A Wireless Intrusion Detection System for Secure Clustering and Routing in Ad Hoc Networks

Luciano Bononi and Carlo Tacconi

Department of Computer Science, University of Bologna, Mura Anteo Zamboni 7, 40127, Bologna, Italy
{bononi,ctacconi}@cs.unibo.it

Abstract. Intrusion detection and secure routing schemes have been proposed for increasing the security and reliability in critical scenarios like mobile ad hoc networks. In this paper we present an integrated secure routing system based on Intrusion Detection Systems (IDS) and SUCV (Statistically Unique and Cryptographically Verifiable) identifiers. The proposed IDS has been used for the support of secure AODV routing, named IDS-based Secure AODV (IS-AODV), in a wireless ad hoc network scenario. Our IDS solution is based on the detection of behavior anomalies on behalf of neighbor hosts, with passive reactions, aiming to create a *cluster* whose route paths will include only safe nodes, eventually. We implemented a simulation model to test the effects and overheads of the proposed IDS scheme when defending the AODV routing functions. Results show that the proposed IDS is effective in isolating byzantine hosts, and it assists the AODV secure routing scheme to converge in finding end-to-end safe routes.

Key words: Intrusion Detection System, Secure Routing and Clustering, Statistically Unique and Cryptographically Verifiable Identifiers, Mobile Ad Hoc Networks

1 Introduction

In Mobile Ad Hoc Networks (MANETs) the set of dynamically interacting mobile hosts should cooperate and share wireless capabilities and resources to enable end-to-end communication. Intermediate hosts act like routers to extend the connectivity of peer-devices located out of the radio-communication range of each other.

This is obtained by effectively relaying messages in a multiple hop transmission sequence, along a dynamically determined routing path of radio links. The MANET scenario is widely considered a stressing scenario for routing protocols, due to hosts' mobility, which may cause frequent route updates and link failures. Several multi-hop routing protocols like for ad hoc networks have been proposed: most popular examples include DSR [4], OLSR [2], DSDV [3], AODV [5]. A majority of these protocols relies on the assumption of a trustworthy cooperation among all participating devices: unfortunately, this may not be a realistic assumption in real systems. Malicious nodes could exploit inherent characteristics of MANETs to launch various kinds of attacks. Conventional methods and infrastructures for hosts' identification and authentication may not be available on MANETs, since the availability of a Certification Authority (CA) or a Key Distribution Center (KDC) cannot be always assumed over dynamic and infrastructureless networks.

Many *Intrusion Detection System* (IDS) solutions have been proposed for wired networks, based on monitoring of realtime traffic at statically defined strategic points: switches, gateways, and routers. In MANETs, nodes' mobility cannot be restricted in order to let the IDS to operate or collect data.

Security solutions have been proposed at the routing layer in MANETs. As an example, *Secure Routing* schemes have been designed to incorporate security features into routing protocols. Secure routing protocols are either completely new or, in some cases, they can be seen as security mechanisms embedded into existing routing protocols, like the popular AODV and DSR. Several architectures and detection mechanisms for realizing integrated IDSs and secure routing protocols have been proposed for MANETs. They will be sketched in the related works section II.

In this paper, we illustrate the design of a secure routing protocol (based on AODV), called IDS-based Secure AODV (IS-AODV), implemented by adopting an IDS solution and the concept of *Statistically Unique and Cryptographically Verifiable* (SUCV) identifiers [20] [21], for IPv6-based MANETs. IS-AODV is based on SUCV and mutual verification of nodes behaviors during the path creation processes. SUCV identifiers are used to realize a secure binding between IPv6 addresses and cryptography keys, without requiring any trusted CA or KDC.

To the best of our knowledge, different solutions incorporating the same concepts have been proposed in SecAODV [22] concerning the SUCV adoption, and in the *watchdog* solution [9], concerning the *mutual verification* concept.

IS-AODV is basically different from secAODV [22], because it uses the IDS as the basis for implementation of secure AODV routing. In order to control the behavior of neighbors during the route discovery and data forwarding phases, in IS-AODV each node monitors the traffic whose path includes the node itself. Unlike SecAODV, when a node N perceives a suspect behavior from a neighbor host, the IDS reaction in IS-AODV is *passive*, that is, the information about the possible node corruption is not advertised to other nodes. As a reaction, the node N does not rely, and does not assist any suspect neighbor node in the implementation of routing and communication. In this way, as long as malicious nodes are present, only safe routes will survive in the route creation and route maintenance processes, and a *cluster* would emerge that will eventually include only safe nodes. In addition, unlike secAODV, the proposed IS-AODV scheme does not require any cryptography operation in the *intermediate* nodes.

IS-AODV is different from the *watchdog* solution proposed in [9], because our mechanism is designed to defend a Distance Vector routing protocol (like AODV), while the watchdog is created to defend a Source Routing protocol (like DSR). Basically, the watchdog system must know where a packet will be in two hops: this information is present in packets managed with the DSR protocol, but not with distance vector protocols, like AODV. For this reason, to implement the mutual verification under AODV, our IS-AODV mechanism introduces one low-overhead additional field for standard AODV Route Request (RREQ) and Route Reply (RREP) messages (see section 3.3). In addition, a public key cryptography (or more lightweigth symmetric cryptography, after a safe path is found), is used to verify the signature added in routing and data packets, by end-nodes only. This allows the end-to-end check to detect if at least a corrupted node in the path has modified packets (to be discarded). Unlike the watchdog mechanism, IS-AODV don't expliciteły accuse a node if it drops a packet: *i)* because a packet drop behavior may happen due to collisions, and *ii)* because the node that realizes a drop-attack would be self-excluded from the path creation process. Moreover, when a misbehaving node is found, IS-AODV adopts a passive reaction, while the watchdog mechanism sends an explicit message to the path source to notify the presence of unsafe nodes. To conclude, IS-AODV is different with respect to the proposed cooperation enforcement schemes like CORE [18] and CONFIDANT [19], because *i)* IS-AODV is realized to defend a Distance Vector protocol like AODV, *ii)* the information about corrupted or safe nodes is not advertised to other nodes and *iii)* the spoofing attack has not critical effects (see Appendix A: IP attack). The effect of MAC layer collisions on IS-AODV is discussed in section 4.

The paper structure is the following: in Section 2 we illustrate the state of the art in secure routing protocol solutions and IDSs, in Section 3 we illustrate the design, implementation and assumptions of the proposed IDS mechanism, in Section 4 we illustrate a simulation model and results obtained, and in Section 5 we draw some conclusions. In the Appendix (and in [24]) we sketch discussion and solutions to possible attacks considered for this system.

2 Related Works

2.1 Secure Routing Protocol

Recent solutions for implementing secure routing protocols and IDSs over MANETs can be found in this section.

The Secure Routing Protocol (SRP) proposed in [14] is based on DSR protocol [4], and contrasts the malicious behavior that may be originated by the discovery process of topological information. The basic assumption of SRP is that any two *end-to-end* nodes of a communication process would have a preliminary security association. Accordingly, SRP does not require: *i)* that any of the *intermediate* nodes perform cryptography operations, and *ii)* that intermediate nodes have a prior security association with the end nodes. ARIADNE [15] is a secure on-demand routing protocol that relies on highly efficient *symmetric* cryptography solutions. The ARAN [16] mechanism prevents modification, impersonation and fabrication attacks through the implementation of message authentication, integrity and non-repudiation mechanisms. SEAD [17] supports DSDV routing [3], and it is a robust solution against multiple uncoordinated attackers aiming to create incorrect routing information in other nodes. The protocol uses efficient *one-way hash functions* and it does not use asymmetric cryptography operations.

2.2 Intrusion Detection Systems

In [9], two techniques to improve throughput in ad hoc networks are described: *i)* in an effort to enforce the node cooperation, and *ii)* to detect the presence of byzantine nodes that fails to forward packets. The proposed solution is based on the implementation of *watchdogs* that identify misbehaving nodes, and a *pathrater* that helps end-nodes to avoid malicious nodes in the routing path choice. In [10] nodes are classified into *trusted* and *ordinary* nodes, and a watchdog mechanism is executed on the trusted nodes. Every node that subsequently joins the network has to prove its trustworthiness to be admitted to the trusted group. The main assumption in [10] is that any node will always behave in trusted or malicious way, undefinitely. In [6], an IDS prevents attacks by implementing an Intrusion Detection Module (IDM) and an Intrusion Response Module (IRM). The IRM is based on a local counter (for every node i) $C_{i,j}$ respectively associated to any other neighbor node j, that is incremented whenever a malicious act of node j is encountered. When the $C_{i,j}$ value reaches a predefined threshold then the suspect-warning about the node j is actively propagated to the entire network by node i. In [11], individual IDS agents are placed on every node, to monitor all local activities (including user and system side activities). When an IDS agent detects a local intrusion, it initiates a global response: all IDS agents will cooperatively participate in global intrusion detection actions to isolate the corrupted node. In [12] the system uses *Network Monitors* distributed on a subset of selected nodes into the network, to detect attacks against AODV routing. In [13] the system uses an IDS based on neighbor node's snooping of packets transmissions: a node hearing two consecutive transmissions, along the path from source to destination, checks that the packet and its route information is not modified in flight by malicious nodes. This approach uses two modes of operation: *i) passive* (to protect a single host from attacks), or *ii) active* (to cooperatively protect the nodes of an ad hoc cluster). In [22], a secure routing protocol based on AODV and IPv6 is proposed. It includes the SUCV mechanism (like in [25]) for non-repudiation and authentication, and it does not require the availability of a CA or KDC. RREQ and RREP packets have been extended by adding the RSA public key of the source node and the digital signature of the routing message. Upon receiving an RREQ message, each intermediate node authenticates the source node, by verifying the message integrity and by verifying the signature with the source node's public key. In this solution, the routing protocol and the IDS can be considered independent to each other. Each node (out of the route path) monitors the traffic activity within the radio range, to detect intrusions, determined as anomalous behavior of observed nodes.

3 The security system design

At the network layer, we can assume that a MANET is defined as the set of cooperating nodes adopting a common routing protocol. Under this assumption, it is possible for safe nodes to assume the routing protocol specification as a common set of guidelines representing the *normal behavior*. Every node diverging from the normal behavior is locally considered *unsafe*. So, the proposed *anomaly-based detection mechanism* allows the detection of many types of attacks, by defining an attack or anomalous behavior as *"a different behavior than the one defined by homogeneous protocol specifications"*.

3.1 System components and definitions

The security system mechanism presented in this work to support a secure routing solution for the AODV protocol, is based on two main components:
1) the Intrusion Detection System (IDS), which is based on *host and anomalies detection* with *passive* reaction.
2) the Statistically Unique and Cryptographically Verifiable (SUCV) identifiers, to ensure a secure binding between IPv6 address and public key, without requiring any CA or KDC.

If a safe route between two safe end-points exists, the aim of our mechanism is to find that route, eventually. On the other hand, the secondary aim of our scheme is to create an emerging cluster of safe nodes. To realize such aims, the first point is the safe route construction and maintenance process. This is obtained by exploiting:
i) the AODV definition (of RREQ and RREP phases),
ii) the end-to-end authentication of source and destination nodes. This authentication is obtained by adopting a Public Key Cryptography scheme, where keys are bound to node identities by means of a SUCV mechanism,
iii) the end-to-end signature verification for routing and data packets, to detect any malicious activity by corrupted nodes appearing in the originated path,
iv) the IDS-based mutual observation and control of routing and data transmissions between neighbor hosts, to detect behavior anomalies.

To summarize, during a path-discovery process, each node belonging to the forming-path monitors the routing or data packets forwarded by other nodes, within one-hop distance, to detect anomalous behaviors. When the number of behavior anomalies exceeds a predefined threshold (see section 3.4) , the observed node is considered corrupted by the observer. In this case, the IDS reaction is *passive*, that is, the information about host corruption is not advertised to neighbor nodes. As a reaction, the accused node is not trusted and not assisted (undefinitely or temporarily, see 3.4) by the accusing node. The choice to adopt **passive reactions** against malicious nodes is motivated because *active* reactions would require some kind of distributed majority (voting or ranking) procedure. This procedure may be very expensive, due to high number of service messages. In addition, all voting messages would need authentication obtained by cryptography operations. In absence of authentication, corrupted nodes could bias the majority or, under some scenarios, they could coordinate themselves to locally attack and control the voting process, and to accuse safe nodes. For these reasons, we decided to adopt the *passive* reaction, based on the "trust nobody" assumption: every safe node aims to create a *secure cluster* by exploiting only local (implicitly trusted) information obtained by sniffing packets forwarded by one-hop neighbors. After the creation and maintenance of the secure path between end-nodes, the data confidentiality, integrity, and authentication can be implemented by a more lightweigth symmetric cryptography scheme.

In general, IS-AODV is independent by the cryptography schemes adopted: as an example, one-way hash functions (like MD5 or SHA-1) could be used for SUCV IDs, public key cryptography scheme (like ECC or RSA) and the symmetric cryptography scheme (like AES or DES) can be freely adopted according to the system, network and application requirements.

3.2 Design goals and system assumptions

The proposed security system is realized to achieve the following objectives. As described in [1], an IDS for ad hoc networks:
g1) should not introduce new weaknesses in the system, that is it should ensure self-integrity without enabling new attack directions;
g2) should need few system resources and should not degrade the system performances by introducing significant computation and communication overheads;
g3) should be always on in background, transparently to the users.
In addition, under the routing viewpoint, we define the additional objectives:
g4) end-to-end communications are performed only on safe routes: a safe route is a path realized by safe nodes, connecting two safe end-points;
g5) if a safe route exists between two safe end-points, it will be adopted, eventually;
g6) a cluster composed by safe nodes transparently emerges as a side effect of the IDS passive reactions: that is, without propagating any information about the node corruption;
g7) no need for cryptography operations in the intermediates nodes: only end-points implement cryptography functions (like in transport/application level services). This choice saves energy resources and increases communication efficiency in the system (see *g2*). This is even more important for battery-based and low computation-power portable devices;
g8) no need to identify the attack type, if any: the system activity simply preserves correct routing protocol specifications;
g9) support for end-to-end authentication, confidentiality and *integrity.*

The following assumptions are the basis for the proposed mechanism realized in a MANET environment:
a1) At the routing viewpoint, the end-points of a communication (source S and destination D) are implicitly safe;
a2) every link between the participating nodes is bidirectional;
a3) nodes operate in promiscuous mode at the MAC layer, meaning that nodes can listen to their neighbours' transmissions;
a4) all safe nodes have the IDS activated, unless they may be considered as malicious nodes;
a5) all system nodes (both safe and malicious ones) know a pre-defined one-way hash function, which characterize the MANET;
a6) the MANET is implicitly homogeneous under the AODV routing protocol viewpoint.

3.3 System Overview

In general, AODV [5] is based on two reactive transmission phases: the Route Discovery and Route Reply phases. When a source S wants to send a packet to a destination D and the routing path is unknown, a Route Discovery phase is initiated, by flooding Route Request (RREQ) broadcast packets. Every intermediate node inserts its own IP address in the IP header when propagating the RREQ (RREP) packets, so the next-hop receiver would know the previous node propagating the RREQ (RREP). If the destination receives the first copy of a RREQ, it responds with a unicast Route Reply (RREP) message that is propagated backward to the source by the chain of nodes that propagated forward the first RREQ. In this way a candidate bidirectional routing path is made active for subsequent unicast data transmissions, by giving local instructions to each intermediate node about next-hop nodes towards D and S, respectively. Figure 1 shows the modules' architecture of a node implementing the IDS. The IDS module captures all the node traffic from/to the MANET, and it filters packets that should be further processed by the AODV routing protocol. Every packet received by adjacent nodes during a path discovery process is checked, to verify if the packet is sent by a previously identified malicious node. Every packet received by the next-hop node in a pre-defined path, is checked to verify if it has been corrupted (like

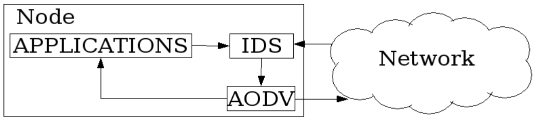

Fig. 1. Module architecture of a node with the proposed IDS

in watchdog mechanism). In both cases the packet is immediately discarded. In other words, malicious nodes are excluded from the paths they attempt to attack.

3.3.1 AODV modifications AODV has been slightly modified to implement IS-AODV:
i) RREQ and RREP message headers have been extended to include a pair of SUCV identifiers. The overhead introduced is quite marginal;
ii) the AODV routing table is made more connection-oriented, being enriched by including data structures about end-nodes, defined within the IDS mechanism.
The latter point may be considered a violation of the principles of implementation of the network layer, by mixing network and transport issues. On the other hand, recent works based on cross-layering principles applied to the protocol layers have widely collapsed layer barriers, between transport, network and MAC layers, by allowing a more simple, adaptation-based and reactive protocol stack implementation in wireless systems.

In the following, we are going to illustrate the definition of SUCV identifiers and the extension fields for AODV routing packets, that have been introduced by the IDS implementation. The definition of the mutual verification scheme, and the IDS detection and reactions will follow this illustration.

3.3.2 SUCV Identifiers Differently from IP addresses, SUCV identifiers [20] are flat identifiers with no topology-related meanings. Basically, the SUCV IDs introduce the advantage of an implicit cryptography binding between a node's identifier and its public key (or certificate). A node auto-configures its own Crypto-Based IDentifier (CBID) by doing the following operations:
1) it creates a pair of public and private keys (P_K and PrK).
2) it creates its own CBID: $CBID = hash(P_K)$, where the hash function is shared by the all network's nodes, as a system configuration parameter (assumption *a5*).
In this way the key management is simplified, since no third parties need to be involved either in creating or in distributing the public keys. Provided that the bit-length of the CBID's is large enough, these identifiers have two very important properties: they are *statistically unique* and *bound in secure way to a given node*. Any other node can easily verify the CBID signature without relying on any centralized security service, such as a Public Key Infrastructures (PKIs).

The *authentication, confidentiality* and *integrity (see g9)* implemented in our target system is based on public key cryptography, and more specifically on the SUCV (or CBID) identifiers. When a node receives the $[\mathbf{CBID}, \mathbf{P_K}]$ pair (in a message header), it calculates the hash function of the public key P_K, and it compares the result with the received $CBID$: if the value is the same, the P_K will be used to decrypt the $\{\text{DIGEST}\}_{PrK}$ included into the RREQ or RREP.

3.3.3 RREQ header extension To adopt the CBID identifiers we have extended the RREQ and RREP messages by adding some fields (see figure 2). With the IPv6 protocol, the CBID is half of the IPv6 address.

Original IPv6 RREQ	
P_{KS}	$IPv6_{prev}$
$\{DIGEST_{RREQ}\}_{PrK_S}$	

Original IPv6 RREP		
P_{KD}	$IPv6_{prev}$	RREQ_ID
$\{DIGEST_{RREP}\}_{PrK_D}$		SEQ_No

Fig. 2. RREQ and RREP extensions.

In the RREQ message the following fields have been added:
P_{KS}: public key of the source node;
$\{DIGEST_{RREQ}\}_{PrK_S}$: Digest of the RREQ message, including the extension fields, excepted the destination sequence number and hop count value.
$IPv6_{prev}$: IPv6 address of the previous node propagating the RREQ during the path creation process between source S and destination D, used to implement the mutual verification of the path creation (see below).

The route discovery phase is based on public key fields to be included into the RREQ (and RREP) header extensions. In this way the IDS supports the safe route creation over the most general scenario, without any assumption about any information sharing among MANET's nodes. Conversely, if a system information-sharing exists about the node identifiers and the related public key (as an example, by using an Hello-type broadcast message), the P_{KS} and P_{KD} could be removed in the RREQ and RREP extension fields, to reduce overheads. After the creation of the safe route-path, successive data transmissions are based on a more efficient and lightweigth symmetric key mechanism. The symmetric key exchange could be realized just after the creation of the safe route, that is, without including symmetric keys in the headers of broadcasted RREQ and RREP messages.

3.3.4 Mutual verification of the path creation. By looking at figure 3, the mutual verification process is explained: $IPv6_{prev}$ is set on a node to identify the previous node in the path (as indicated by arrows):
1) the intermediate node $N1$ will receive RREQ from source node S;
2) upon reception of one RREQ from previous node S, $N1$ sets the $IPv6_{prev}$ value with IPv6$_S$. $N1$ then re-broadcasts the RREQ (which will propagate to neighbors $N2$ and S);
3) mutual verification of node S: S will detect the RREQ forwarded by $N1$. S checks that $IPv6_{prev} = IPv6_S$, and it compares last RREQ with its own cached RREQ copy. S determines in this way if $N1$ has correctly forwarded the RREQ, or not;
4) all intermediate nodes, including $N1$ and $N2$, do behave like S when propagating RREQs (and RREPs along the reverse path).

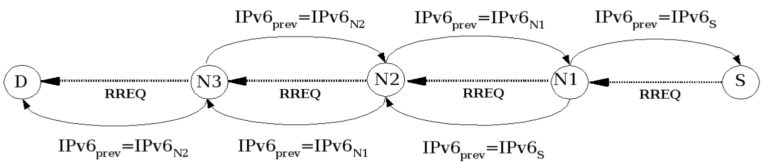

Fig. 3. $IPv6_{prev}$ setting.

3.3.5 RREP header extension In the RREP message the following fields have been added to the RREP header (see figure 2):
P_{KD}: public key of the destination node;
$IPv6_{prev}$: $IPv6$ address of the previous node along the return path;
$\{DIGEST_{RREP}\}_{PrK_D}$: Digest of the RREP message, extension fields included;
$RREQ\_ID$: copy of the RREQ ID value that has generated this RREP;
SEQ_No: copy of the RREQ's originator sequence number value that has generated this RREP.

The $IPv6_{prev}$-based mutual verification management, as shown in figure 3, is repeated in the opposite forwarding direction for RREPs.

3.3.6 Conservative Property to avoid the RREQ_ID and Sequence Number attack effects The RREQ_ID and SEQ_No fields are used in RREPs to verify the definition of a safe route. This is required because the *RREQ ID attack* and the *sequence number attack* could be performed by byzantine nodes to interfere with the route construction. When an intermediate node N_I receives a RREP from N_{I+1}, it checks (in its own local log) if it previously overheard the corresponding RREQ forwarded in the opposite direction (from N_{I+1} to N_{I+2}). The checks performed include the correct IP settings, and the originator sequence number and RREQ ID corresponding to the RREP received. In addition, N_I checks if it has previously received and forwarded a RREQ from N_{I-1} (that is, its previous node in the path between N_I and the source node). If the two conditions are true, then N_I forwards the RREP back to N_{I-1}, by contributing in this way to define the bidirectional verified route path between S and D.

3.4 IDS detection and reactions

In this section, the IDS detection and reaction processes are defined. In previous section, we illustrated how each network node is assumed to monitor only the traffic whose transmission path (or route discovery phase) includes it as an intermediate node.

The IDS management of RREQs and RREPs requires additional data structures. The IDS reaction is based on a counter $MB_{i,j}$ of malicious behaviors detected by node i for each neighbor j. This counter is similar to the "reputation" concept used in other works. When the counter $MB_{i,j}$ exceeds a predefined **threshold value, TV** ($TV = 3$ in our experiments) then the node i will undefinitely or temporarily consider node j as a corrupted node. The value of TV is related to the degree of security: $TV = 10$ would result in tolerant networks (low security level) while $TV = 1$ would result in low tolerant network (high security level).

If network nodes are assumed to be possibly infected by malicious code (as an example, virus-like attacks), then they could be temporarily suspected. In this way, once a "suspect validity time" expires (this validity time value must be properly defined according to the network features) the node could be reconsidered during path formation processes.

The IS-AODV RREQ-management requires the maintenance of three sets of IDs, for each node N in a path:

First Nodes: the set of nodes from which N receives the first valid RREQ that must be forwarded, according to the AODV specifications;

Alternative Nodes: the set of nodes from which N receives an RREQ whose RREQ IDs was already processed (that is, RREQ copies);

Next Nodes: the set of nodes from which N should receive the RREP. These nodes are identified as the nodes that correctly forwarded an RREQ received from N (i.e. whose $IPv6_{prev}$ indicated N).

The IS-AODV RREP-management requires an additional set of IDs for each node, to be updated during every route discovery process:

Selected Paths: the set of nodes to whom N sent an RREP that must be forwarded back to S, according to the AODV specifications;

The purpose of the above mentioned sets will be illustrated in the following examples. Let's consider the following path where the arrows illustrate the direction of the target packet flow:

$$N_1 \rightarrow N_2 \rightarrow N_3$$

if N_1 sends a (routing or data) packet along the route to N_3, then N_1 is assumed to overhear the packet forwarded by N_2. If N_2 corrupts the packet, then N_1 can detect the corruption, by counting a byzantine behavior for node N_2. When the counter of malicious behaviors for node N_2 exceeds a **threshold value** on N_1, then N_1 will not interact with N_2, by locally simulating a *link-break*, under the routing protocol viewpoint, that is, by excluding the malicious node N_2 from the route path. Corrupted nodes are considered the same way as nodes that moved away, unless they behave in a correct way. Anyway, this reaction is not enough, to create a safe path between two safe end-points. The following example illustrates how unsafe paths can be avoided by the IDS reactions. By looking at figure 4.a, let us assume that $NC1$ realizes a RREQ corruption, (for this case the *RREQ ID attack* is excluded), and that

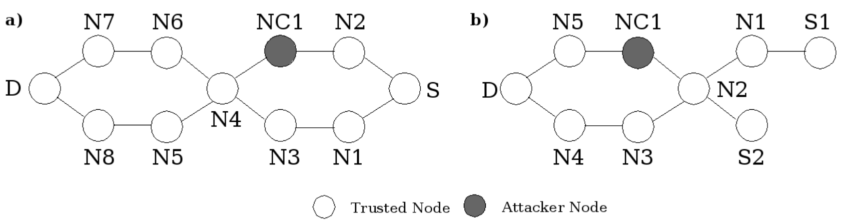

Fig. 4. a)Network with an attacker node; b)Network with two source nodes and only one destination.

the RREP sequence from D to S, obtained after the route discovery process, is going to be forwarded on the following reverse path:

$$D \rightarrow N8 \rightarrow N5 \rightarrow N4 \rightarrow NC1 \rightarrow N2 \ .$$

Node $N2$ stops the RREP forwarding because it has checked the $NC1$ RREQ's corruption. For this reason, after a timeout, S will start a new route discovery process, by sending a new RREQ broadcast message. Note that malicious node $NC1$ still participates to this process.

On the other hand, $N4$ (like each other node) maintains a *Selected Paths* set indicating the nodes where $N4$ has already forwarded a RREP message (that is, including $NC1$), and an *Alternative Nodes* set indicating the nodes where $N4$ has not still forwarded a RREP message. For this reason, upon reception of a new RREQ message from S to D, $N4$ will exclude nodes belonging to the *Selected Paths* set (that is, $NC1$). As an example, in figure 4.a, $N4$ will select $N3$ to receive the RREQ, and to respond later with the RREP message. When the *Alternative Nodes* set is empty, the *Selected Paths* set is restarted (that is, all nodes propagating RREQs are considered valid for forwarding RREPs).

This management is implicitly derived by the concept of **AODV black list**, that we sketch in the following. When a node $N4$ forwards a RREP on a reverse path, it would expect to receive data packets, and not another RREQ message from the path source S. If a node $N4$ receives another RREQ from the same source S to destination D, it may realize that:
i) at least one unidirectional (S to D) link is present between $N4$ and S, or
ii) at least one attacker node is present between $N4$ and S.
In both scenarios the RREP path must be (at least temporarily) discarded by node $N4$. If alternative paths exist, $N4$ will select one of these, as an example:

$$D \rightarrow N7 \rightarrow N6 \rightarrow N4 \rightarrow N3 \rightarrow N1 \rightarrow S.$$

The route validity and the identity of previous- and next-hop nodes in a valid path can be assumed by a node $N4$ when it receives an ACK (e.g. from $N6$) under a bidirectional TCP-like connection, or a Data packet (e.g. from $N3$) under a unidirectional UDP-like connection. While this happens, $N4$ would discard every other RREQ aiming to find a route between S and D. If the routing path explicitely expires on $N4$ due to AODV route entry expiration or a link-layer failure, then RREQs would be accepted again by $N4$ to recover the S-to-D path failure. Solutions for attacks to these policies can be found in the "Coordinated DOS attack" in the Appendix and in [24].

3.4.1 Corrupted RREPs: if the destination node D receives a corrupted RREQ and no other safe RREQ has been received in the discovery process, then D will send an explicitly corrupted RREP anyway. This will allow to identify the current path as a path including at least a corrupted node, by causing the updates to the *Selected Path* set of intermediate nodes. In general, any corrupted RREP will not modify any routing table, and will be simply discarded by the source node S.

3.4.2 Conservative Property to avoid Routing loops: the following rule is implemented to avoid route loops: if a RREP is received from a node N that belongs to RREQ's *Alternative Nodes* set or *First Nodes* set, then N will be accused, because a node can receive RREPs only from nodes belonging to *Next Nodes* set of the corresponding RREQ message. For the same reason a data packet is forwarded from S to D only if it is received by the last node inserted into the *Selected Path* set.

3.5 AODV's route maintenance

AODV is a on-demand routing protocol, which means that nodes not involved in active communication paths do not maintain any routing information. The Route Error (RERR) message is created by intermediate nodes of a path to inform the path neighbors about a detected link failure. This is one of the proactive activities of AODV for nodes on the active path. This proactive function may introduce the *RERR attack*: a malicious node could flood the MANET with false RERR messages. To contrast this attack a high-cost checking procedure would be needed. As an alternative solution, the RERR messages should not be used in the system: only the end-points of a path should decide if a new route discovery process must be started. In our proposal, the IDS simply discards all RERR messages received, if any.
3.5.1 Route updates and Sequence numbers The proactive route-update implemented in some versions of AODV is based on the packets' sequence-number parameters, and may cause a refresh of cached route paths on intermediate nodes. This proactive function could introduce a possible performance loss, described in the following example. By considering the network shown in figure 4.b, let us assume that the path from D to $S1$ is:
S1 → N1 → N2 → N3 → N4 → D.
If $S2$ wishes to communicate to D, let us assume $S2$ sends a RREQ, and the corresponding RREP is forwarded on the following reverse path (including the attacker $NC1$):
D → N5 → NC1→ N2 → S2 .
Given the route update function on node N2, the path from D to S1 will be updated as:
S1 → N1 → N2 → NC1 → N5 → D.
To summarize, if $NC1$ tries to corrupt the RREP to $S2$, then $S2$ and $N5$ will detect the corruption of the RREP, but the connection between $S1$ and D will be broken by the proactive route update of $N2$. This will cause a new RREQ process to be activated by $S1$ (since it will detect the corrupted route path, when receiving the first packet, or after a timeout). For the aforementioned reasons, under byzantine attacks, the proactive route-update mechanism realized by intermediate nodes, could result in a performance loss. So, the proposed IDS adopts a connection-oriented routing table data structure: the path between two end-points S and D is modified only by a new route discovery process initiated by S or D [1].

3.6 Attacker Model and solution

The attacker model considered is based on *active* and *internal* attack types. The following list illustrates a set of attacks described in [7],[8], that have been considered in the IDS and IS-AODV design. A short description of the IDS solution to contrast a given attack type is provided in the Appendix, and in [24]. The list of attacks includes: Black Hole, Route Disruption, Route Invasion, Modify and Forward, Denial of Service, End-node impersonation, Coordinated DOS attack, RREQ ID attack, IP attacks,Coordinated adjacent node attack.

4 Performance Analysis

4.1 Introduction

To perform the performance investigation, a MANET system model has been implemented with the *ns2 Network Simulator*. The MAC layer model implements the IEEE 802.11 DCF protocol. The IS-AODV model is derived from the Uppsala University AODV model (AODV-UU)[23], freely available, and almost compliant with a real AODV implementation code. The complete IDS implementation has been modeled as an additional feature of MANET nodes.

[1] Note that we can simply force the end-to-end route update in AODV, by setting the D bit in the standard RREQ packet to value 1: only the destination can create an RREP

4.2 Simulation parameters and metrics

Simulation duration	300 sec	Maximum Speed	20 m/s
Simulation Area	1500m * 300m	Packet rate	(CBR) 4 pkt/sec
Mobile hosts number	50	Host pause time	100 sec
Transmission Range	250 m	Connections Number	10, 20, 30
Movement model	Random waypoint	Corrupted nodes number	10 %, 25%, 50%

Table 1. Simulation parameters

Table 1 shows some most significant simulation parameters. It is worth noting that the speed of nodes is 10m/s on the average, and 20m/s maximum, with the pause time of 100 seconds under a Random Waypoint mobility model on a long rectangle-shaped area. These assumptions may be considered quite unrealistic, but they have been defined in this way in order to stress the IDS and the routing mechanisms. All the attack types that have been implemented in the model, mainly against the RREQ and the RREP messages, are listed in previous subsection. Corrupted nodes try to establish connections with others nodes (both safe and corrupted ones). Our interest in the analysis is on connections originated between two safe end-points (as assumed in the mechanism's design). We will skip general results about AODV routing performances that could be found in the literature. Our main interest is on effects and overheads of the proposed IDS and secure routing scheme (IS-AODV), with respect to standard AODV: *i)* the packet overheads introduced in RREQ and RREP packets, *ii)* the additional computation required for implementing the IDS and secure routing scheme, and *iii)* the number of additional RREQs needed to find a safe route, in a given scenario. The packet overheads introduced can be considered marginal (see section 3), and this analysis has been skipped. The computation overheads can be considered marginal too, since the proposed scheme introduces few additional data structures in every node (less than 2 KB for the proposed scenario), and the significant computation (mainly for implementing cryptography functions) is delegated to end-nodes, only. Since the proposed system creates additional *virtual link breaks*, and route discovery processes, due to corrupted nodes' effects, and due to possible ambiguous effects of collisions and hidden terminals on the mutual verification mechanism, the main evaluation metric we will discuss here is the comparison of the average number of RREQs issued by a source node, needed to establish a end-to-end connection (under AODV), and a safe end-to-end connection (under IS-AODV). The *Average Number of RREQs* shown in the figures is not the number of link failures in the system, but it is the average number of RREQs that the source node must send to complete a route path creation (as a reaction to missing path or link failures in existing paths). This evaluation will be obtained under different percentages of attacker nodes, and under different mobility and collision effects, in the MANET scenario:

i) while the network is attacked and all the nodes were static during last 100 seconds, that is, when IS-AODV is active and nodes start to have good knowledge of their respective one-hop neighbors: *IS-AODV On (only safe routes), 100 sec. static scenario*;

ii) while the network is attacked, IS-AODV is On, and mobile nodes cause more difficult secure-path creations: *IS-AODV On (only safe routes), steady-state mobile scenario*;

iii) without attacker nodes, that is, by matching the standard AODV path formation process: *IS-AODV Off (pure AODV).*

These three scenarios are compared to test the security system behavior under the attacks, with respect to ideal scenarios with no attacks (with standard AODV). We performed experiments with runs of 300 seconds of simulated time, and 50 nodes in the area. Results shown are within confidence intervals whose confidence level is 95%.

4.3 Simulation Results

In this section we present the obtained simulation results, with variable percentage of corrupted nodes, effects of mobility, collisions and hidden terminals for the performance index shown. Only most significant figures are shown due to space limitations. The figures 6.a and 6.b show the *Average Number of RREQs* needed for each active route-path under the AODV protocol in the MANET scenario with 50 active nodes, 30 active end-to-end connections (whose hop-count is indicated in the X axis). The percentage of corrupted nodes is 10% in figure 6.a and 50% in figure 6.b, respectively. By looking at the figures, the curves *IS-AODV Off (pure AODV)* show the average number of RREQs required by sources to find a generic route in the system, as a function of the path hop-count. The average value is comprised between 1 (that is, the optimal value) and 2. This slightly sub-optimal effect is produced by the mobility and by some MAC-layer frame-loss effects (as an example, collisions due to RREQs broadcast storms on the destination node). The difference between static and mobile scenarios is marginal for this performance index (so only one is shown), because a path creation is fast enough to complete without significant effects of the modeled node mobility. The route-path length has marginal effect, and this indicates that one route path can be easily found within few attempts, given the simulated system characteristics. The curve *IS-AODV On (only safe routes), steady-state mobile scenario* show the same index above, as a function of the path length, in a steady-state scenario with mobile nodes, IS-AODV active, 10% attacker nodes in figure 6.a, and 50% attacker nodes in figure 6.b, respectively. The average number of RREQs to obtain a secure path increases with the path length, as expected, because the probability to have attackers in the candidate paths increases accordingly. The same consideration is valid in the comparison between 10% and 50% attacker nodes scenarios. The mobility effect of nodes contrasts the secure clustering that would emerge given the IDS effect in IS-AODV: nodes that locally accuse other nodes may move and lose this knowledge-base useful to create safe paths. The effect of the secure clustering is shown in the curve *IS-AODV On (only safe routes), 100 sec. static scenario*. The only difference with respect to previous curve is given by the static uniform distribution of nodes in the area. The average number of RREQs in the system reduces because nodes acquire more persistent information about neighbor nodes, and identify the attackers by excluding them in the current and future path creation processes. The average number of RREQs attempts that would be aborted during a path creation by the IS-AODV effects can be obtained as the difference between the IS-AODV On and IS-AODV Off curves.

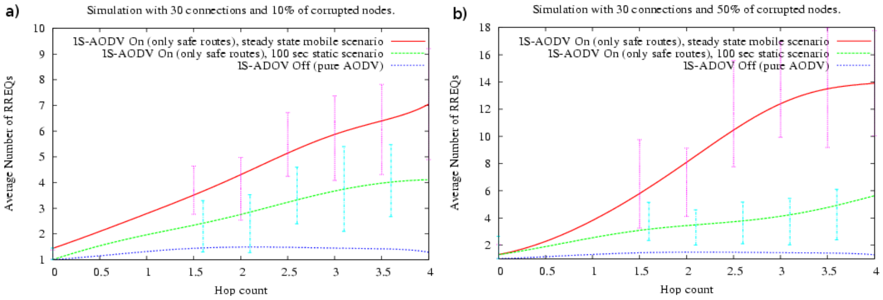

Fig. 5. Average Number of RREQs as a function of the mobility and hop distance

The figures 7.a and 7.b show a comparison of the effects of collisions and hidden terminals on the IS-AODV mechanisms (10% and 50% corrupted nodes). The critical effects, under this viewpoint, are given by the signal collisions on the receivers, and by the hidden terminal effects on nodes implementing the mutual verification of path creation. A discussion of these critical effects can be found in the discussion of watchdog problems in [9]. As an example, by looking at figure 4.a, if $N1$ is unable to sniff the RREQ sent by $N3$ to $N4$ (e.g. due to S transmitting) then $N1$ will not propagate the related RREP received from

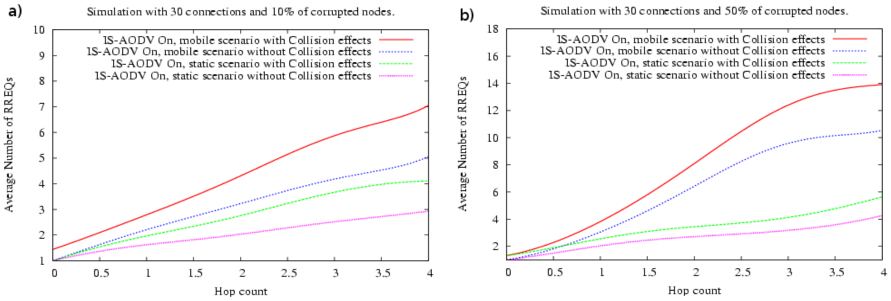

Fig. 6. Average Number of RREQs: hop distance and collision effects

$N3$. This is due to the conservative design of our IDS. In IS-AODV, these effects translates in an increase in the number of RREQs needed to obtain a safe route. This overhead is shown in the curves *IS-AODV On, mobile scenario with collision effects* compared with *IS-AODV On, mobile scenario without collision effects* for the mobile scenario. In the static scenario, the overhead effect is shown in the curves *IS-AODV On, static scenario with collision effects* compared with *IS-AODV On, static scenario without collision effects*. We are currently working on less conservative IDS solutions to overcome this problem.

The percentage of safe nodes that accuse a corrupted node, and the percentage of corrupted nodes that have been discovered by at least one safe node is initially zero. When these two percentage values are 100% the network would be completely clustered (every safe node has discovered every attacker neighbor). An example of the clustering effect of safe nodes, after 300 seconds of simulated time, and 30 active connections in mobile scenarios, is shown by sample data reported in table 2, for variable percentages of attacker nodes in the system.

Malicious nodes in the network	% Safe nodes accusing ≥ 1 attacker	% Attacker nodes discovered by ≥ 1 neighbor
10%	9%	27%
25%	51%	24%
50%	39%	37%

Table 2. Clustering effect of safe nodes after 300 seconds: 30 connections, 50 mobile nodes

5 Conclusions and future works

In this work, we defined and tested a new solution based on IDS and SUCV identifiers to assist the AODV routing protocol in finding end-to-end safe routes in a MANET scenario, called IDS-based Secure AODV (IS-AODV). The overhead represented by the number of RREQs during route discoveries has been evaluated. This appears as a fair cost to pay, given the challenging assumptions of the MANET scenario, to have some additional guarantees about the end-to-end security of communications. Simulation results confirmed that the proposed IDS contributes to a transparent clustering of safe nodes, which isolate the attackers with a passive reaction. This fact is quite important, since passive reactions i) do not require additional communication to propagate the information about corruption on the network, ii) do not require any voting procedure, and iii) do not enable additional types of attacks. The speed in the creation of a secure clustering would depend on external factors like node mobility. In IS-AODV, packet overheads are limited to additional header fields in RREQ and RREP packets, while computational overheads (mainly for cryptographic operations) are concentrated on the end-nodes, only. Intermediate nodes perform a one-hop neighbors' control policy, similar to a watchdog solution. In future works, we plan to execute more detailed and accurate simulations, by working on system and mechanism tuning and design. Additional policies will be considered for the IDS design, e.g. the management of the variable suspect validity time discussed in the appendix. We plan to investigate cross-layering principles applied to the physical, MAC, clustering and routing layers, to help the system monitoring and to increase the control functions on all neighbor nodes.

References

1. P.Albers, O. Camp, J. M. Parcher, B. Jouga, L. Me, R. Puttini. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. *WIS 2002. In the 4th International Conference on Enterprise Information Systems, 2002.*
2. T. Clausen, P. Jaquet, A. Laouti, P. Minet, P. Muhlethaler, A. Quyyum, L. Viennot, Optimized Link State Routing Protocol , *Internet Draft, draft-ietf-manet-olsr-06.txt, work in progress, Sep 2001.*
3. C. E. Perkins, P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers , *Proceedings of the SIGCOMM 94 Conference on Communications Architectures, Protocols and Applications, August 1994.*
4. D. B. Johnson, D. A. Maltz, Y-C Hu, J. G. Jetcheva, The dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR), *Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress, Feb 2002.*
5. C. Perkins, E Belding-Royer, Ad hoc On-demand Distance Vector (AODV), *Request For Comments (RFC) 3561, July 2003.*
6. S. Bhargava and D. P. Agrawal. Security Enhancements in AODV protocol for Wireless Ad Hoc Networks. *in Proceedings of Vehicular Technology Conference, 2001.*
7. H. Deng, W. Li and D. P. Agrawal. Routing Security in Wireless Ad Hoc Networks. *IEEE Communications, October 2002.*
8. P. Ning and K. Sun. How To Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols. *in Proceedings of the 4th Annual IEEE Information Assurance Workshop, pages 60-67, West Point, June 2003.*
9. S. Marti, T.J. Giuli, Kevin Lai and Mary Baker. Mitigating Routing Misbehavior in Mobile Ad-hoc Networks. *in Proceedings of the 6th Annual ACM/IEEE international Conference on Mobile Computing and Networking, pp. 255-265, 2000.*
10. A. Patcha and A. Mishra. Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks. *in Proceedings of the Radio and Wireless Conference, RAWCON 2003.*
11. Yongguang Zhang, Wenke Lee and Yi-An Huang. Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks, Volume 9 Issue 5, September 2003.*
12. C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe and K. Levitt. A Specification-based Intrusion Detection System for AODV. *In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 125 134. ACM Press, 2003.*
13. J. Undercoffer and Anupam Joshi. Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad-hoc Networks. *Technical Report, UMBC, October 2002.*
14. P. Papadimitratos, Z. J. Haas, Secure Routing for Mobile Ad hoc Networks , *Proceedings of the SCS Communication Networks and Distributed Systems, Modelling and Simulation Conference (CNDS 02), pp. 27-31, January 2002.*
15. Y. C. Hu, A. Perrig, D. B. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks , *Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom 02), pp. 12-23, September 2002.*
16. B. Dahill, B. N. Levine, E. M. Royer, C. Shields, A Secure Routing Protocol for Ad hoc Networks , *Technical Report, UM-CS-2001-037, University of Massachusetts, August 2001.*
17. Y. C. Hu, D. B. Johnson, A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Wireless Ad hoc Networks , *Proceedings of the 4th IEEE Workshop on mobile Computing Systems and Applications (WMCSA 02), pp. 3-13, June 2002.*

18. P. Michiardi, R. Molva. Core: A COllaborative REputation mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. *Proocedings of IFIP Communication and Multimedia Security Conference 2002.*
19. S. Buchegger, J-Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks) *Proceedings of Mobihoc 2002.*
20. G. Montenegro and C. Castelluccia.Crypto-Based Identifiers (CBIDs): Concept and Applications. *ACM transaction on information and system security, vol. 7 num. 1, February 2004, page 97-127*
21. C. Castelluccia and G. Montenegro. Protecting AODV against Impersonation Attack. *ACM Mobile Computing and Communications Review vol. 6 num. 3,July 2002*
22. Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis. Secure Routing and Intrusion Detection in Ad Hoc Networks. *Proceedings of the 3rd International Conference on Pervasive Computing and Communications (PerCom 2005).*
23. Uppsala University AODV implementation
    http://www.docs.uu.se/docs/research/projects/scanet/aodv/aodvuu.shtml
24. http://www.cs.unibo.it/˜bononi/Publications/is-aodv_tr_2006.pdf
25. R. B. Bobba, L. Eschenauer, V. D. Gligor, and W. Arbaugh. Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks. In proc. IEEE Global Telecommunications Conference, December 2003.

Appendix

A Attacks and solutions

The following list illustrates a set of attacks described in [7],[8], followed by a short description of the IDS solution to contrast each attack type:

Black Hole: not possible because only the destination D can create and send the valid RREP message;

Route Disruption: not possible because only nodes belonging to a path can try to disrupt it, and this fact will be discovered by S and D;

Route Invasion: not possible, because nodes cannot insert themselves to a created route, given the *First Nodes, Alternative Nodes* and *Next Nodes* sets existence and management; **Modify and Forward:** not possible, because under the system assumption *a2* (bidirectional links) the attacker can be detected and eventually accused (isolated) by safe nodes. Modified packets can be always discovered at end points;

Denial of Service (DOS): if false RREQs are created and sent to waste the channel resources, a RREQ limit could be fixed. On the other hand, it is not possible to contrast MAC layer channel occupancy and wastage by malicious nodes;

End-node Impersonation: can be made statistically and arbitrarily unprobable, thanks to SUCV identifiers.

In conclusion, there are some kind of attacks against AODV and the security system proposed that would require special conditions and reactions:

Coordinated DOS Attack: this type of attack can be dangerous only under specific topology conditions: as an example, in figure 4.a, if $NC1$ and $N5$ are coordinated malicious nodes they could create some problems to $N4$, which specifically is included in all possible paths between source S and destination D.

This DOS attack cannot be excluded, but it requires favourable conditions hard to be maintained undefinitely, as an example, due to hosts' mobility and existence of possible alternative paths. When $N4$ is successfully forwarding packets and it receives a new RREQ from S to D from its neighbors, it could perform some kind of periodic cryptography-based control to avoid this DOS attack. This would imply some computation overheads in intermediate nodes, but this overhead could be under control of a crypto-check frequency parameter. As an example, one cryptography-based control every K RREQs received.

RREQ ID attack: an attacker may arbitrarily increase the RREQ ID field *i)* for being included into the path or *ii)* to block the subsequent RREQ IDs in the next discovery processes. The first attack would not have success because the destination will check the *digest* and the corruption will be identified. The second attack can be avoided by using a combination of *i)* the RREQ ID time validity (must be set equal to the AODV's PATH DISCOVERY TIME value), and *ii)* the *Selected Path* set. The RREQ ID validity time expiration defines the time before the RREQ ID could be processed again. The management of the *Selected Path* set avoids that a node keeps repeating this attack.

IP attack: if an attacker frequently changes its IP (like if it was a new node each time) then a safe node would observe a high neighbors' number. Anyway, it could classify the one-hop nodes into the following sets:
i) (still) *trusted* set;
ii) corrupted set;
iii) not again identified or *new* set.
In the IDS, the safe nodes would give priority to the *trusted* set with respect to the *new* set, during the path discovery process. In this way corrupted nodes attempting to realize this kind of attack would be excluded. Let us suppose that the corrupted node NC_k forges its IP with the IP_{NT_j} of a trusted node NT_j by attempting to make it accused by the other safe nodes. Every other trusted node NT$_i$ exposed to this attack in the network could be in the following possible scenarios:
1) both NC_k and NT_j are one-hop neighbors of NT$_i$: NT$_i$ receives two RREQ (or RREP) copies (one corrupted from NC_k, and one safe from NT_j) with the same IP_{NT_j} address,within the PATH DISCOVERY TIME related to the current route discovery process. In this case, NT$_i$ does not increase its counter $MB_{i,j}$ of malicious behaviors detected by node i(see section 2.4) on behalf of NT_j. For this reason the trusted node NT_j is not excluded by the other safe nodes.
2.a) NC_k is one-hop neighbor of NT_i, while NT_j is not: NT$_i$ receives one corrupted RREQ (or RREP) from NC_k, and increases the $MB_{i,j}$ for the node IP_{NT_j}.This accusation has no critical effect, because NT$_i$ locally excludes a node which is not its neighbor.Given the passive reaction implemented by nodes, such wrong information is not propagated in the network.In addition, it is possible to define a "suspect validity time" for the suspect nodes. When this validity time expires the suspect node could be considered safe, again. For this reason, if the NT_j would move to NT_i it will be considered safe, eventually.
*2.b)*both NC_k and NT_j are one-hop neighbors of NT$_i$ and a collision occurs so that NT$_i$ receives only the message copy from NC_k. This scenario appears as similar to the previous one, and the safe node NT_j would erroneously increase its counter $MB_{i,j}$ of malicious behaviors detected by node i. The adoption of the Threshold Value (TV) and the "suspect validity time" would reduce the performance loss in these scenarios.

Coordinated adjacent node attack: In this type of attack two or more collaborative adjacent node colludeto create anomalous routing event. For example in the path:

$$\mathrm{S} \rightarrow \mathrm{A} \rightarrow \mathrm{M1} \rightarrow \mathrm{M2} \rightarrow \mathrm{B} \rightarrow \mathrm{D}.$$

if M2 corrupt the RREQ or M1 corrupt the RREP, the safe nodes A and B cannot detect these anomaluos behaviors. In this case the digest verification at the end node S and D help the route creation process, detecting a packet corruption of one or more intermediate node. So a new RREQ process starts on a different route (see 3.4), if exist.