Universidade Federal do Paraná

Departamento de Informática

Michele Nogueira Lima
Helber Wagner da Silva
Aldri Luiz dos Santos
Guy Pujolle

A Security Management Architecture for Supporting Routing Services on WANETs

Relatório Técnico
RT-DINF 001/2010

Curitiba, PR
2010

Resumo

Due to the raising dependence of people on wireless networks for using critical applications, high level of reliability, security and availability is claimed to assure secure and reliable service operation. Wireless ad hoc networks (WANETs) experience serious security issues even when solutions employ preventive or reactive security mechanisms. In order to support network operations and security requirements of critical applications, we present SAMNAR, a Survivable Ad hoc and Mesh Network Architecture. Its goal lies in managing adaptively preventive, reactive and tolerant security mechanisms to provide essential services even under attacks, intrusions or failures. We use SAMNAR to design a path selection scheme for WANET routing. The evaluation of this path selection scheme considers on scenarios using both urban mesh network mobility and propagation models. Results show the survivability achieved on the routing service under different conditions and attacks.

1 Introduction

Recent technological advances in wireless networking have popularized the use of portable devices, raising the dependence of people on them for executing anywhere and anytime critical applications, like business-critical applications in financial transactions or life-critical applications in healthcare. Such dependence claims simultaneously for high level of reliability, security and availability to assure secure and reliable service operation even under failures, intentional threats or accidents. Wireless ad hoc networks (WANETs) – mobile or stationary – have envisioned to support ubiquitous computer connectivity by self-organized portable devices, also called nodes, communicating among themselves in a wireless and multi-hop fashion.

WANETs, such as mobile ad hoc networks (MANETs), wireless sensor networks (WSN) or wireless mesh networks (WMNs), experience serious security problems due to their particular characteristics. Wireless communication can endure interferences or malicious interceptions, whereas multi-hop communication assumes that each node will act properly its functions to support network services. Further, WANET's self-organization increases the complexity of security management operations as access control, node authentication, secure routing and cryptographic key distribution.

Most of existing security solutions for WANETs [1–7] employ preventive or reactive security mechanisms, detecting intrusions and thwarting attacks by cryptography, authentication and access control mechanisms [8]. Each security mechanism addresses specific issues having limitations to cope with different types of attacks and intrusions. Preventive defenses, for example, are vulnerable to malicious nodes that already participate in network operations, whereas reactive defenses work efficiently only against well-known attacks or intrusions. Due to these limitations, researchers have developed intrusion tolerant solutions [9], as a third defense line, to mitigate the impact of attacks and intrusions by fault-tolerance techniques, typically redundancy and recovery mechanisms. However, security solutions remain still focused on one specific issue or layer of the protocol stack, being ineffective to ensure essential services of wireless ad hoc networks.

Security management lies in one of the key research challenges on WANETs due to their characteristics, critical application requirements and restrictions on defense lines [10]. Security management consists of facilities to control security mechanisms and services and, then, thwart attacks or intrusions. Since critical applications require new capabilities from WANETs for supporting essential services even under attacks and intrusions [11], designing new approaches for security management is a demanding task. In this work, we introduce SAMNAR, a Survivable Ad hoc and Mesh Network ARchitecture,

whose goal is to provide support for designing survivable essential network services against attacks and intrusions. SAMNAR manages preventive, reactive and tolerant security mechanisms in an adaptive and coordinated way, focusing on the support for the survivability of essential services as link-layer connectivity, routing and end-to-end communication.

We employ SAMNAR to support the routing service in order to design a survival path selection scheme. The designed scheme is standalone of any protocol and consists in choosing the most survival paths. Hence, the scheme takes into account several criteria that correlate both network conditions and three defense lines. For associating all criteria and taking inferences, fuzzy logic is employed due to its low computational intensiveness. Evaluation results, considering metrics of survivability and performance, show mitigation on the impact of different routing attacks as well as low performance loss for WANETs.

The article proceeds as follows. Section 2 discusses related works. Section 3 presents our assumptions, as well as network and attack models. Section 4 details the SAMNAR architecture. Section 5 describes the proposed survival path selection scheme. Section 6 presents evaluation results of the proposed scheme. Finally, Section 7 concludes the article and provides future directions.

2 Related work

This section gives an overview of existing security management architectures for network survivability. Initially, security management architectures for network survivability were proposed to improve both security and dependability of information systems in the Internet context [12–14]. Albeit the importance of all architectures to support the survivability concept, we highlight SABER [13] and SITAR [14] architectures due to their completeness in terms of survivability properties as resistance, recognition, recovery and adaptation. SITAR is an architecture for surviving distributed services and comprises different components, such as proxy servers, monitors, audit control module and adaptive regeneration module. Thus, SITAR coordinates all components and controls any requests and responses in a centralized or partially distributed way.

The SABER architecture [13] integrates also different security mechanisms to improve the survivability of Internet services. Its multi-layer approach blocks, evades and reacts to a variety of attacks in an automated and coordinated way. Its components, as DoS resistant module, IDS and anomaly detection, migration process and automated soft-patching system,

are controlled by a coordinated infrastructure providing the communication and correlation among the components in a decentralized fashion.

In the last years, survivability concepts have also been applied in wireless and mobile networks. Existing works can be categorized in two classes, those to improve network survivability managing mechanisms for tolerating faults and those that propose security management architectures to survive intrusions and attacks [15–18]. In [15], a security management architecture towards a survivable access control in WANETs is proposed, being the survivability achieved by the creation of secure groups. In [16], an architecture is defined to improve WLAN survivability against attacks that harm access points. In [17] and [18], security management architectures for survivable wireless sensor networks have been designed, focusing on DoS attacks and on multiple attacks, respectively. However, all those architectures handle only one specific service and do not employ more than two defense lines together, being still unable to attain simultaneously all survivable properties, as resistance, recognition, recovery and adaptation.

3 Self-organized network and attack models

Network model: We focus on multi-hop wireless ad hoc network consisting of n mobile or stationary nodes. The network is self-organized and nodes are randomly distributed in an area A with density $d = n/A$. Mobile nodes move into this area following a given mobility model. Neither routing support infrastructure exists nor a central control entity to manage network resources. Hence, nodes have similar functionality contributing in the network maintenance, management and routing process.

No node has complete knowledge of the network topology, requiring routing to communicate with nodes that are out of its radio range. Each node possesses a single channel with a common transmission range r and bandwidth w. All nodes can be data sources communicating via unicasting transmissions. Nodes into the transmission range of a node x are called neighbors of x and the communication with them is single-hop.

We assume that NP paths are available for the transmission of data packets from a source node to a destination node. Any multipath routing protocol can be employed in order to discover these paths. All paths are node-disjoint; that is, they have no nodes in common. Hence, they are independent in the sense that success or attack of one path cannot imply success or attack of another. However, as nodes utilize a single channel, node disjointness cannot guarantee the total independence of paths due to interferences caused by simultaneous transmissions of different routes [19].

We consider the existence of a public key infrastructure (PKI) to bind cryptographic public keys with their respective node identities. Each node possesses a security credential based on its public key certificate. Node credentials have an expiration time and should be renewed periodically. Security credentials are used for authenticating nodes and controlling the access into the network [20]. Messages must be also authenticated and those that cannot be authenticated are discarded. Since a PKI exists, nodes use public keys to encrypt and, hence, protect the route discovery and data forward phases. Moreover, such nodes use a reputation system [5] to continuously evaluate the reputation of its neighbors.

Attack models: This work focuses on attacks that can compromise routing service and it does not address attacks that can degrade or disrupt MAC or physical layers. Taking into account that unauthorized nodes cannot joint the network due to the access control and authentication mechanisms; and also that some types of attacks, such as eavesdropping, Sybil and packet fabrication or modification, can be prevented by traditional encryption, authentication and integrity mechanisms, we concentrate our analyses on authorized nodes acting in a malicious or selfish fashion alone or in collusion. Attacks yielded by misbehaving (malicious or selfish) nodes, such as *blackhole*, *grayhole*, *wormhole* and *sinkhole*, cannot be prevented uniquely by authentication mechanisms.

In *blackhole attack*, misbehaving nodes drop data packets, but they continue to participate in routing operations. Hence, whenever a misbehaving node is selected on a path, data will be lost on the path. Grayhole (selective forwarding) attack is a variant of blackhole attacks where misbehaving nodes will select which packet will be dropped. Those attacks select only packets of applications that are vulnerable to packet loss, such as real-time applications. Authentication techniques cannot prevent this attack. When a node is under adversarial control, all cryptographic keys are available to the attacker. Thus, the attacker can generate messages that appear to be authentic. Moreover, nodes try to mask their misbehavior by their correct participation in the route discovery phase and, therefore, being undetected by many intrusion detection systems.

Wormhole results from colluding misbehaving nodes coordinating their actions. In *wormhole* attack, two colluding misbehaving nodes cooperate by tunneling packets each other in order to create a shortcut in the network. This tunnel can be created by using a private communication channel, such as a pair of radios and directional antennas, for instance. Misbehaving nodes use the wormhole's low cost appearance to attract data flows, and then they disrupt the network by selectively dropping the data packets or to perform traffic analysis.

In *sinkhole* attacks, a misbehaving node attracts surrounding nodes with unfaithful routing information, and then alters the data passing through it or performs other attacks, such as grayhole. Existing mechanisms against sinkhole are inefficient because of misbehaving nodes take off their correct participation in the routing process. Finally, due to the security credential for joining the network, a node cannot lie about its identity and, hence the network is protected against attacks that fake identities, such as Sybil attacks.

4 The SAMNAR architecture

The SAMNAR, Survivable Ad hoc and Mesh Network ARchitecture, is inspired on the human body immune system. It defines a new security management approach by the adaptive coordination of preventive, reactive and tolerant defense lines. Preventive defense lines comprise security mechanisms attempting to avoid attacks, such as cryptography, firewalls and access control techniques. Reactive defenses try to detect and react against intrusions by security mechanisms, such as reputation systems and intrusion detection systems. Tolerant defenses aim to mitigate damages caused by attacks or intrusions, and recover compromised services. Redundancy is one of the techniques employed to reach recovery.

SAMNAR focuses on supporting essential services, as link-layer connectivity, routing and end-to-end communication. SAMNAR consists of three modules: **survival**, **communication** and **collect**. Fig. 1 illustrates these modules considering a network node/device. The **survival module** holds five independent components, being four of them related to SAMNAR properties – resistance, recovery, recognition and adaptability – and a control component. These properties represent, respectively, the network capability of repelling attacks; detecting attacks and evaluating the extent of damage; restoring disrupted information or functionalities; and quickly incorporating lessons learned from failures and, thus, adapting to emerging threats.

The *resistance component* consists of preventive mechanisms, such as firewall, access control, authentication and cryptography. This component works in a self-protection and self-adjusting fashion where preventive mechanisms and their configuration will be changed depending on the network or environment conditions. The rule of a distributed firewall, for instance, can be more rigorous in certain environments, while simpler rules can be applied in more secure environments. Another example is the cryptographic key size that can be larger depending on the environment or network condition.

The *recognition component* comprehends reactive mechanisms to identify

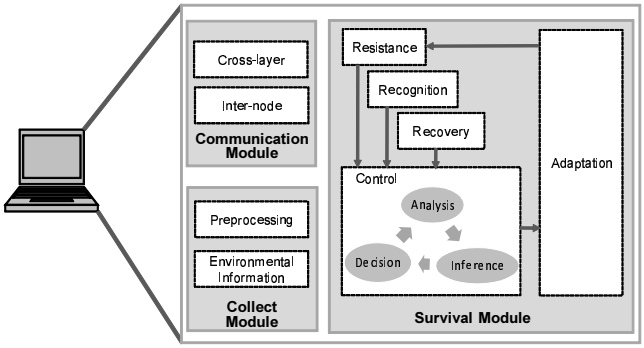


Figura 1: SAMNAR Architecture

malicious behaviors, such as IDSs, reputation systems, anti-malwares and anti-spammers. Recognition mechanisms can have also the capability of reacting and stopping intrusions. All the mechanisms will be reconfigured if necessary by the adaptation component. New configurations, such as IDS rules, depend on the network and environment conditions. This component provides to the control component information about detections, trustworthiness of neighbor devices, among others.

The *recovery component* consists of mechanisms to enhance the attack tolerance of network essential services. Mechanisms to restore disrupted information or functionality, such as replication or redundancy, have been employed as tolerant mechanisms. The application of two cryptography algorithms successively and the replication of message pieces are examples of redundancy. Sending redundant message pieces by different routes increases the probability of the message to be received by the destination node and the possibility of message recovery in case of piece losses. However, redundant strategies should consider resource limitations, as well as service and application requirements [21].

The *adaptation component* complements the previous ones. It is responsible for adapting preventive, reactive and tolerant mechanisms, as well as local or network configurations. It can make the replacement of a given protocol or a defense mechanism, such as changing a weaker cryptographic algorithm for a stronger one, depending on the necessities and requirements on time. Further, this component can change the key size of a cryptographic algorithm, the rules into an IDS or a firewall, the used route and others in accordance with the network condition or decisions taken by the control component.

The *control component* manages and coordinates all modules in the architecture. It receives information from communication and collect modules as well as from the resistance, recognition and recovery components. Its purpose lies in correlating and analyzing all information in order to make inferences

and decisions. All decisions feed the adaptation component that defines and updates parameter values of other modules or components. Adaptation component learns with taken actions and later, it can take the same action if the node or network presents a similar condition.

The **communication module** is responsible by cross-layer and inter-node communications. The *inter-layer component* offers the exchange of information inter-layers. It supplies information from different network layers to control component, hence it takes decisions based on all network layers and achieves the survivability for all of them. The *inter-node component* provides communication, exchange and synchronization of information among the nodes aiming to guarantee the survivability of the whole network. Example of this information is the node configuration or network intrusion detections.

The **collect module** holds mechanisms to gather all data required by the survival module. The collect module is composed of the *preprocessing component* and the *environmental information component*. The first one is exploited when gathered data need to be processed before sending to the survival module. Normalizations, previous calculations and others are examples of preprocessing used to facilitate analyses and inferences of the survival module. The second component stores information gathered periodically about the network conditions, sending it to the survival module when required.

5 Survival Path Selection Scheme

Since routing is an essential service for WANETs, we develop a path selection scheme based on the SAMNAR architecture. The path selection scheme aims to choose routes that can guarantee the routing service even under attacks or intrusions, using both *conventional criteria* and *security criteria* for choosing the most survivable paths. Conventional criteria allow the resource and performance management, and we employ remaining energy (energy rate) and path length as network information (*environmental information*). Further, other criteria could be used, as path throughput or link stability. Defense mechanisms support security criteria, being **certificate expiration time** and **cryptographic key length**, criteria from preventive defenses; **node reputation**, from reactive defense; and **path degree**, criterion representing tolerance. Other security criteria could also be added, such as the type of cryptography and the percentage of false positive or false negative.

Fig. 2 illustrates the correlation between the SAMNAR architecture and its instance, the survival path selection scheme. We describe each module and its application on the path selection scheme as follows.

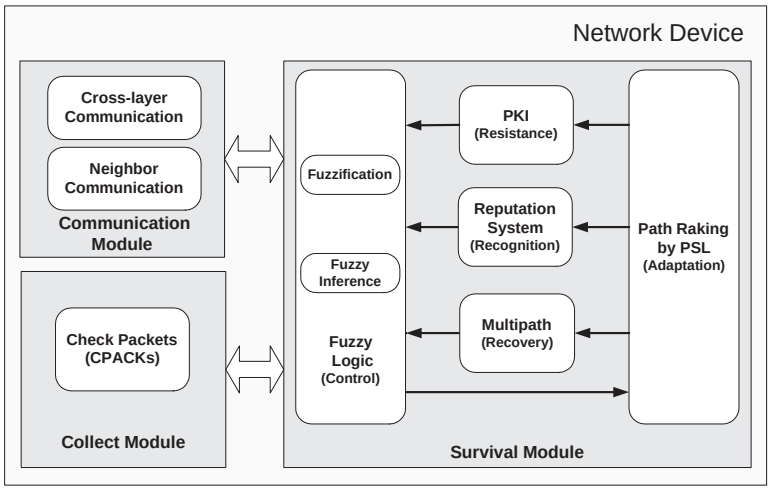


Figura 2: Survival path selection scheme

5.1 Survival module

Each component of the survival module, as resistance, recognition, recovery, adaptation and control, are specified for the path selection in this subsection. The resistance component consists of a public key infrastructure that supports cryptographic operations and digital certifications. A reputation system composes the recognition component and the use of a multipath routing protocol achieves properties defined by the recovery component. The adaption and control components comprise fuzzification, fuzzy inference and path ranking.

The path selection scheme employs fuzzy logic [22] as control component. *Fuzzy logic* (FL) is a multivalued logic, allowing the definition of intermediate values between conventional measures, like true or false. FL correlates security and conventional criteria and provides values to select the most survivable path. Since the high dynamism and uncertain states of WANETs make difficult to determine thresholds and patterns, FL was used for being a powerful tool to take decisions based on imprecise and noisy data [22, 23].

The control component calculates a path survivability level (PSL) for each route following the FL stages: input fuzzification and inference. Based on PSL, the adaptation component ranks paths, being the most survivable route chosen for data transmission. However, the PSL value can change with criterion updates resulted from new data collections. Thus, the set of selected routes can also adaptively change.

Fuzzy inference process maps inputs to outputs by rules that follow the form **if-then**. Inputs and outputs values lie in fuzzy sets into the interval

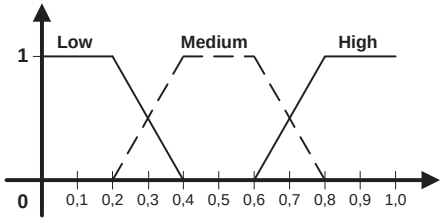


Figura 3: Energy (E) function

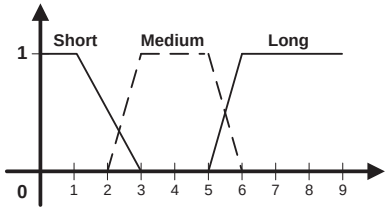


Figura 4: Path length (L) function

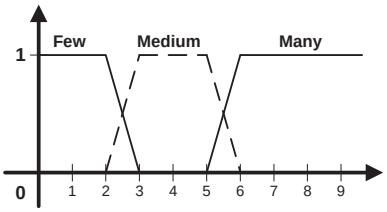


Figura 5: Path degree (D) function

[0.0,1.0], in which 0.0 represents absolute falseness and 1.0 represents absolute truth. The set of rules composes the knowledge base of the path selection scheme, generating outputs used to make decisions. Path survivability levels are estimated by fuzzy inference process.

5.1.1 Fuzzification

Fuzzy rules manipulate values in the fuzzy interval from 0.0 and 1.0, even if input values lie in different intervals. Conventional and security criteria used as input values are represented by linguistic terms as “strong”, “weak”, “large”, “small”, among others. Each criterion has a set of linguistic values, which are mapped to fuzzy interval by membership functions. This process is called *fuzzification* and follows trapezoidal functions since they have been extensively used in real-time applications due to their simple formulas and computational efficiency [23, 24].

Distinct and independent conditions, represented by conventional criteria, affect differently path survivability level. Remaining energy, for example, has impact on survivability since nodes with higher energy rate can participate in the path by a longer time period enhancing path stability. Stable paths are preferred for decreasing the number of route discoveries caused by path breaks. Route discoveries enable the participation of new malicious nodes in routes, reducing the probability of survivability. Further, paths with high remaining energy can tolerate overload attacks. Hence, high remaining energy improves the survivability level.

Remaining energy is represented by the following linguistic terms: *low*, *medium* and *high*, in which Fig. 3 represents the membership function of energy rate (E). Fuzzy inference considers the remaining energy of each path (E^i), estimated by the minimum value among the rates of all n nodes in the path i. Thus:

$$E^i = min(E_1^i, E_2^i, \ldots, E_n^i) \tag{1}$$

Path length (L) denotes the number of intermediate hops between the source node and the destination node. Higher path length results in lower performance. For security, higher path length augments the probability of existing malicious nodes in the path. Thus, shorter paths are preferred than longer ones. Path length variable has three fuzzy sets: *short*, *medium* and *long*. Based on results of [25] for the average path length, paths with 1 or 2 hops are considered short, paths with 2, 3, 4, 5 and 6 are considered medium, and paths with more than 6 intermediate hops are considered large. Fig. 4 presents the membership function for path length.

Security mechanisms generate security criteria values used to take decisions. Certificate expiration time (T), for example, presents two fuzzy sets, *imminent* and *far*. If the certificate expires within 10s or less, it is imminent, and far when it expires within 60s or more. These values were chosen based on results found in [26], in which they argue that the majority of path durations lie in the interval of 10 and 20 seconds. Expiration time smaller than path duration enhances the likelihood of the certificate to be compromised due to updates when the path is still alive. Thus, more imminent certificate expiration time reduces the survivability level and this criterion represents preventive defense lines.

For cryptographic key length (K), two fuzzy sets are defined, *short* and *long*, as in [27]. If the secret key is 40 bits or less, it is considered short, and it is long with 128 bits or more. Longer key lengths make cryptographic mechanisms more resistant to attacks. Thus, the survivability level is directly proportional to the key length.

The reputation (R) of a path i is the lowest node reputation value in the path. Considering the existence of a reputation system in the network that generate values in the interval between 0.0 and 1.0 to indicate node behavior, the path reputation linguistic variable owns two fuzzy sets, *good* or *bad*. Path with higher good reputation values are preferred. Good reputations are those with values equal or higher than 0.8. The reputation of the path i with n nodes is calculated as:

$$R^i = min(R_1^i, R_2^i, \ldots, R_n^i) \tag{2}$$

Path degree (D) represents tolerant defense lines, being defined by the minimum node degree among all n nodes participating in a path i (Eq. 3). The node degree is defined by the number of its direct neighbors. Higher neighbor number augments the probability of finding redundant or alternative paths, and thus can improve the tolerance and survivability. Path degree linguistic variable has three fuzzy sets: *few*, *normal* and *many*. Fig. 5 presents the membership function for this linguistic variable.

$$D^i = min(D_1^i, D_2^i, \ldots, D_n^i) \tag{3}$$

The fuzzy logic inference results in the path survivability level (PSL). Knowing the independence among the six criteria, their relation with PSL follows the Eq. 4:

$$PSL \propto E \bullet K \bullet R \bullet D \bullet \frac{1}{L} \bullet \frac{1}{T} \tag{4}$$

Only for exemplifying the importance of security criteria and their impact in order to make decision on PSL, Fig. 6 correlates K and L criteria, note that with L up to 5, L is not an important factor to improve the PSL, being K more than 50 the main factor. However, for L higher than 5, both L and K improve the PSL, although it only achieves 0.45. As defined in Eq. 4, PSL is minimized by high values of L.

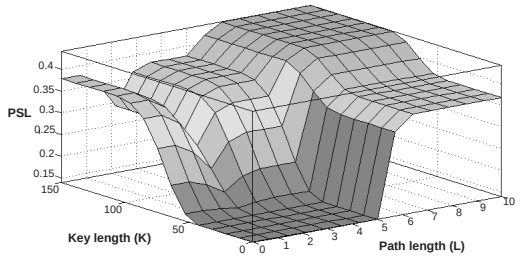


Figura 6: Correlating selection criteria and PSL

5.1.2 Fuzzy inference and path ranking

Fuzzy inference follows fuzzy rules composed of fuzzy sets. In our case, Larsen's max-product inference mechanisms [22] calculate the path survivability level. For each linguistic variable, their values on fuzzy set are combined by means of algebraic product operation. Next, the highest PSL value is chosen by the adaptation component for data transmission.

The adaptation component ranks each path by its PSL, choosing the path with the highest PSL. The selected path is used until it is broken or until a

new data collection phase occurs. If the path is broken before that, the next path with higher PSL is used. If a new data collection phase finishes and values change the path ranking, the source and destination nodes will use the most survival path. This process allows the self-adaptation of routing on network changes.

5.2 Collect and communication modules

Special packets, called check packets (CPACKs), are sent to perform periodic data collections. Each CPACK owns a cryptographic message digest to prevent forgeries. After generating the message digest, nodes send check packets for all paths the node knows. The route discovery process follows the specification of the routing protocol being independent of the path selection scheme. Routes associate a source to a destination node, being data collections initialized by source nodes. CPACKs are forwarded hop by hop to the destination and, in each intermediate nodes, CPACKs gather criteria values and store them on specific fields. Arriving at the destination node, it sends the packet back. The packet can use any route to return to the source.

A CPACK owns eight main fields: *destination IP address*, *source IP address*, *way*, *energy rate*, *reputation*, *validation*, *path degree* and *hop*. Source and destination addresses assist the packet routing and the field "way" indicates if CPACK is going to or coming back from the destination node. If "way" value is 0, it is going to destination node and collects data. If "way" value is 1, the packet is just forwarded, without gathering data. "Energy rate", "reputation", "validation" and "path degree" fields store, respectively, the smallest value of remaining energy, node reputation, expiration time and node degrees found in the path. The "hop" field accumulates the number of intermediate nodes in the path.

Fig. 7 illustrates the data collection phase, where a source node (node A) has discovered two routes, R1 and R2, to achieve the destination node (node B). These routes have been found by the discovery phase of the routing protocol, being independent of this scheme. With a time interval equal to x seconds between one data collection and other, one CPACK is sent to each known path. After data collection, source node calculates the survivability level for each path (PSL).

CPACKs are lost when they do not find route to the destination node or to come back to the source. Thus, the survivability level of this path remains with initial values. As it has the smallest values among other paths, it is not selected. The path survivability level will be updated with the next data collection.

Different layers of the protocol stack provide data used for path selection.

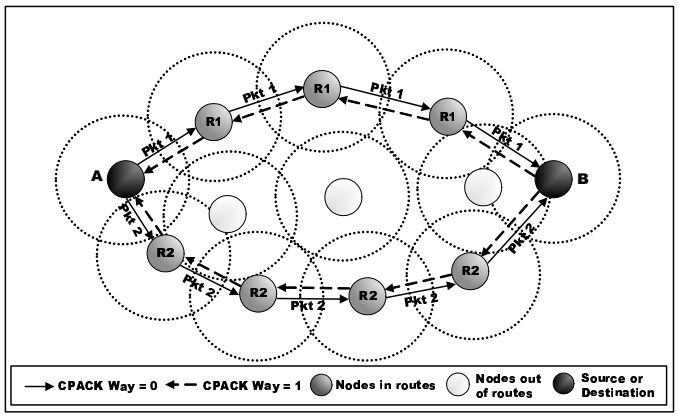


Figura 7: Data collection phase

Further, few of criteria values result from the cooperation among nodes, in general, neighbors. Criteria values from the PKI are generated on the application layer and used by the routing layer. Neighbor nodes supply reputation values generated on the application layer.

6 Evaluations of the path selection scheme

We analyze the protocol-independent path selection scheme using Network Simulator (NS-2) version 2.30. Simulations were performed considering two networks: an ad hoc network with two-way random mobility, called **CASE 1**, and an urban mesh network employing a realistic node mobility and signal propagation, called **CASE 2**. For the sake of evaluation, the path selection scheme was instantiated on the routing protocol AOMDV (On-demand Multipath Distance Vector Routing in Ad Hoc Networks) [28]. This protocol was modified to provide security criteria values and to execute functionalities defined as *data collection*, *fuzzy inference* and *path selection*. Multipath node-disjoint routes were used in order to provide redundancy.

Analyses evaluate two main aspects: the survivability improvement achieved by the path selection scheme and its impact on network performance. For this, we compare results produced by the AOMDV modification, called AOMDV-SL, with those yielded by AODV and AOMDV in the presence of **black-hole (BH)** or **grayhole (GH)**, and combinations of both attacks with the **sinkhole (Sink)** attack. AOMDV-SL provides preventive, reactive and tolerant security information regardless of a specific secure protocol, reputation scheme, cryptographic mechanism or key distribution infrastructure. AOMDV has no security mechanisms against the entire set of strong

colluding attacks; however we have considered them due to their performance.

We have used the following metrics for evaluating the survivability improvement achieved by our scheme and its impact on the network performance. For all these metrics, we have calculated a confidence interval of 95%.

- **Misbehavior drop ratio (MDR)** - measures the proportion of data packets dropped due to attacks over the total of data packets dropped. For the sake of analyses, we have implemented mechanisms on NS-2 to log data packets maliciously dropped.
- **Packet delivery ratio (PDR)** - calculates the percentage of data packets delivered at the destination over the total amount of data packets sent by the source.
- **End-to-end delay of data packets (E2E delay)** - consists of propagation delays, queuing delays at interfaces, retransmissions delays at the MAC layer, as well as buffering delays during route discovery step.

6.1 CASE 1: Wireless ad hoc networks

Simulation settings

The IEEE 802.11 protocol operating with the distributed coordination function (DCF) is used as medium access control (MAC) protocol. The radio model presents similar characteristics to a commercial Lucent's WaveLAN radio interface with a nominal bit-rate of 2 Megabit per second (Mb/s) for the shared-media radio and nominal radio ranges of 100 and 250 meters. The radio range of 100 meters was used to force a higher number of nodes in multi-hop paths.

The mobility model applied is the random way-point model, in which node speeds are randomly chosen between zero meters per second (m/s) and a maximal speed (M) of 1 m/s or 15 m/s. Pause time was fixed to 100 s minimizing the impact of network dynamism in the results. The data traffic used in the simulations is CBR (Constant Bit Ratio) with 20 source nodes defined randomly. Each source generates data packets of 512 bytes and transmits them with a rate of 4 packets per second (pkt/s). Data traffic sessions happen at a random time in the simulation. The network interface queue size of the nodes was set to 64 packets for routing and data packets.

The network area dimensions were fixed for all simulations in 1000 m by 300 m, and the total number of nodes n placed randomly in this area is

of 50 nodes. In the beginning of each simulation, malicious nodes are chosen randomly from the total number of nodes. The percentage of number of malicious nodes varies from 0% up to 50%. AODV and AOMDV use configuration parameter values defined in the RFC 3561 [29], since these values were considered as the best ones for the performance of both protocols. Examples of configuration parameters are route lifetime, time to live (TTL) of Internet Protocol (IP) header packets and the interval between hello messages. The total simulation time was 500 seconds and each plotted point is an average of 35 simulations.

Simulation results

First, we analyze survivability improvements achieved by our scheme. Fig. 8 compares the MDR resulted from AODV, AOMDV and AOMDV-SL protocols under different attacks. Also in Fig. 8, we examine the percentage of data packets dropped due to blackhole (BH), sinkhole combined with blackhole (Sink-BH) and sinkhole combined with grayhole (Sink-GH) attacks for all protocols. We observe that BH attacks result always in the highest ratio of packets dropped due to attacks (MDR) independent of the protocol. Considering this aspect, we verify that our scheme has improved the survivability of data packet, that is, it has reduced the MDR value in the presence of the three attacks. AOMDV-SL decreases the MDR in relation to other protocols by 30% up to 50% of those produced by AODV or AOMDV in the presence of up to 20% of misbehaving nodes in the network. This reduction tends to decrease with higher percentages of misbehaving nodes. Comparing the behavior of AOMDV-SL when the maximal speed M of nodes is 1 m/s and 15 m/s, we verified that the MDR value is practically the same for both situations, independent of the percentage of misbehaving node.

We performed some experiments to examine the impact of the six criteria in the decision scheme and, consequently, in the results. For this, we compare also in Fig. 8 the results of simulations where nodes hold radio range (r) of 250 m with results where nodes hold r of 100 m. In scenarios with r of 100 m, some criteria will be forced to yield different behaviors, such as higher path lengths and higher node degree.

In Fig. 8, we verify that the behavior detected in results for r of 250 m is also detected in results for r of 100 m. However, we observe that globally our scheme presents a slighter improvement of data packet survivability for r of 100 m than for r of 250 m. Further, the ratio of dropped packets due to attacks has been reduced for all protocols independent of attack type. We investigate these aspects by means of Fig. 9. It compares the criteria values for r of 250 m and 100 m in the presence of BH attacks in MANETs. We

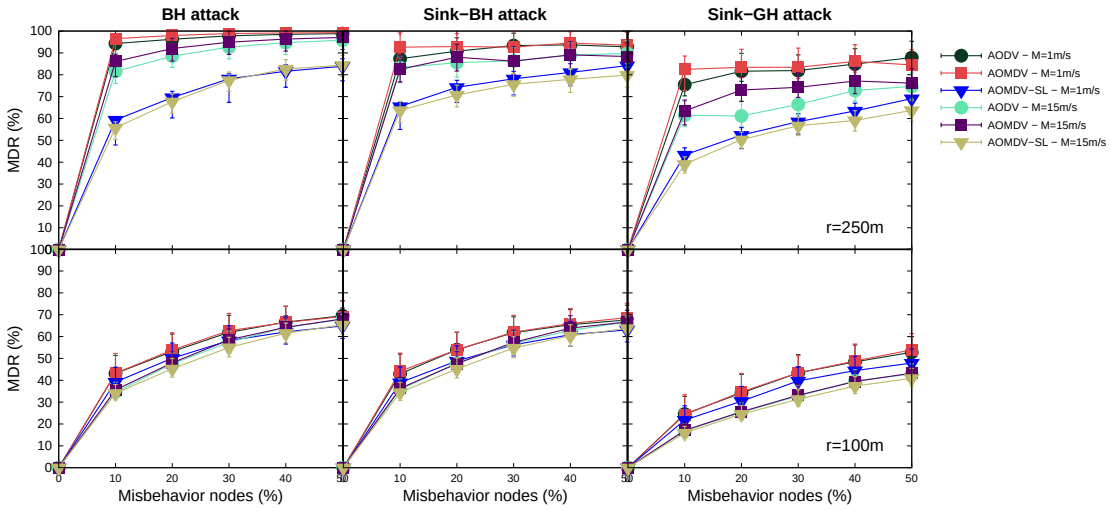


Figura 8: MDR in MANETs under different attacks

show values for a percentage of misbehaving nodes of 25%. However, based on the results from other percentages of misbehaving nodes and different attacks, we observed that the behavior represented here is independent of the percentage of misbehaving nodes.

In Fig. 9, we can see that the increase in the value of r results in slight differences for the values of energy (E), reputation (R), cryptography key length used by the nodes (K) and certificate expiration time (T). We emphasize that changes in the energy are small and they cannot be observed in these figures. On the contrary, the increase in r value provides great changes in path length (L) and node degree (D).

With r of 250 m (at the right side in Fig. 9), the network has always higher node degree and short path length, considering both maximal node speed, 1 m/s or 15 m/s. As we have assumed in Section 5, short path lengths are better for network survivability since they reduce the probability of misbehaving nodes in the paths. In the same way, a higher node degree increases the network redundancy due to the possibility of finding more routes from the data source and destination. These considerations are shown in Fig. 8, where results from simulations with r of 250 m are better than the those produced by simulations with r of 100 m.

Fig. 10 compares the results of PDR for all evaluated protocols considering, respectively, r of 250 m and 100 m. For all protocols, as higher the percentage of attacks, lower is PDR. We observe that AOMDV-SL under BH attacks and r of 250 m results in a slight decrease in PDR of about 5% up to

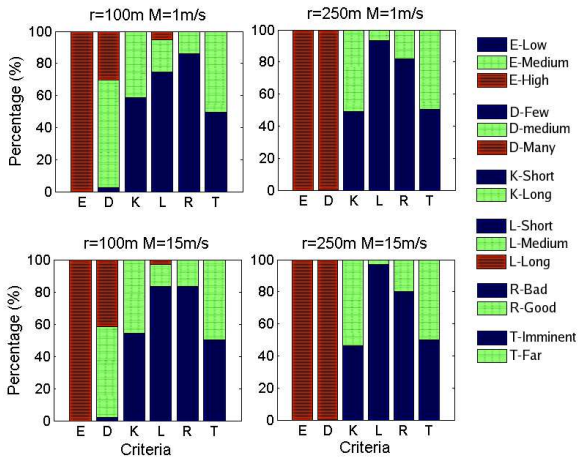


Figura 9: Criteria values

10% in relation to AODV and AOMDV. This decrease tends to be irrelevant when the network is under Sink-BH or Sink-GH attacks, being always into the confidence interval of PDRs provided by other protocols.

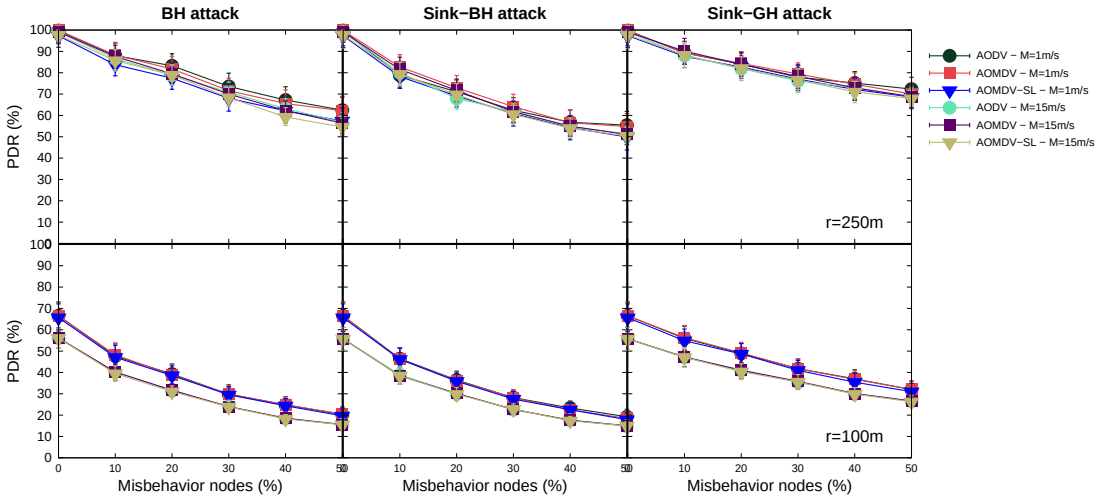


Figura 10: PDR in MANETs under different attacks

As well as for r of 250 m, the PDR produced by AOMDV-SL with r of 100 m varies in about 5% up to 10% in relation to the PDR of AODV or AOMDV. However, the PDR of AOMDV-SL is higher than those produced by AODV or AOMDV in lower percentage of misbehaving nodes, and this difference tends to be irrelevant for higher percentages. Moreover, the PDR

behavior is similar considering the maximal speed of the nodes 1 m/s or 15 m/s.

In Fig. 11, we examine the impact of our scheme on the network latency. When r is equal to 250 m, AOMDV-SL increases the network latency in about 0.10 s for M of 15 m/s, and in about 0.15 s for M of 1 m/s. The difference between the latency produced by AOMDV-SL and by other protocols is independent of the attack and is almost constant for all misbehaving node percentages.

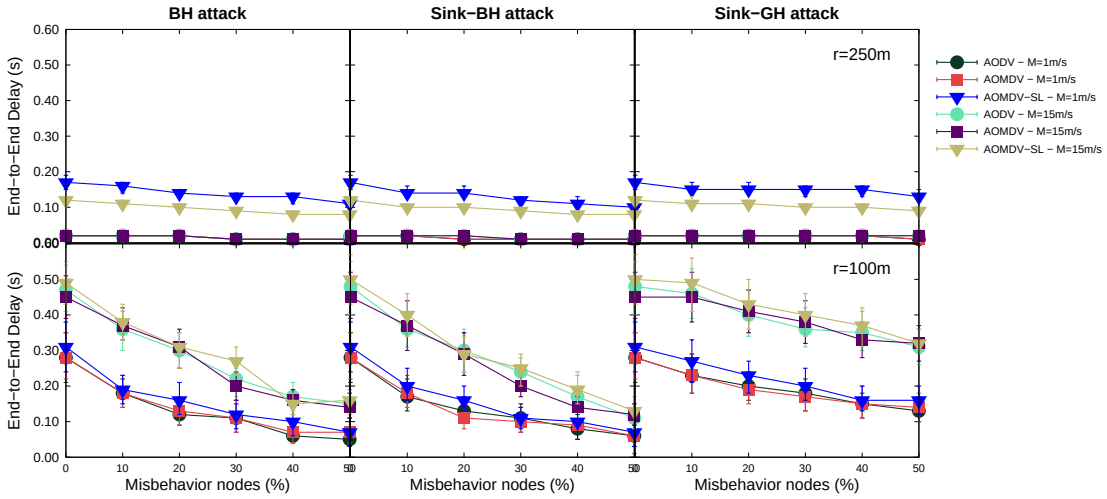


Figura 11: Latency in MANETs under different attacks

For r of 100 m, the maximum node speed M presents a great impact in the network latency for all protocols being higher for the cases where M is equal to 15 m/s. When compared the AOMDV-SL latency with the latency of AODV and AOMDV on the same value of M, we verify that their latency is similar. Moreover, we observe that for all protocols the latency tends to decrease with the increase in the percentage of misbehaving nodes. The network latency under Sink-GH attack presented the worst case for all protocols when the percentage of misbehaving nodes is higher than 30%.

6.2 CASE 2: Wireless mesh networks

Simulation settings

Nodes use the IEEE 802.11 distributed coordination function (DCF) as medium access control (MAC) protocol and IEEE 802.11b as radio model for communication with transmission power of 15 dBm and received card sensitivity of

-93 dBm, receiving at 1 Mb/s. If the channel gain is lower than -67 dB then it is not possible to decode the transmission with marginal reliability. The used gain margin was 3 dB, requiring above -64 dB of communication channel gain.

We have employed Udel Models in order to have a realistic mobility and signal propagation [30]. Udel Models are composed of signal propagation and mobility patterns in which network environment is considered. The environment includes urban and suburban features, such as buildings, sidewalks, and roads, and within this environment, pedestrian mobile nodes move from office to office through hallways and along sidewalks, while vehicle nodes move along roads and aircraft move anywhere in the three dimensional space above the city. Buildings and other reflective objects in this environment influence the signal propagation, as well as node mobility.

Each simulation was composed of 500 mobile nodes and 29 fixed infrastructure nodes distributed in an area of 500 meters by 500 meters. In these scenarios, we observe our scheme in a high density network. Fig. 12 illustrates this area representing the core of Chicago city and indicating the positions of the fixed nodes. Mobility and propagation models consider buildings and streets in this area in order to define node movement and its signal propagation. Mobile nodes have pedestrian characteristics, such as the speed of mobility and activities executed throughout the day.

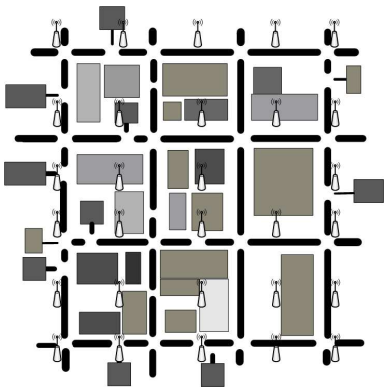


Figura 12: Chicago city core: fixed nodes

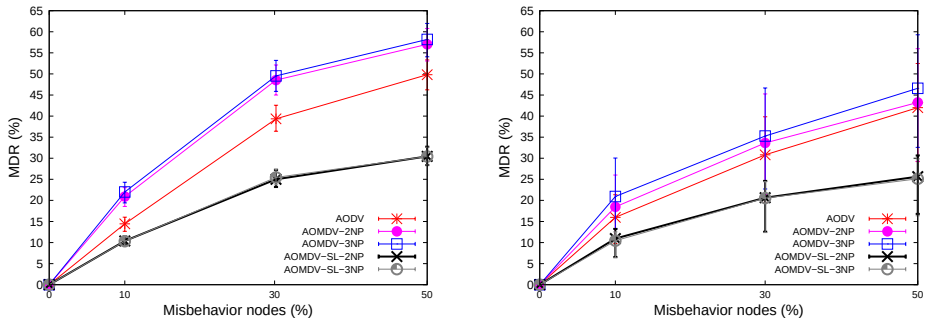
Evaluations investigate two situations. In **Situation 1**, we changed the node mobility and signal propagation for each simulation in order to verify our scheme under different network movement patterns. Further, three different periods of the day were taken into account in order to diversify the sample analyzed since Udel models differentiate pedestrian activities throughout the day. The mobility and propagation scenarios of each simulation are deter-

ministically described by input files. Due to the complexity in generating these files, Udel model web site offers some of them. We used files from version 1.2 and restricted to 15 the number of simulations for the first case because there are only 15 available files. In **Situation 2**, we observed our scheme under 35 independent simulations with different traffic behavior in each one, but with the same transmission rate (3 pkt/s).

Simulation results

We investigate the behavior of the misbehavior drop ratio (MDR) in Wireless Mesh Networks under Backhole (BH) attacks. These attacks have been chosen for analyses based on the results of the CASE 1. BH attacks produce the highest ratio of packets dropped due to attacks independent of the protocol and for both maximal node speed examined. In Fig. 13, we consider the maximal number of paths (NP) equals to 2 and 3 for AOMDV and AOMDV-SL.

In Fig. 13, we observe that our scheme, AOMDV-SL, increases the survivability of data packets since it reduces the ratio of packets dropped due to attacks evaluated by the MDR. This can be observed when compared the MDR yielded by AOMDV-SL with AODV, AOMDV-2NP and AOMDV-3NP. The MDR of AOMDV-SL-2NP and AOMDV-SL-3NP reduces of 5% up to 28% the MDR found by the other protocols. We note also that this reduction is higher in the presence of elevated percentage of misbehaving nodes. We can also see that MDRs resulted from scenarios over different periods of the day (Situation 1) are lower than scenarios where the network was under different traffic behaviors (Situation 2).



(a) Situation 1 (b) Situation 2

Figura 13: MDR in WMNs under BH attacks

Fig. 14 compares for each protocol under 30% of misbehaving nodes the percentage of dropped packets caused by expiration of packet TTL (TTL),

the lack of routes (NRTE), the overload in the queue (IFQ) and misbehaving nodes (MIS). We verify a reduction in the percentage of MIS drops, as well as NRTE drops, resulted from the existence of multiple paths and from the AOMDV failure recovery mechanism. The percentage of TTL drops stays almost the same, whereas the percentage of IFQ drops increased due to data collections of our scheme.

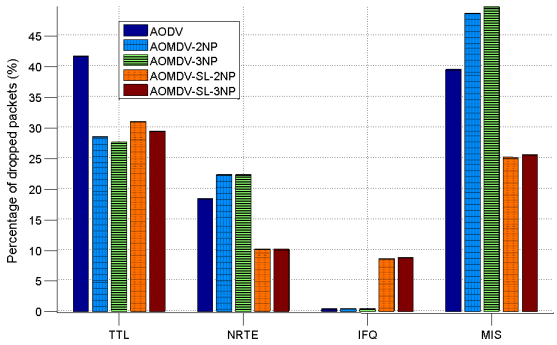
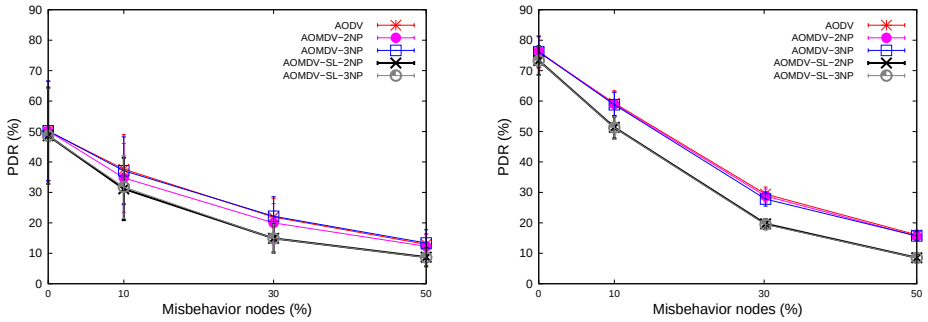


Figura 14: Comparing dropped packets

The impact of our path selection scheme on PDR and latency are presented in Fig. 15 and Fig. 16, respectively. The PDR of AOMDV-SL, independently of the NP value, decreases in relation to the PDR of AODV or AOMDV. The reduction on PDR using AOMDV-SL tends to increase with the rise in the misbehaving node percentages. However, it is always between 5% and 10%. The PDR for all evaluated protocols is lower in Situation 1, where different periods of the day are considered.

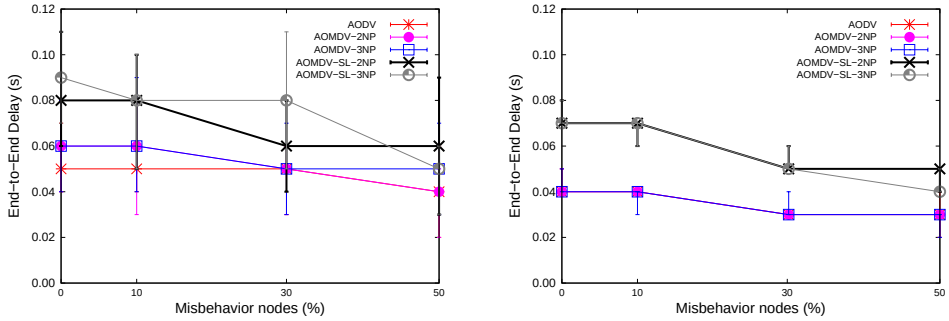


(a) Situation 1 (b) Situation 2

Figura 15: PDR in WMNs under BH attacks

AOMDV-SL increases the network latency in relation to AODV and AOMDV. The rise in latency is of about 0.10 s for Situation 1 and about 0.04

s for Situation 2. This difference tends to be irrelevant for higher percentages of misbehaving nodes in the network.



(a) Situation 1 (b) Situation 2

Figura 16: Latency in WMNs under BH attacks

7 Conclusion and future work

This work presented a survivable management architecture for ad hoc and mesh networks called SAMNAR. Its goal lies in making these networks able to provide essential services even in face of attacks and intrusions. SAMNAR is based on a coordinated integration among the preventive, reactive and tolerant defense lines, being able to self-adapt to different network conditions.

Based on SAMNAR, we designed a protocol-independent path selection scheme where a low-cost mechanism correlates security and conventional criteria to better choose survival paths and self-adapting to attacks and failures. We evaluated survivability improvements and performance of our scheme by simulations where realistic node mobility and signal propagation were taken into account for WANETs. Results showed that our approach significantly decreases the impact of routing attacks with minimal performance loss. As future works, adaptive aspects must to be enhanced to improve the network performance and survivability.

Referências

[1] Y. Hu, D. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," *Journal ad hoc networks*, vol. 01, pp. 175–192, 2003.

[2] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," in *IEEE INFOCOM*, vol. 4. Washington, DC, USA: IEEE Computer Society, 2004, pp. 2404–2413.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *ACM MobiCom*. New York, NY, USA: ACM Press, 2000, pp. 255–265.

[4] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks," in *ACM WiSe*. New York, NY, USA: ACM Press, 2003, pp. 41–50.

[5] M. T. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy, "A reputation-based mechanism for isolating selfish nodes in ad hoc networks," in *MOBIQUITOUS*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 3–11.

[6] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *ACM MobiHoc*. New York, NY, USA: ACM Press, 2001, pp. 299–302.

[7] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE*, vol. 6, no. 3, pp. 106–107, 2002.

[8] I. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. 23–30, 2005.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, pp. 38–47, February 2004.

[10] A. Pras, J. Schonwalder, M. Burgess, O. Festor, G. Perez, R. Stadler, and B. Stiller, "Key research challenges in network management," *IEEE Communications Magazine*, vol. 45, no. 10, pp. 104–110, October 2007.

[11] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable Secure Computer*, vol. 1, no. 1, pp. 11–33, 2004.

[12] K. John, C. Dennis, H. Alexander, W. Antonio, C. Jonathan, H. Premkumar, and D. Michael, "The willow architecture: comprehensive survivability for large-scale distributed applications," in *DSN*. Washington, DC, USA: IEEE Computer Society, 2002.

[13] A. Keromytis, J. Parekh, P. N. Gross, G. Kaiser, V. Misra, J. Nieh, D. Rubenstein, and S. Stolfo, "A holistic approach to service survivability," in *ACM SSRS*. New York, NY, USA: ACM, 2003, pp. 11–22.

[14] F. Wang and R. Upppalli, "SITAR: a scalable intrusion-tolerant architecture for distributed services," in *DISCEX*, vol. 2, 2003, pp. 153–155.

[15] T. Aura and S. Mäki, "Towards a survivable security architecture for adhoc networks," in *International Workshop on Security Protocols*. London, UK: Springer-Verlag, 2002, pp. 63–73.

[16] M. Virendra, S. Upadhyaya, V. Kumar, and V. Anand, "SAWAN: a survivable architecture for wireless LANs," in *IEEE IWIA*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 71–82.

[17] D. Kim, C. Yang, and J. Park, "Adaptation mechanisms for survivable sensor networks against denial of service attack," in *ARES*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 575–579.

[18] Y. Qian, K. Lu, and D. Tipper, "A design for secure and survivable wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 30–37, 2007.

[19] A. Tsirigos and Z. Haas, "Analysis of multipath routing-part i: the effect on the packet delivery ratio," *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 138–146, 2006.

[20] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," *IEEE/ACM Transaction Network*, vol. 12, no. 6, pp. 1049–1063, 2004.

[21] M. N. Lima, A. L. dos Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks." *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, 2009.

[22] L. A. Zadeh, "Fuzzy logic," *Computer*, vol. 21, no. 4, pp. 83–93, 1988.

[23] S. T. Welstead, *Neural Network and Fuzzy Logic Applications in C/C++*. New York, NY, USA: John Wiley & Sons, 1994.

[24] H. Liu, J. Li, Y.-Q. Zhang, and Y. Pan, "An adaptive genetic fuzzy multi-path routing protocol for wireless ad hoc networks," in *SNPD/SAWN*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 468–475.

[25] K. Seada, K. Westphal, and C. Perkins, "Analyzing path accumulation for route discovery in ad hoc networks," in *IEEE WCNC*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 4377–4382.

[26] Y. Han, R. J. La, A. M. Makowski, and S. Lee, "Distribution of path durations in mobile ad-hoc networks: Palm's theorem to the rescue," *Computer Networks*, vol. 50, no. 12, pp. 1887–1900, 2006.

[27] J. Nie, J. Wen, J. Luo, X. He, and Z. Zhou, "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks." *Fuzzy sets and systems*, vol. 157, no. 12, pp. 1704–1712, 2006.

[28] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in *IEEE ICNP*, 2001, pp. 14–23.

[29] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc on-demand distance vector (aodv) routing," Published Online, Internet Engineering Task Force, RFC Experimental 3561, July 2003. [Online]. Available: http://rfc.net/rfc3561.txt

[30] V. Sridhara and S. Bohacek, "Realistic propagation simulation of urban mesh networks," *Computer Networks*, vol. 51, no. 12, pp. 3392–3412, 2007.