An Architecture for Survivable Mesh Networking

Michele N. Lima*,†, Helber W. da Silva†, Aldri L. dos Santos‡, Guy Pujolle*

*Laboratoire d’Informatique de Paris 6 (LIP6) Université Pierre et Marie Curie
Paris, France 75016

†Computer Science Department Federal University of Ceará
Fortaleza, Ceará, Brazil 81531-990
helberhws@great.ufc.br

‡ Department of Informatics Federal University of Paraná
Curitiba, Paraná, Brazil 81531-990
aldir@inf.ufpr.br

Abstract—Wireless mesh networks have gained increasing interests, but the lack of security guarantee has retarded their deployment. Security solutions have applied preventive or reactive mechanisms, being inefficient to put all attacks off. We design a survivable architecture for ad hoc and mesh networks to enhance the network capability of providing essential services even in face of attacks or intrusions. Our approach integrates preventive, reactive and tolerant defense lines in a self-adaptive way. Based on our architecture, we create a survival path selection scheme, and evaluate it through simulations using urban mesh network mobility and propagation models. Results show a decrease in the impact of routing attacks with minimal performance loss.

I. INTRODUCTION

Wireless mesh networks (WMNs) are composed of two main node types, mesh routers and mesh clients, working in a multi-hop and self-organized way [1]. WMNs are a type of mobile ad hoc networks (MANETs) differentiating them from due to additional routing functions supported by mesh routers. These nodes maintain the mesh connectivity and hold minimal mobility, multiple wireless interfaces and less resource constraints than mesh clients.

WMN researches have tackled issues on network functionalities, such as routing and the integration of different technologies, without considering security [1]. However, the lack of security guarantees makes WMNs undependable, retarding their deployment. Mesh routing, for example, is exposed to many attacks and some of them are hard to prevent [1].

In general, existent WMN security solutions apply preventive or reactive mechanisms such as cryptography, firewalls or intrusion detection systems (IDSs) [1]. However, these solutions are inefficient to put all intruders and attacks off [2]. Solutions based on cryptography, for instance, are vulnerable to internal or denial of service (DoS) attacks, and efficient IDSs are difficult due to dynamic network topology. Survivability has gained interest from industry and research communities in the last years due to the limitations of security mechanisms [3]. Some architectures have been proposed to make WLANs, MANETs and WSNs survivable, i.e., able to provide essential services even in the presence of attacks and intrusions. However, none of them focuses on WMNs. Further, those architectures are specific for one given service using only one or two defense lines.

This paper presents a survivable architecture for ad hoc and mesh networks, called SAMNAR. Its goal is to offer essential network services, as connectivity, routing and communication, even in face of attacks and intrusions. Unlike classic security solutions, our architecture enhances the network survivability by a coordinated integration among preventive, reactive and tolerant defense lines. SAMNAR holds independent modules and components giving them flexibility and autonomy.

As a showcase, we use SAMNAR to build a protocol-independent path selection scheme for WMNs. Our scheme considers conventional and security criteria for choosing routes and self-adapting in case of attacks or failures. A low-cost computational mechanism correlates both criteria, being security ones provided by the three defense lines. We evaluate our scheme through simulations where realistic mobility and propagation models for urban mesh networks are used. These models consider the presence of buildings into simulations, yielding more realistic insights than those ones from simplistic models. Results show that our approach decreases the impact of routing attacks with low performance loss.

The rest of this paper is organized as follows. Section II depicts the related works. Section III details SAMNAR. Section IV explains the case study. Section V describes the simulation environment and results. Section VI presents conclusion and future works.

II. RELATED WORK

In the last years, researchers have applied survivability concepts in wireless and mobile networks. Those works can be categorized in those that improve the network survivability in face of failures without considering security as [4], and few ones that have proposed survivable architectures against intrusions and attacks [5], [6], [7], [8]. In [5], an architecture towards a survivable access control in ad hoc networks is proposed, being the survivability achieved by the creation of secure groups. In [6], an architecture is designed to improve WLAN survivability against attacks that harm access points. In [7] and [8], survivable architectures for WSNs have been developed, the former against DoS attacks and the latter against multiple attacks.

Though, for the best of our knowledge, no architecture was proposed for enhancing the survivability of essential services in WMNs. Some WMNs works on access control [9], authentication [10] and routing [11] have only sought to make them more resilient to attacks. In [11], an opportunistic and credit-based routing is proposed against DoS attacks where high-throughput links are selected to greedy forward data in.
a multipath way. Without addressing resiliency, other works have also emphasized the selection of routes in WMNs [1], [12], [13]. However, none of them utilize security criteria to take decisions.

In this work, we showcase our architecture building a survival path selection scheme that correlates security and conventional criteria. The correlation between both criteria seeks to enhance the network survivability with minimal of performance loss.

III. SURVIVAL ARCHITECTURE

Survivability is a network capability of providing essential services in a timely manner, even in occurrence of attacks, intrusions, failures or accident [3]. This section describes SAMNAR, a Survivable Ad hoc and Mesh Network ARchitecture whose goal is to offer network operations or minimal service levels despite passive or active attacks. SAMNAR is based on the cooperation of the three defense lines, preventive, reactive and tolerant, and on the capability of network adaptation.

In SAMNAR, preventive defenses, such as cryptography, firewalls and access control services, correspond the first obstacle to attacks. As these defenses block certain ones and are incapable of preventing others, reactive defenses as IDSs act to detect and stop them. However, reactive defenses also have limitations and some intruders can harm a giving node or the network. Thus, tolerant defenses work proactively to ensure the continuance of minimal service level by mechanisms as redundancy, until those preventive or reactive defenses can adapt them and take actions against attacks or intrusions.

SAMNAR contains the survival, communication and collect modules. Fig. 1 illustrates them considering a network node/device. The survival module holds five independent components, being four ones related to SAMNAR properties, resistance, recovery, recognition and adaptability, and the control component. The 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 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.

The recognition component comprehends reactive mechanisms to identify 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 will 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.

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 replace 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, the adaptation 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. The control component correlates and analyzes all information in order to make inferences and take decisions. All decisions are sent to the adaptation component that define and send satisfactory parameter values to other modules or components. Adaptation component learn with taken actions and later, it can take the same action if the node or network present 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 so that it takes decisions based on all network layers and achieves the survivability for all of them. The inter-node component provides communication, exchange and synchro-
nization 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. It is out of the architecture scope to define the collection method. However, the survival module specifies adaptively which data and information must be collected following its requirements. 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 treated 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.

IV. CASE STUDY: PATH SELECTION

Based on SAMNAR, we created a path selection scheme for WMN in order to show the use of our approach. This scheme utilizes both conventional criteria and security criteria for choosing more survivable paths. Conventional criteria allow the resource and performance management, and we chose remaining energy (energy rate) and path length as network information (environmental information). However, other criteria could be added or replace them such as path throughput, link stability and others.

We assume that WMN nodes employ at least one mechanism from each defense line corresponding thus to the resistance, recognition and recovery components of the SAMNAR survival module. For this case study we use cryptography and key management systems as resistance component; reputation systems as recognition component; and multiple routes as recovery component. Thus, security criteria comprise cryptographic key length, certificate expiration time, node reputation and path degree, but other security criteria could be applied.

A push-pull procedure collects periodically criteria values by check packets (CPACKs) (collect module). Nodes send one CPACK for each known path. As routes associate a source to a destination node, only source nodes initialize path verifications. CPACKs are forwarded hop by hop to the destination node and, in all intermediate nodes, criteria values are gathered, and either added to previous values in the packet or an average value is calculated with this value (preprocessing component).

When CPACKs return to source nodes, those values are analyzed (the analysis function of control component) and survivability path levels (PSLs) are calculated for each route (the inference function of control component). CPACKs are lost when they do not find route either to reach the destination node or to come back to the source node. Thus, a given path with lost CPACK remains with its previous PSL value and it will not be selected if its PSL value is smaller than the PSL value of other paths. PSLs are updated with each data collection.

As correlating many criteria and selecting an optimal path set is a NP-complete problem [14], source nodes can calculate PSLs by fuzzy logic (FL), for instance. FL is a multivalued logic, allowing the definition of intermediate values between measures like true (1.0) and false (0.0). Thus, the first step to calculate PSL is to normalize gathered values into an interval between 0.0 and 1.0 by trapezoidal functions (preprocessing component), as we already used previously in [15].

We defined normalization and fuzzy rules based on how each criterion affects the network survivability. High energy rates ($E$) allow nodes to participate in a given path by a longer time period, enhancing the path stability. Stable paths are preferred due to the decreasing in the route discovery number caused by path breaks. Route discoveries enable the participation of new malicious nodes in the routes, minimizing the survivability. Further, paths with a high energy rate can better tolerate overload attacks. Thus, high energy rates improve the survivability. Path length ($L$) is 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.

For security criteria, we classified certificate expiration time ($T$) as imminent or far. If the certificate expires in 10s or less, it is imminent, and far when it expires after 60s or more. Expiration times smaller than path durations enhance the risk of the certificate to be harmed due to updates when the path is still alive. Thus, more imminent certificate expiration time decreases the survivability. We categorized cryptographic key length ($K$) as short or long. If the secret key is 40 bits or less, it is deemed short, and it is long with 128 bits or more. Longer key lengths make encryptions more resistant to attacks.

The reputation of a given path ($R$) corresponds to the lowest node reputation value in the path. Considering the existence of a reputation system in the network, where values between 0.0 and 1.0 are generated to indicate the node behavior, paths with higher good reputation values are preferred. Good reputations are those with values equal or higher than 0.8.

Path degree ($D$) represents tolerant defense line, being defined by the minimum node degree of all nodes participating in a path. 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 it can improve the tolerance and survivability.

After value normalization, fuzzy rules are employed to calculate the PSL. Based on all these arguments and assuming the independence among the six criteria, the general rule to infer PSL values follows:

$$PSL \propto E \cdot K \cdot R \cdot D \cdot \frac{1}{L} \cdot \frac{1}{T} \quad (1)$$

After the PSL calculation, the survivability level of each path is ranked, being chosen the path with the highest PSL (the decision function of the control component). The chosen 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 the values change the path ranking, the source and destination nodes will use the most survival path. This process allows the routing self-adaptation to network changes.

V. EVALUATION

We evaluated our protocol-independent path selection scheme by NS-2 simulator version 2.30. Our simulations apply Udel models that gives realistic node mobility and signal propagation in an urban mesh network [16]. We assumed an area of about 500 sq meters in the core of the Chicago city where 29 infrastructure nodes are uniformly distributed, and 500 outdoor and indoor pedestrian mobile nodes move respecting building positions, traffic lights and others.

Nodes use the IEEE 802.11 distributed coordination function (DCF) as medium access control (MAC) protocol, and IEEE 802.11b as radio model for communications with transmission power of 15 dBm and received card sensitivity of -93 dBm, receiving at 1Mbps. 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.

CBR (Constant Bit Ratio) data packets are transmitted by 20 random source nodes with a rate of 3 packets per second (pkt/s), considering a video application. Each packet has 512 bytes and transmission sessions happen at random instants into 600s of simulation. Network interface queue size was set to 1000 packets for routing and data packets.

The AOMDV (On-demand Multipath Distance Vector Routing in Ad Hoc Networks) protocol was extended to support our path selection scheme, providing security criteria values and functionalities as data collection, fuzzy inference and path selection. Further, routes are compelled to follow the network infrastructure. Thus, a mobile node, when receiving a route request (RREQ) from an infrastructure node, waits 100 ms for relaying it. Simulations used multipath link-disjoint.

Analyses compare our extended AOMDV (AOMDV-SL) with original AODV and AOMDV under 0%, 10%, 30% and 50% of blackhole malicious nodes [1]. For AOMDV and AOMDV-SL, the used number of paths (NP) was 2 and 3.

Our evaluation investigates two cases. In the first one, we changed node mobility and signal propagation for each simulation in order to verify our scheme under different network movements. 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 deterministically 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 the second case, we observed our scheme under 36 independent simulations with different traffic behavior in each one, but with the same transmission rate (3 pkt/s).

Assuming a confidence interval of 95%, we introduce three metrics to evaluate the effectiveness of AOMDV-SL in reducing attack impact and its cost to the network performance. Misbehavior drop ratio (MDR) measures the proportion of packets dropped due to misbehave blackhole nodes over the total of data packets 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) measures the transmission delay of data packets delivered successfully. This delay consists of propagation delays, queuing delays at interfaces, retransmissions delays at the MAC layer, as well as buffering delays during the route discovery.

A. Results and analysis

Fig. 2 and 3 show simulation results for the cases 1 and 2, respectively. In the two cases, we observe similar behaviors for the three metrics, discriminating them only by numerical values. Case 1 presents lower numerical values than case 2, being justified by the different period of the day employed in the simulations. Further, we note that the increase in the number of paths used by AOMDV and AOMDV-SL results in slight differences for all metrics. This occurs due to the uniform distribution of infrastructure nodes in simulation areas that limits the number of different paths found between sources and destinations.

In the two cases, we observe similarly that our path selection scheme yields a significant reduction in the impact of blackhole attacks. The MDR of AOMDV-SL-2NP and AOMDV-SL-3NP decreases of 5% up to 28% the MDR found by AODV, AOMDV-2NP and AOMDV-3NP. We note also that the reduction in MDR rises in presence of elevated percentage of blackhole nodes in the network. In addition, Fig. 4 compares for each protocol under 30% of blackhole nodes the percentage of dropped packets caused by expiration of packet TTL (TTL),
the lack of routes (NRTE), overload in the queue (IFQ) and misbehavior nodes (MIS). As previously mentioned, we verify the reduction in the percentage of MIS drops as well as the reduction in the percentage of NRTE drops, resulted from the choice of more stable paths. The percentage of TTL drops stays almost the same, whereas the percentage of IFQ drops increased due to data collections of our scheme.

In summary, results demonstrate that the developed scheme minimizes significantly the impact of blackhole attacks in routing. A trade-off between the reduction of attack effect and network performance is within of the cost expected to the network control and management. Further, results show that this trade-off is minimized for high percentage of misbehaving nodes.

VI. CONCLUSION AND FUTURE WORK

This work presented a survivable architecture for ad hoc and mesh networks called SAMNAR. Its goal is to make them able to provide essential services even in the presence 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 built 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 our scheme by simulations where realistic node mobility and signal propagation were used. Results showed that our approach significantly decreases the impact of routing blackhole attacks with minimal performance loss. As future works, we plan to enhance recovery and redundancy aspects of path selection scheme in order to improve the network performance.

REFERENCES