solutions in the literature*

There are basically three defense lines devised to protect MANETs against the packet dropping attack as illustrated in Fig. 11. The first defense line (for prevention purposes) aims to forbid the malicious nodes from participating in packet forwarding function. Whenever the malicious node exceeds this barrier, a second defense line (for incentive purposes) is launched, which seeks to stimulate the cooperation among the router nodes via an economic model. Finally, once the two previous defense lines have been broken, a third one (for detection/reaction purposes) is launched aiming to reveal the identity of the malicious node and excludes it from the network.

First defense line schemes

Many researchers have been interested to develop several mechanisms to identify the malicious nodes that attempt to involve themselves in the routing path, and then take control over data/control packets. In the sequel, we give an overview of the major proposals which aim to recognize the malicious nodes at earlier stage of misbehaving before causing any damage to the network.

The authors of [12] have proposed a solution to cope with the black hole attack in AODV. First, they suggest to disable the ability of an intermediate node to send a RREP and allow only the final destination to do that. This technique avoids the black hole problem but increases the route establishment delay, especially in the case of large networks. Furthermore, since no authentication is used in RREP message a smart

[1] n is the chain's length.

TABLE III: Cryptographic primitives comparison

		Approach		
		Symmetric-key cryptography	**Asymmetric cryptography**	**One way hash chain**
Comparison Criteria	**Speed**	Fast	Slow	Fast
	Scalability	Not scalable	scalable	scalable
	Computational overhead	Moderate	High	Lighweight
	Clock synchronization	No	No	Mandatory
	Storage capacity	Large	Large	O(log (n))[1]
	DoS Resiliency	Resilient	Not resilient	Resilient

attacker can forge a RREP message on behalf of the legitimate destination (by spoofing its IP address). As such, this solution is inappropriate for coping with this attack. To overcome these shortcomings, they have proposed another solution which requires that the intermediate node adds its next hop's information to the RREP packet before sending it. On receiving this packet, the source node sends a special packet to the next hop of the intermediate node in order to verify that it has a route to the destination and also it is a neighbor of the intermediate node. This special packet contains a field dubbed check result which might be filled by the next hop node. When the source node receives the reply to this packet it extracts the check result information and decide accordingly whether this route is safe or not. If so, it sends out the data packets, otherwise it initiates a new route discovery or waits for subsequent RREPs. While this solution can avoid the black hole attack launched by a single node, it is unable to detect a collusive attack conducted by both of intermediate and next hop nodes. Moreover, its main disadvantage is the induced overhead if the check process is repeated for each intermediate node replying to the RREQ.

To ascertain the safety of the established path, a new scheme is proposed in [13] to secure AODV. This scheme can be briefly described as follows; once the normal path discovery procedure is finished, the source node sends special control packets to request each originator of RREP packet to send back its current neighbor set. On receiving more than one reply, the node starts comparing the received neighbor sets. If the difference between them is larger than a predefined threshold then a black hole attack is identified. To mitigate its impact, a cryptography-based reaction mechanism is designed, whereby the source node recognizes the true destination. Subsequently, a new control message is sent to the destination to establish the correct path. This method can reduce the likelihood of a successful black hole attack, but it cannot guarantee its prevention.

To secure OLSR against the colluding black hole attack, in which two malicious MPR nodes collude each other to prevent TC messages from being relayed correctly, a solution is proposed in [36]. This solution is based on a slight modification to the standard Hello message by adding the 2-hop neighbors set to the advertised set of one hop neighbors. Based on this information, any node can detect whether one of its neighbors has sent a false Hello message by searching any contradiction between the received neighbor sets. This solution can prevent the nodes that spoof links with non-neighboring nodes from being selected as MPR. However, the high mobility of nodes can paralyze the network due to the huge number of the induced false alarms. Moreover, these contradictions can no more stand if the attacker spoofs links with far-away (more than two hops away) or not existing nodes.

TOGBAD approach was proposed in [43] to defend against colluding black hole attack in tactical MANETs, in which a successful attack can lead to human life loss. The proposed solution is designed to secure OLSR protocol, however it is suitable for any routing protocol based on Hello message exchange. Each network node extracts the neighbors list from the received Hello messages and sends it to the supervisor node. This latter, which is the only node running the TOGBAD scheme, uses the received information to construct the network topology graph. This graph is built based on the Cluster-Based Anomaly Detector (CBAD) introduced in [20] and [35]. Next, upon reception of a message from a node, the supervisor node extracts the number of neighbors claimed by the sender node and compares it with the size of this sender's neighbor set as calculated from the topology graph. If the difference between the claimed neighbors set and the one extracted from the graph exceeds a predefined threshold, then the supervisor concludes that this is an attempt to launch an attack and consequently an alarm is triggered. The extra messages sent by each node to the supervisor leads to an enormous control overhead increase in the network. Likewise, an excessive increase in computation overhead at the supervisor node is also observed. Therefore, this scheme is not suitable for MANETs due to the limited energy and computation resources of wireless nodes.

The herein described approaches aimed at attacks avoidance by means of preventing malicious nodes from being selected as part of the routing path of data packets. According to [7], the attacks can be avoided by prevention based mechanisms only if the applied techniques are perfect, which is hard to achieve in MANETs. Otherwise, someone will find out how to get around them; for example, in OLSR a malicious node can participate correctly to MPR selection phase however it fails to forward data packets when it is selected as MPR. In such case prevention techniques are useless. Besides, most of the attacks and vulnerabilities have been the result of evading the prevention mechanisms. Given this reality, detection and response are vital approaches for MANETs.

Second defense line schemes

As we have mentioned in section II, a selfish node does not want to waste its resources for the benefit of other nodes. Hence, it refuses to forward other's packets but it still uses their services to communicate. To cope up with such behavior, one possible solution is to deprive the selfish node from the services provided by the rest of the network. Therefore, it will be obliged to cooperate. Otherwise it will be isolated from the network and never get its packets forwarded. This class of solutions is also referred to as *Incentive based schemes*.

One of the most reputable works in this category is the model introduced in [9]. This work proposes the use of a virtual currency, dubbed nuglets, as a payment currency in order to motivate each node to forward other's packets. Using nuglets, the authors have proposed two payment models: the Packet Purse Model (PPM) and the Packet Trade Model (PTM). In the former model, the packet sender loads some nuglets in the packet before sending it. The forwarder of this packet earns some nuglets as a payment for the service. If the quantity of nuglets in the packet reaches zero, then it is dropped. In the latter model, as opposed to the former one the packet's final destination rewards the intermediate nodes using its own nuglets. This model can be described as follows: each intermediate node earns some nuglets by buying a packet from its previous node for some nuglets and then selling it to the next node for more of nuglets, and the total cost will be paid by the destination. The main drawback of this technique is how to ensure that some nodes do not sell the same packet to more than one neighbor to earn extra money? And how to ensure that each receiver indeed has enough money to pay for the service?

To implement both of these models, each node is equipped with a tamper resistant security module that maintains the nuglets counter in order to prevent the nodes from illegitimate increase of their own nuglets.

Another sound work is the protocol SIP (Secure Incentive Protocol) proposed in [44]. In contrast to the previous schemes, SIP adopts a payment model in which node remuneration is accomplished by charging both source and destination nodes and rewarding the intermediate nodes. Moreover, the adopted model allows a node to transmit some extra packets when it has not enough credit for all the packets ready to be sent. The security of the payment process is achieved by dint of tamper-proof module embedded in each node. SIP is designed to work with any secure reactive protocol such as Ariadne [11] and ARAN [25]. The major weakness of this technique is the unfairness problem. The nodes situated in the network edges are less involved in the routing path due to their locations, therefore they cannot earn enough credit to send their packets.

Third defense line schemes

Most of the proposed solutions to handle packet droppers fit into this defense line. Hence, to conduct an in depth study we have classified them into five categories according to their basic ideas:

- *Passive feedback based schemes*: it encloses all the solutions whose the principle consists in overhearing the neighbor's transmission to check its legitimacy.
- A*ACK-based schemes*: in this category, a node might request an acknowledgment from its succeeding neighbors to confirm the well reception of its packet.
- *Reputation-based schemes*: it represents the solutions that judge a node is malicious or well-behaved according to an assessment of its trustworthiness level which is computed based on several observations of its behavior.
- *Cross-layer cooperation based schemes*: this class illustrates the cooperation between two or more layers to either detect or enhance the detection accuracy of packet droppers. A given layer might make another layer aware of the beginning and the end of some operations or the values of some metrics in order to ensure better efficiency and accuracy.

1) Passive Feedback based schemes:

Watchdog [6] is the first work that has dealt with the problem of nodes which agree to forward packets but never do so. It is designed to secure the DSR protocol and is based on the passive feedback technique, described as follows: (i) first, the watchdog node A transmits the packet (p) to its next hop B, as shown in the Fig. 9. (ii) then it overhears the medium, using the promiscuous mode [2] to ensure that B has correctly forwarded the packet (p) towards C. If a misbehaving node is identified in the path towards the destination node, then a response mechanism dubbed Path-rater is launched. The goal of path-rater is to establish a new route that avoids the misbehaving nodes.

This scheme suffers from several weaknesses, as stated in [6]. Since a packet collision might occur and prevent the packet to reach the intended receiver, a forwarder node should not immediately be accused of misbehaving, but rather observed for a longer period to make an accurate decision. So, the detection of malicious nodes can take a long time. Moreover, power control transmission and collusion between group of nodes can trick the watchdog node. Finally, a malicious node can falsely accuse a legitimate node as misbehaving in order to exclude it from the network.

Many techniques have been proposed to enhance the robustness of Watchdog. Among them, the work presented in [17] which proposes to choose more than one Watchdog node to avoid the devastating impact of false reports sent by the malicious nodes. To this end, the nodes are classified to ordinary, trusted and Watchdog nodes in terms of their trustworthiness. The trusted nodes are assumed to be the first nodes that initially form the network. The Watchdog nodes are selected periodically from the trusted nodes exclusively. On

[2] When the promiscuous mode is enabled, it allows the node to capture all the frames sent in its vicinity regardless of their destination addresses, and then sends them to the higher layers for analysis purposes.

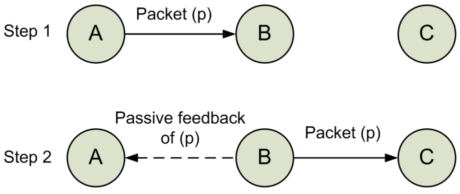


Fig. 9: The principle of passive feedback

receiving the first reply for the route discovery process that has launched, the source node sends out in the secure Watchdog channel a special message to inform the Watchdog nodes about the ongoing transmission. Then, these nodes start monitoring the intermediate nodes connecting the source and destination nodes in order to report any misbehavior. This scheme can indeed detect and isolate the malicious nodes acting alone or in groups, however the induced overhead due to the new control messages is important.

In order to cope with the aforementioned problem of false reports, Ex-Watchdog is proposed in [39]. In this scheme, each node maintains a table containing information about all the paths it is involved in. Each entry of this table stores the following information: identifiers of the source and destination nodes, the identifier of the path connecting the source to the destination and finally the sum of all packets sent, forwarded or received through this path. Upon receiving a message reporting an intermediate node as malicious, the source node will not increase the failure tally of this node immediately as the Watchdog does. However, it sends out a special message to the destination node through an alternative path. This message contains the same fields as each entry in the table except that the path identifier is replaced by the malicious node's address. When the destination node receives this message, it checks first if there is a matching entry for the source and destination addresses in the table.

If so, then it compares the sum value received and the one kept in its table. If the two values match then the accused node is not malicious since all the packets sent by the source are received at the destination. In contrast, if the two values are different, then a reaction mechanism is triggered.

If no matching entry exists, then the reported node is malicious. As a result, a confirmation message is sent back to the source node. The absence of an alternative path to the destination makes the source unable to check the correctness of the report, and thus cannot recognize which node is malicious; the reporter or the reported.

2) *ACK based schemes:*

To circumvent the limitations of the passive feedback based solutions, an explicit acknowledgment has been used by several schemes as a way to confirm the well reception of a packet by the far-away neighbors.

a) *ACK-based schemes in reactive protocols:*

Two hop ACK based scheme is proposed in [27] to overcome the limitation of passive-feedback technique when power control transmission is used. To implement this scheme, an authentication mechanism is used to prevent the next hop from sending a forged ACK packet on behalf of the intended two hop neighbor. The main drawback of this scheme is the huge overhead. In order to reduce the overhead, the authors have proposed in [30] that each node asks its two hop neighbor to send back an ACK randomly rather than continuously. Likewise, this extension also fails when the two hop neighbor refuses to send back an ACK. In such situation, the requester node is unable to distinguish who is the malicious node, its next hop or the requested node.

To overcome the previous ambiguity in determining the true malicious node, [38] focuses on detecting malicious links instead of malicious nodes. The authors propose the 2ACK scheme to detect malicious links and to mitigate their effects. This scheme is based on 2ACK packet that is assigned a fixed route of two hops in the opposite direction of the received data traffic's route. In this scheme, each packet's sender maintains the following parameters; (i) list of identifiers of data packets that have been sent out but have not been acknowledged yet, (ii) a counter of the forwarded data packets, (iii) and a counter of the missed packets. According to the value of the acknowledgement ratio (Rack), only a fraction of data packets will be acknowledged in order to reduce the incurred overhead. This technique overcomes some weaknesses of the Watchdog/pathrater such as: ambiguous collisions, receiver collision and power control transmission.

Both of the previous works remain vulnerable to the attacks launched by group of nodes. To counter these attacks, [32] provides a framework to mitigate the damage caused by the colluding black hole attack in AODV. The proposed technique has a moderate overhead induced by the ACK sent back by the destination during selected intervals of data transfer period. Throughout the data packets transmission, a flow of special packets is transmitted at random intervals along with the data. The reception of these special packets invokes the destination to send out an ACK through multiple paths. The ACK packets take multiple routes to reduce the probability that all ACKs being dropped by the malicious nodes, and also to account for possible loss due to broken routes or congestion in certain nodes. If the source node does not receive any ACK packet, then it becomes aware of the presence of attackers in the forwarding path. As a reaction, it broadcasts a list of suspected malicious nodes to isolate them from the network.

b) *ACK-based schemes in proactive protocols:*

The authors of [49] have proposed a simple mechanism to detect the malicious nodes that drop TC packets in OLSR. To do so, these nodes spoof links with the target's two hop neighbors in order to gain an MPR position in the network. This approach requires that each node receiving TC message has to send an authenticated ACK back to the TC's source node. This requirement is carried out only if the receiver node is two hop neighbor of the TC's source node. In this scheme, each MPR node maintains a table containing its entire two hop neighbors set of link tuples and their corresponding trust values. During MPR selection phase, any node involved at least in one tuple whose the trust value equal to 0 should not be chosen as the unique MPR. Therefore, any misbehavior from a neighbor node can be easily detected.

We have proposed in [50] a three hops acknowledgment based scheme to cope with the cooperative black hole attack in OLSR. Our scheme adds two extra packets to OLSR, Hello-rep packet which is a slight modification to Hello message and a small acknowledgment packet. In this solution, each MPR node M acquires the list of its 3-hop neighbors reached through a distinct pairs of two consecutive MPR nodes (M1, M2), where M2 is the MPR node of M1 and this latter is the MPR of the node M. Afterwards, the node M selects one node, from this list, to which it requests an authenticated acknowledgment as a confirmation of the reception of the TC message that it has generated/forwarded. Notice that the authentication process is carried out using a pre-established secret key between node M and the requested node. If the number of missed acknowledgements overtakes a predefined threshold then the MPR nodes M1 and M2, relaying M and the requested node, are considered as malicious and consequently they will never be selected as MPR.

c) Requirements of ACK-based schemes:

All the nodes running a solution based on acknowledgment need to maintain a timeout (To) value. This timeout represents an upper bound of the time that the sender node has to wait for the ACK to arrive. The determination of this timeout value is critical since a small value induces a large number of false accusations and a large value increases the memory required to store the outgoing packets for further comparisons. Fig. 10 depicts an example of the lower bound of the timeout value maintained by node A for the reception of Two hop ACK from node C. The timeout value should be greater than the estimated threshold (Th) value which can be calculated as follows

$$Th = T_2 - T_1 \tag{1}$$

where T_1 and T_2 are the sending (reception) time of the packet (ACK), respectively. This threshold is estimated for a successful transmission at MAC layer without any retransmission, which is not a realistic assumption in MANETs, thus the timeout value should satisfy the following condition

$$To > Th + (AVG\_RT \times 1\_hop\_delay) \tag{2}$$

where AVG_RT is the average number of retransmissions of a packet at MAC layer, and 1_hop_delay is the one hop transmission delay which includes packet transmission delay, random backoff delay at the MAC layer and the processing delay.

3) Reputation based schemes:

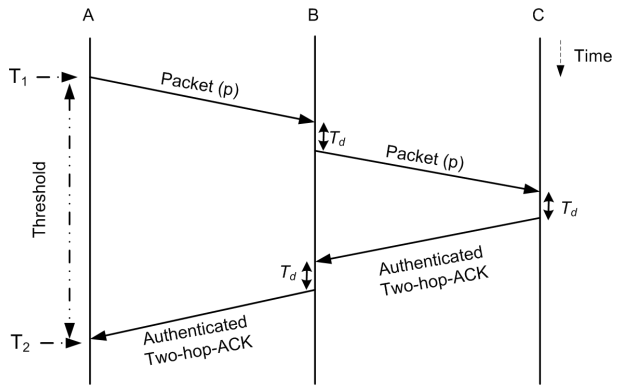
The reputation is the art of using historic observation about the behavior of a node to determine whether it is trustworthy or not. Each node must form an opinion regarding the other nodes based on their observed past behaviors. Then the nodes with low reputation are punished or avoided while establishing routes. The major drawback of this category is the excessive traffic exchange needed for sharing the reputation information between the nodes. Moreover, a serious vulnerability of reputation based schemes is the fact that any compromised node can send forged reputation information in order to decrease the trust level of some nodes. In what follows, we describe three representative schemes that use the reputation mechanism.

In [10], CONFIDANT protocol is introduced in order to secure source routing protocols against adversary nodes. This protocol aims to exclude the malicious nodes from participating to the route discovery phase and route the packets around them. The exclusion of these nodes is carried out using a dedicated reputation system. CONFIDANT consists mainly of the following elements: (i) the monitor, (ii) the reputation system, (iii) the trust manager, and (iv) the path manager. The role of the monitor is to ensure that each packet sent by a node is correctly forwarded by its next hop. This is achieved through the use of passive-feedback technique or by observing route protocol behavior. If an anomaly is detected, the node triggers an action via the reputation system. This latter manages a table containing the identifiers of all the known nodes and their corresponding rating. This rating is updated only if a sufficient evidence of misbehavior is acquired. In its turn, the trust manager is responsible for sending and receiving alarm messages that inform the nodes about the detected adversaries. Finally, the path manager is responsible for launching the adequate reaction and guarantees the establishment of safe routes.

CONFIDANT is suitable for small networks with low mobility; however it might be less efficient for large networks since each node needs to maintain a huge table for reputation purposes. Likewise, the high mobility of nodes increases significantly the communication overhead. Additionally, this protocol inherits all the problems of passive-feedback based schemes since it uses this mechanism for the monitoring function.

Another scheme based on reputation system is the so called Friend and Foes that has been proposed in [18]. This scheme aims to prevent the selfish nodes from disrupting the network operations by refusing to participate correctly to the forwarding process. Its idea is inspired from the society principle which says that people agree to cooperate as long as they notice that there is a fair tasks distribution in the group. This scheme seeks to reward the cooperating nodes and punish the selfish nodes which refuse to cooperate. In this scheme, each node A advertises the set of nodes to whom it is not willing to forward packets along with the set of its friends. To do so, node A classifies the network's nodes in three sets, which are periodically updated, as described below. The friend nodes set for which a node accepts to relay the packets, the enemy nodes set for which no service is provided and the selfish nodes set which consists of nodes known to act as node A is an enemy. When node A sends a packet it searches for a route in which the next hop is a friend node and whenever it is requested to forward a packet it does so only if the requester node is a friend. The major drawback of this scheme is the large number of packets exchanged to advertise the friends and enemies sets.

A sound scheme is introduced in [48], in which the authors have proposed a new anomaly detection system dubbed



T_d : (Processing + queuing) delay at nodes B and C

Fig. 10: TWO hop ACK threshold for minimum timeout

RADAR to detect anomalous mesh nodes in Wireless Mesh Networks (WMNs) [28]. The salient features of RADAR can be summarized as follows: (i) reputation is used to evaluate each node's behavior by abstracting and examining the appropriate observations, e.g. data packets, a secure and dependable reputation management mechanism is then used to define, quantify and propagate the trust values of each node, ensuring the robustness and accuracy of the normal profiles feeding to detection engine; (ii) two light-weight anomaly detectors were employed to capture the node's behavior drifts in terms of reputation by exploring their temporal and spatial properties respectively, and they were seamlessly coupled to achieve higher detection accuracy and lower false positive rate. Notice that RADAR was specified and implemented with DSR routing protocol in order to detect misbehaving nodes that violate routing mechanisms at the network layer. It is found efficient in detecting nodes, involved in packet drop and spoofing attacks.

4) Cross-layer cooperation based schemes:

Most of the existing solutions rely on the Watchdog technique to ensure the correct forwarding of packets by the neighboring nodes; however this technique suffers from certain weaknesses, particularly when power control is applied. In [40], the authors have proposed a low cost approach dubbed (SMDP) to circumvent the aforementioned drawbacks of Watchdog. They have designed a cross layer scheme that ensures higher detection accuracy. In this scheme, it is required that the routing protocol be aware of the beginning and end of each continuous traffic routed through it. This can be accomplished through cross-layer cooperation between network and session layers.

At the end of each session, every node involved in the forwarding path sends out two signed packets, one to each successor node containing the number of packets sent to it, and the other packet towards its predecessor node contains the number of packets received from it. According to the received packets, each node broadcasts to its one hop neighbors a special packet called Forwarding Approval Packet (FPA) as a proof of its cooperation. On receiving this packet the neighbors of the sender can judge whether this node has correctly forwarded the packets or not. The main advantage of this scheme is its high detection accuracy that significantly reduces the number of false alarms.

5) Other schemes:

In this section we give a brief overview of the major contributions which could not be affected to any of the previous classes.

The authors of [19] have proposed two solutions to cope with the black hole attack in AODV. In the first solution, it is required that the source node waits until receiving more than two RREPs after each broadcasted RREQ (i.e. multi path routing). Upon reception of these messages the source node checks any appearance of shared nodes between the identified routes. If a shared node is identified then the source node sends the data packets to the destination through multiple routes using different packet IDs and sequence numbers. Otherwise, no packet will be sent. Notice that the appearance of shared nodes between different routes is not a sufficient condition to guarantee their safety since a malicious node might be involved in several routes. Moreover, this solution generates additional computational overhead due to the extra processed RREPs. Besides, if no shared node is identified then the source node delays or abandons the transmission of the data packets, leading to a severe degradation of the network performance.

To circumvent these drawbacks a second solution has been proposed. This new solution exploits the packet sequence number to detect the malicious nodes trying to hijack the traffic flow. To this end, each node maintains two extra tables containing the sequence numbers of the last packets sent (received) to (from) every node in the network, respectively. Upon reception of a RREP packet, the source node that has initiated the RREQ compares the sequence number extracted from the RREP and the one saved in its table. If they match then the safe route is identified, otherwise the responding node is deemed as malicious. This solution is faster than the previous one, however a malicious node can easily analyze the traffic passing in its vicinity and update its tables by the adequate packet sequence number, thereby it avoids the detection scheme.

Since the mobility of nodes is the most apparent feature of ad hoc networks, the conventional schemes based on static training data might not be efficient to deal with the black hole attack in such environment. [45] provides an alternative proposal that takes into account the rapidly changing topology of the network. This proposal uses the destination sequence number as a metric to detect any deviation from the normal network state. This state is updated dynamically at regular time intervals in order to enhance the detection accuracy. A special component named *discrimination module of anomaly detection* is used to distinguish the normal states from the abnormal ones. Its role is to measure the amount of deviation and compare it to a predefined threshold to find out whether an attack is occurred in the path toward the destination. To conclude, this scheme is effective to deal with the black hole attack in highly mobile networks however the update interval is a critical metric that should be assigned an appropriate value that ensures a better accuracy and performance.

In addition to the herein presented contributions, the reader may refer to the following papers to enrich its knowledge regarding the packet dropping attack [51], [46], [31], [37] and [33].

C. Discussion

As described in Fig. 11, most of the solutions in different defense lines are routing layer dependent but cooperation with session layer would improve the detection rate as stated in [40]. Furthermore, since packets might be dropped due to MAC protocol rules as illustrated in section II, an additional diagnostic provided by MAC layer remains a key component for a robust detection scheme. This cooperation may significantly reduce the false alarms by discerning normal behavior from the malicious one (i.e. the inter-layer attack described in section III-B).

A summary of the characteristics of the surveyed schemes is presented in Table IV. In this table, we emphasize the most prominent features of each scheme in terms of its robustness, scalability, induced overhead and the reaction mechanism adopted to exclude the detected attackers. Moreover, this table allows us to identify the strong and weak points of each scheme in order to develop an eventual hybrid solution that merges two or more schemes, from different defense lines, together to ensure a perfect protection against the packet droppers. The features of each scheme are highlighted based on the following metrics:

- The defense line to which the scheme belongs.
- Its robustness against the collusive black hole attack, in which two or more nodes collude to launch the attack.
- The additional overhead generated by the scheme in terms of the new packets sent and the extra computations required to carry out the scheme.
- The impact of the scheme on routing protocol's performance such as end-to-end delay and packet delivery ratio.
- Is the scheme providing any reaction technique to penalize the detected attackers?
- Is the scheme scalable to large networks? i.e. whether the scheme maintains its efficiency when the network becomes larger and dense.
- The architecture of the scheme: centralized, distributed or stand-alone; defined as follows:

  Centralized: the core part of the scheme is running on an unique supervisor node which monitors the whole network and the rest of nodes need to report to the supervisor node for information processing.

  Distributed: all the nodes run the same scheme and exchange information between each other.

  Stand-alone: similarly, each node runs the same scheme however the communication between nodes is not necessary.

Another summary of the main assumptions and limitations of each class of the schemes studied throughout the paper is provided in Table V. As we can see from this table all these approaches are built on a set of assumptions that are either unrealistic or hard to achieve in a hostile environment like MANETs. Hence these assumptions limit the applicability of these approaches to some specific network configurations and constitute their major drawbacks.

V. Challenges

As discussed in the previous sections, most of the proposed solutions are built on a number of assumptions which are either hard to realize in a hostile and energy constrained environment like MANETs or not always available due to the network deployment constraints. Moreover, these solutions are generally unable to launch a global response system whenever a malicious node is identified. In contrast, they either punish the malicious node locally without informing the rest of the network or divulge its identity to the network through costly cryptographic computations. Moreover, even though the malicious node is punished in a part of the network it can move to another part and continues causing damage to the network until it is detected again. Due to these reasons, many challenges have to be carefully considered in order to design a robust solution to cope with the packet dropping attack. These challenges can be summarized as follows. First, the attackers' behaviors are tailored to the specific routing protocol, making it impossible to build a general model for characterizing the attacker. Secondly, how to use this model to achieve a high-level resistance against these attacks while maintaining network performance. Recently, most of the proposed solutions are focused on adding new components to the original protocol to assess the deviation of the neighboring nodes and monitor their behaviors. However the use of these additional components might remove an important performance optimization. A simple way to secure MANETs against the increasing threat of the packet droppers without affecting their performance is to take into account the security metric at an earlier stage of the design process of routing protocols. This new design process could be similar to the co-design technique used for developing the embedded systems. A complementary way to achieve the best trade-off between security and performance is to aggregate the three defense lines discussed in this paper to guarantee the cooperation of nodes in the network.

VI. Conclusion

In this paper we have presented a survey of the state of the art on securing MANETs against packet dropping attack. The attack schemes, as well as prevention, detection and reaction mechanisms have been explored. We categorized them into three categories according to their goals and their specific strategies. A comparative study between them was then conducted to highlight their respective effectiveness and limitations. We concluded that most of the proposed schemes in the first, second or third defense line are based upon certain assumptions that are not always valid due to the dynamic nature of MANETs and their specific characteristics. Many researchers have been motivated to apply game theory to enforce nodes cooperation in MANETs, such as the works done in [24] and [34], by examining its similarities with the social behavior of human in a community. These works assume that a node tries always to maximize its benefit by choosing

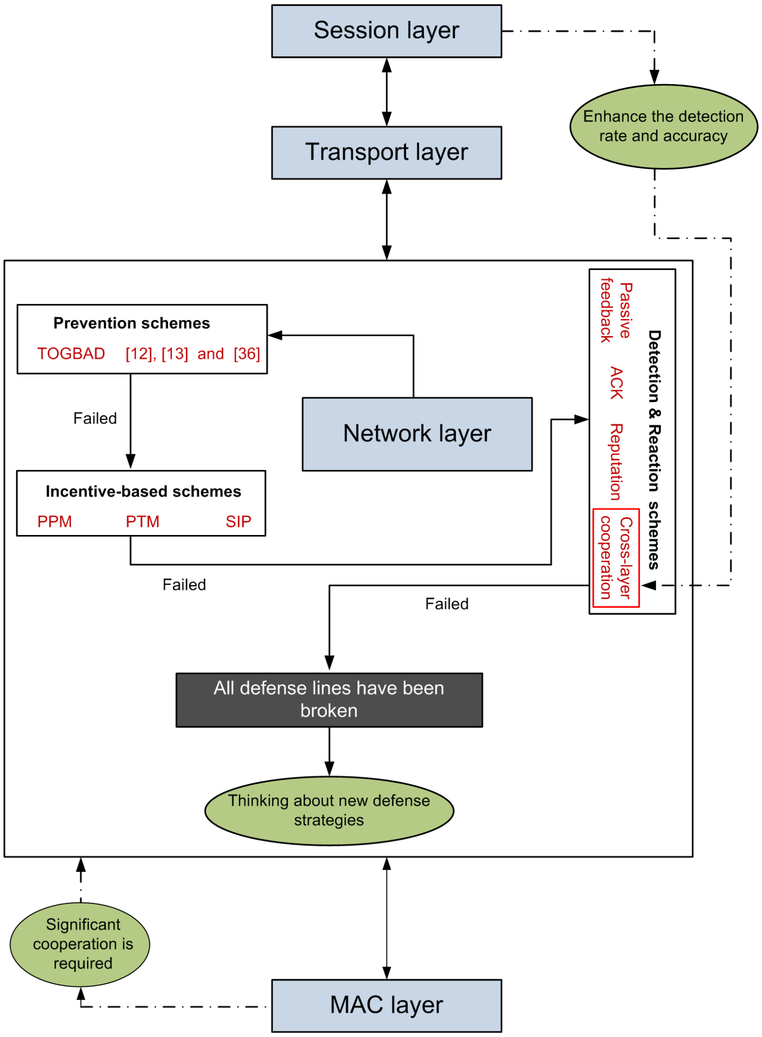

Session layer
Enhance the detection rate and accuracy
Transport layer
Prevention schemes
TOGBAD [12], [13] and [36]
Failed
Network layer
Incentive-based schemes
PPM PTM SIP
Failed
Detection & Reaction schemes
Passive feedback
ACK
Reputation
Cross-layer cooperation
Failed
All defense lines have been broken
Thinking about new defense strategies
Significant cooperation is required
MAC layer

Fig. 11: A holistic perspective on the defense lines against packet dropping attack

whether to cooperate in the network or not. However, those works are generally based on the assumption that the majority of the nodes are misbehaving, which is not an usual case in MANETs. We believe it is an interesting and significant topic for further exploration with more realistic assumptions, especially tailored for packet dropping attack.

References

[1] A. Shamir, How to Share a Secret, *Communications of the ACM*, 22(11): 612-613, November 1979.

[2] L. Lamport, Password Authentication with Insecure Communication, *Communications of the ACM*, 24(11): 770-772, November 1981.

[3] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, *CRC Press*, October 1996.

[4] IEEE 802.11 wireless LAN media access control (MAC) and physical layer (PHY) specifications, ANSI/IEEE Std 802.11, 1999.

[5] D. B. Johnson and D. A. Maltz, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft), Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.

[6] S. Marti, T. J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, *In Proc. of the* 6^{th} *annual international conference on Mobile computing and networking (MOBICOM '00)*, Boston, Massachusetts, USA, August 2000.

[7] B. Schneider, Secrets and Lies. Digital Security in a Networked World, John Wiley & Sons, inc, 1^{st} edition, 2000.

[8] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes, PGP in constrained wireless devices, *In Proc. of the* 9^{th} *USENIX Security Symposium* ,Denver, Colorado, August 2000.

[9] L. Buttyan and J. P. Hubaux, Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Mobile Ad Hoc Networks, Swiss Federal Institution of Technology, Lausanne, Switzerland, Tech. Rep. DSC/2001/001, January 2001.

[10] S. Buchegger and J. Y. Le Boudec, Performance Analysis of the CONFIDANT Protocol, *In Proc. of the* 3^{rd} *ACM International Symposium on Mobile Ad Hoc Networking & computing (MOBIHOC'02)*, Lausanne, Switzerland, June 2002.

[11] Y. C. Hu, A. Perrig and D. B. Johnson, Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks, *In Proc. of the* 8^{th} *ACM International Conference on Mobile Computing and Networking* , Westin Peachtree Plaza, Atlanta, Georgia, USA, September 2002.

[12] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless ad hoc networks, *IEEE Communication Magazine*, 40(10): 70-75, October 2002.

[13] B. Sun, Y. Guan, J. Chen and U. W. Pooch, Detecting black- hole attack in mobile ad hoc networks, *In Proc. of the* 5^{th} *European Personal Mobile Communications Conference*, Glasgow, UK, April 2003.

[14] C. Perkins, E. Belding-Royer and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, *IETF RFC 3561 (Experimental)*, July 2003.

[15] W. Mao, Modern Cryptography: Theory and Practice, *Prentice Hall publisher*, July 2005.

[16] T. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), *IETF RFC 3626 (Experimental)*, October 2003.

[17] A. Patcha and A. Mishra, Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks, *In Proc. of Radio*

TABLE IV: Characteristics of the surveyed schemes

	Characteristics							
	Defence line	**Defense against the collusive attack**	**Computation overhead**	**Communication overhead**	**Latency**	**Scalability**	**Punishment**	**Architecture**
Watchdog [6]	3^{rd}	N	Low	N	N	Y	N	Distributed
CONFIDANT [10]	3^{rd}	N	Low	Low	N	Y	Y	Distributed
H. Deng 1 [12]	1^{st}	N/A	N	N	N	Y	N	Distributed
H. Deng 2 [12]	1^{st}	N	Low	Low	Y	Y	N	Distributed
B. Sun [13]	1^{st}	N/A	Low	Medium	High	Y	N	Distributed
TOGBAD [43]	1^{st}	N/A	Very high at the supervisor node	N	N	Y	N	Centralized
Friend & Foes [18]	3^{rd}	N/A	Low	High	High	N	Y	Distributed
Al-Shurman Scheme1 [19]	N/A	N	Low	Medium	High	N	N	Stand-alone
Al-Shurman Scheme2 [19]	N/A	N/A	Low	N	Low	N	N	Stand-alone
Nuglets (PPM) [9]	2^{nd}	N/A	Low	N	N	N	Y	Stand-alone
Nuglets (PTM) [9]	2^{nd}	N/A	Low	N	Low	N	Y	Stand-alone
SIP [44]	2^{nd}	N/A	Low	low	Low	Y	Y	Stand-alone
SA-OLSR [49]	3^{rd}	N/A	Low	High	N	Y	N	Stand-alone
B. Kannhavong [36]	1^{st}	N/A	Low	N	N	Y	N	Stand-alone
Nidal et al [39]	3^{rd}	N/A	Low	Low	N	N	N	Distributed
SMDP [40]	3^{rd}	N	Medium	Medium	N	N	N	Distributed
K. liu [38]	3^{rd}	N	Low	Low	N	Y	N	Stand-alone
S. Ramaswami [32]	3^{rd}	Y	Low	Low	N	Y	Y	Distributed
Two hop Ack [27]	3^{rd}	N	High	High	N	N	N	Stand-alone
Random Two hop Ack [30]	3^{rd}	N	Low	Low	N	Y	N	Distributed
Three hop Ack [50]	3^{rd}	Y	Medium	Low	N	Y	N	Distributed
RADAR [48]	3^{rd}	N	Low	Low	N	Y	Y	Distributed

and Wireless Conference (RAWCON '03), Boston, Massachusetts, USA, August 2003.

[18] H. Miranda and L. Rodrigues, Friends and Foes: Preventing Selfishness in Open Mobile Ad hoc networks, *In Proc. of the 23^{rd} International Conference on Distributed Computing Systems Workshops (ICDCSW'03)*, Providence, RI, USA, May 2003.

[19] M. Al-Shurman, S. M. Yoo and S. Park, Black Hole Attack in Mobile Ad Hoc Networks, *In Proc. of the 42^{nd} Annual Southeast Regional Conference (ACMSE'04)*, Huntsville, ALabama, USA, April 2004.

[20] M. Jahnke, J. Tolle, M. Bussmann, and S. Henkel, Components for Cooperative Intrusion Detection in Dynamic Coalition Environments, *In Proc. of NATO/RTO IST Symposium on Adaptive defense in Unclassified Networks*,Toulouse, France, April 2004.

[21] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, *IEEE Security & Privacy*, 2(3): 28-39, May 2004.

[22] M. Fischlin. Fast verification of hash chains, *In Proc. of the RSA Security Cryptographer's Track, CT-RSA 2004 : topics in cryptology* , San Francisco CA, February 2004.

[23] W. Yu, Y. Sun and K. R. Liu, HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks, *In Proc. of the 24^{th} IEEE INFOCOM*, Miami, USA, March 2005.

[24] E. Altman, A. Kherani, P. Michiardi and R. Molva , Non cooperative forwarding in ad hoc networks, *In Proc. of the 4^{th} IFIP International Conferences on Networking*, Waterloo, Canada, May 2005.

[25] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, Authenticated routing for ad hoc networks, *IEEE Journal on Selected Areas in Communications*, 23(3): 598-610, March 2005.

[26] D. Djenouri, L. Khelladi and N. Badache, A survey of Security Issues in Mobile Ad Hoc and Sensor Networks, *IEEE Communications Surveys & Tutorials*, 7(4): 2-28, Fourth Quarter 2005.

[27] D. Djenouri and N. Badache, New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks, *In Proc. of Workshop of the 1^{st} International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecurComm'05)*, Athens, Greece, September 2005.

[28] I. F. Akyildiz and X. Wang, A Survey on Wireless Mesh Networks, *IEEE Communications Magazine*, 43(9), S23-S30, September 2005.

[29] P. Argyroudis and D. O'Mahony, Secure Routing for Mobile Ad Hoc

TABLE V: A comparison on the different approaches: assumptions and drawbacks

	Main assumptions	**Limitations**
Passive Feedback based schemes	Promiscuous mode operation is mandatory No collusion amongst nodes	Inherits all the Watchdog's drawbacks
ACK-based schemes	Authentication mechanism is deployed The requested node always sends back the intended Acknowledgement	Huge overhead generated due to the extra Acknowledgment packets sent. Decision ambiguity if the requested node refuse to send back an Acknowledgment.
Reputation-based schemes	Preestablished list of friend (trusted) nodes	Overhead induced in sharing reputation information amongst the nodes
Incentive-based schemes	Tamper resistant hardware is mandatory for the operations of this category of solutions.	Legitimate nodes might be punished indirectly due to their location in the network. A node can sell the same packet several times to earn more money.

Networks, *IEEE Communications Surveys & Tutorials*, 7(3): 2-21, Third Quarter 2005.

[30] D. Djenouri and N. Ouali and A. Mahmoudi and N. Badache, Random Feedbacks for Selfish Nodes Detection in Mobile Ad Hoc Networks, *In Proc. of the 5th IEEE International Workshop on IP Operations and Management (IPOM'05)*, Barcelona, Spain, October 2005,

[31] V. Balakrishnan, V. Varadharajan and U. K. Tupakula, Fellowship: Defense against Flooding and Packet Drop Attacks in MANET, *In Proc. of the 10th IEEE/IFIP Network Operations and Management Symposium (NOMS 2006)*, Vancouver, Canada, April 2006.

[32] S. S. Ramaswami and S. Upadhyaya, Smart handling of Colluding black Hole attacks in MANETs and Wireless Sensor Networks using Multipath Routing, *In Proc. of the Workshop on Information Assurance*, United States Military Academy, West Point, NY, 21-23 June 2006.

[33] Y. R. Tsai and S. J. Wang, Two-tier authentication for cluster and individual sets in mobile ad hoc networks, *Computer Networks*, 51(3): 883-900, February 2007.

[34] Z. Ji, W. Yu and K. J. Ray Liu, Cooperation Enforcement in Autonomous MANETs under Noise and Imperfect Observation, *In Proc. of the 3rd Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (IEEE SECON)*, Reston, VA, USA, September, 2006.

[35] Tolle, M. Jahnke, N. gentschen Felde, and P. Martini, Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System, *In Proc. of the 25th Military Communications Conference (MILCOM 2006)*, Washington, DC, October 2006.

[36] B. Kannhavong, H. Nakamaya and A. Jamalipour, A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks, *In Proc. of the Global Communications Conference (GLOBECOM '06)*, San Francisco, California, USA, Nov/Dec 2006.

[37] C. Basile, Z. Kalbarczyk and R. K. lyer, Inner-Circle Consistency for Wireless Ad Hoc Networks, *IEEE TRANSACTIONS ON MOBILE COMPUTING*, 6(1): 39-55, January 2007.

[38] K. liu, J. Deng, P. K. Varshney and K. Balakrishnan, An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs, *IEEE TRANSACTIONS ON MOBILE COMPUTING*, 6(5): 536-550, May 2007.

[39] N. Nasser and Y. Chen, Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks, *In Proc. of the Internationl Conference on Communication (ICC 07)*, Glasgow, June 2007.

[40] T. Fahad, D. Djenouri and R. Askwith. On detecting Packets Droppers in MANET: A Novel Low Cost Approach, *In Proc. of the 3rd International Symposium on Information Assurance and Security*, Manchester, UK, August 2007.

[41] X. Wu, D. K. Y. Yau, Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach, *In Proc. of the 3rd International Conference on Security and Privacy in Communications Networks*, Nice, France, September 2007.

[42] T. R. Andel and A. Yasinsac, Surveying Security Analysis Techniques in MANET Routing Protocols, *IEEE Communications Surveys & Tutorials*, 9(4): 70-84, Fourth Quarter 2007.

[43] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle. Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, *In Proc. of the 33rd IEEE Conference on Local Computer Networks (LCN)*, Dublin, Ireland, October 2007.

[44] Y. Zhang, W. Lou, W. Liu and Y. Fang, A secure incentive protocol for mobile ad hoc networks, *Wireless Networks journal*, 13(5): 569-582, October 2007.

[45] S. Kurosawa, H. Nakayama, N. Kato, A. jamalipour and Y. Nemoto, Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamuic Learning Method, *International Journal of Network Security*, 5(3): 338-346, November 2007.

[46] P. Agrawal, R. K. Ghosh and S. K. Das, Cooperative black and gray hole attacks in mobile ad hoc networks, *In Proc. of the 2nd International Conference on Ubiquitous Information Management and Communication (ICUIMC 2008)*, SKKU, Suwon, Korea, Jan/Feb 2008.

[47] M. Amitabh, Security and quality of service in ad hoc wireless networks, *Cambridge University Press*; 1st edition, March 2008.

[48] Z. H. Zhang, F. Naït-abdesselam, P. H. Ho and X. Lin, RADAR: a ReputAtion-based scheme for Detecting Anomalous nodes in wiReless mesh networks, *In Proc. of the IEEE Wireless Communications and Networking Conference (WCNC2008)*, Las Vegas, USA, March 2008.

[49] B. Kannhavong, H. Nakamaya, Y. Nemoto, N. Kato and A. Jamalipour, SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks, *In Proc. of the International Conference of Communication (ICC 2008)*, beijing, China, May 2008.

[50] S. Djahel, F. Naït-Abdesselam and A. Khokhar, An Acknowledgment-Based Scheme to Defend against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol, *In Proc. of the International Conference on Communication (ICC 2008)*, beijing, China, May 2008.

[51] Z. Li, C. Chigan and D. Wong, AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs, *In Proc. of the Global Communications Conference (IEEE GLOBECOM 08)*, New Orleans, LA, USA, NOV/DEC 2008.

Soufiene Djahel is pursuing his PhD at University of Lille1 since October 2007. Prior to that, he was an engineer researcher at INRIA Lille Nord Europe research center, from July to December 2007. He has obtained his engineer degree in computer science and a magister degree in networking and distributed systems from University Badji Mokhtar of Annaba and University Abderrahmane Mira of Bejaia in 06/2004 and 02/2007, respectively. The research interests of Soufiene Djahel lie in the field of security in wireless multihop networks, particularly he focuses on securing routing protocols and MAC layer misbehavior issues. He is reviewer of many conferences and journals in the networking and security field. Soufiene Djahel is an IEEE and IEEE ComSoc student member.

Farid Naït-abdesselam obtained his engineering degree in computer science from University of Sciences and Technologies Houari Boumediene(USTHB) Algiers, Algeria, in 06/1993 and a master degree in computer science from University of Paris Descartes - France, in 09/1994. After two years spent in the industry working as a software engineer, he joined the University of Versailles Saint Quentin, (UVSQ) France in 01/1996, and got his PhD degree in computer science in 01/2000. During the year of 1998, he worked as an associate researcher at University of Western Ontario, London Ontario Canada, on distributed interactive virtual environment and multimedia communications over ATM networks. From 09/1999 to 08/2000 he was an assistant professor at University of Sciences and Technologies of Lille - France. From 09/2000 to 08/2003 he worked as an associate professor at INSA of Lyon and a research member of INRIA Rhne Alpes. Since 09/2003 he is an associate professor at University of Sciences and Technologies of Lille and till 09/2007 a research member of the INRIA Lille Nord Europe. His research interests lie in the field of computer and communication networks with emphasis on architectures and protocols for quality of service and security in IP based networks, mobile ad-hoc, sensor, vehicular, and mesh networks, and overlay networks. Farid Naït-abdesselam is on the editorial board of Wiley Int. J. of Communication Systems, Int. J. of Internet Protocol Technology, Int. J. of Ad Hoc and Ubiquitous Computing and Int. J. of Computer Networks and Distributed Systems. He has been on the technical program committee of different IEEE and ACM conferences, including GLOBECOM, ICC, LCN, and MSWiM, and regularly invited to chair some of their sessions. He is chairing/has chaired the IEEE International Workshop on Wireless Local Networks, the IEEE/ACS International Workshop on Internet Services, and the International Workshop on Peer to Peer Networking. He has served as Editorial Liaison chair of the IEEE LCN Conference, and publicity co-chair of many conferences. Farid Naït-abdesselam is a member of the IEEE, IEEE Communications Society, and IEEE Computer Society.

Zonghua is an associate professor of Institut TELECOM/TELECOM Lille1, France. Previously, he was an expert researcher at the Information Security Research Center of NICT, Japan from April, 2008 to April, 2010. Even earlier, he spent two years for post-doc research at the University of Waterloo, Canada and INRIA, France after earning his Ph.D. in information science from Japan Advanced Institute of Science and Technology (JAIST) in March of 2006. Zonghua also obtained a M.Sc. degree in computer science and a B.Sc. degree in information science from Xidian University, China in 2003 and 2000 respectively. His research embarked on Elliptic Curve Cryptography and security evaluation, and is now focused on network forensics analysis and reputation/security management.