An IDS-based Self-healing Approach for MANET Survival

Leila Mechtri, Fatiha Djemili Tolba, Salim Ghanemi, Damien Magoni

An IDS-based Self-healing Approach for MANET Survival

Leila Mechtri[1], Fatiha Djemili Tolba[2], Salim Ghanemi[3],
[1,2,3]Networks and Systems Laboratory (LRS), Badji Mokhtar University, Computer Sciences dept., P. O. 12, 23000 Annaba, Algeria.
[1]mechteri@lrs-annaba.net,
[2]fatiha.djemili@univ-annaba.org,
[3]ghanemisalim@yahoo.com,

Damien Magoni
University of Bordeaux, LaBRI
351, cours de la Libération, F-33405 Talence
magoni@labri.fr

ABSTRACT
Mobile ad-hoc networks are known to be highly vulnerable to various kinds of intrusions. Since not all of these intrusions are predictable, there might have some serious effects on the network and its nodes before being detected and completely removed. For that, even if the implications of intrusions could be minimized by the intrusion detection system MASID-R, still the need for the recovery of altered or deleted data is a vital step to guaranteeing the correct functioning of the network. In this paper, we present a recovery oriented approach for a self-healing MANET. It is based on the ability of MASID-R to assess the damage caused by the detected intrusions and aimed at enabling the supervised network to heal itself of those faults and damages. Results show that MASID-R is now, able to not only detect intrusions but, at the same time, to assess and fix the damages caused by those intrusions.

Keywords
Self-healing, agent, survivable network, intrusion detection, MASID-R.

1. INTRODUCTION
In recent years, there has been a growing interest in securing the mobile ad-hoc networks (MANET). Some researchers developed cryptographic approaches [1] to guarantee security while many others prefer using secure routing protocols [2][3]. Also, there has been, recently, a great tendency to develop intrusion detection systems (IDS) specifically designed to fit MANET requirements in terms of both security and constraints. However, the obtained security level does not always guarantee that the network is completely free of faults and malfunctioning. More specifically, some intrusions might have some undesirable effects on the nodes or network services being targeted by the intruder before being detected and completely removed. For that, the network should be designed in order to survive such situations and to heal the potential damages without or with minimal human intervention.

This has led to the emergence of the so-called self-healing techniques as essential complementary techniques to achieve truly autonomous survivable networks.

In our previous work [4], the proposed replication framework enabled our IDS called MASID (Multi-Agent System for Intrusion Detection), to recover from individual and/or multiple agent failures, thereby guaranteeing permanent protection of the network on which it is installed. However, the network is not yet reliable since data lost due to intrusions is not recovered. For that, we would like to improve the reliability and consistency of the network, so as to be able to heal itself of faults and to better survive malicious attacks.

In this paper, a new paradigm for a self-healing MANET is presented. It is based on the ability of the adopted intrusion detection system (MASID-R) to assess the damage caused by the detected intrusions. Then, building on this assessment, MASID-R, via its healing agent, initiates and executes the necessary actions to heal the network.

The main objective of this approach is to enable the network to heal itself of faults and damages caused by intrusions and to better survive malicious attacks (mainly packet dropping attacks) and malfunctioning, which would considerably improve the reliability and consistency of the network.

The resulting system is fully autonomous: it accurately detects intrusions launched against it, appropriately responds to them, and perfectly heals the caused damages.

The rest of the paper is organized as follows. Section 2 provides a brief overview of the related work. Then, section 3 details the proposed approach while section 4 describes the conducted experiments and discusses the obtained results. Finally, section 5 concludes the paper and initiates for possible future work.

2. RELATED WORK
The vulnerabilities of the mobile ad-hoc networks and the proliferation of intrusions and thereby the need for survivability have been widely studied in the literature. For instance, there has been considerable research in the fields of network monitoring, intrusion detection, self-healing and fault-tolerant networks. We review here some interesting works in these areas.

In [5], the authors presented a bio-inspired approach to design an intrusion prevention system (IPS) for securing MANET against intrusions. More specifically, this approach implements an analytical computational framework based on the danger theory. Using agents (Sense, Analysis, and Adaptive agents) of multi-layers (??), the proposed IPS analyzes the behavior of system processes and network traffic to detect harmful events. The prevention process is preceded by a training phase, during which normal and dangerous signatures are specified. A danger signal is then activated upon any match with the dangerous signatures. The potential intrusion will therefore be prevented by disconnecting or blocking the suspected connection and the adopted self-healing mechanism (self-healing agent) will be triggered so as to regenerate the damaged components. For that, the self-healing agent is provided with a knowledge base containing all candidate system components, in addition to the healing function. For instance, whenever a healing message is received from the Analysis Agent, a healing component is immediately identified, deployed and tested to keep the system in function. The designed IPS is autonomous and the network's fault repair ability was

considerably enhanced through the adopted self-healing mechanism.

Chonho et al. [6] proposed a decentralized self-healing mechanism that detects and recovers from wormhole attacks in wireless multi-hop sensor networks using connectivity information. This mechanism, denoted SWAT, identifies the locations of malicious nodes, isolates them, and finally recovers the routing structure distorted by them. For that, each sensor node maintains a neighbor list containing the connectivity information about one hop and two hops neighbor nodes. Using this list, a node monitors the connectivity with its neighbors. Anomaly detection within these connections results in the production of a danger signal in the form of a control packet that will trigger the recovery phase in which recovery packets are used to isolate the wormhole nodes and to heal the caused damages within the wormhole sphere based on a pre-established routing tree structure.

In [7], the authors proposed a new intrusion protection mechanism based on the notion of self-healing communities. These communities consist in groups of neighboring nodes among which a network service is distributed so as to mitigate the adverse actions of selfish and malicious nodes. For each end-to-end connection, a chain of self-healing communities along the shortest path are established based on localized simple schemes. The idea, here, is that a self-healing community is perceived as a big virtual node that replaces the conventional single forwarding node. Thus, data delivery is considered as a combination of conventional node-based data forwarding and community-based healing. At each intermediate community in a route, the most recent control packet forwarder is supposed to be the current data forwarder. If this node fails to forward a packet due to maliciousness, selfishness or network dynamics, members in the same self-healing community will make up. This way, routes can be healed locally with minimal latency. Yet, because such self-healing communities might lose shape due to mobility and network dynamics, their reconfiguration is deemed crucial for the survivability of the proposed solution. For that, the authors used end-to-end probing with a probing interval adapted with respect to network dynamics.

In [8], an artificial immune intrusion detection system inspired by idiotypic networks was proposed. More specifically, the pattern recognition technology is adopted to execute the process of intrusion detection. The proposed detection approach is divided into two main phases: (a) a training phase during which, an idiotypic network is built and trained to learn normal patterns and attacks' profiles; and (b) a detection phase to distinguish between normal and abnormal patterns and update the idiotypic network if necessary. The proposed IDS is aimed at detecting and analyzing malicious activities, measuring the effects of these activities, and as a final step it triggers the self-healing process. This latter process is responsible for the diagnosis, fault identification, and the configuration of anomalous activities. Furthermore, the self-healing system is responsible for candidate fix generation (??), damage repair, self-testing and deployment.

3. THE PROPOSED IDS-BASED SELF-HEALING APPROACH

Self-healing [9] can be defined as the property that enables a system to perceive that it is not operating correctly and, without (or with) human intervention, make the necessary adjustments to restore itself to normality.

From that perspective, we divided the proposed self-healing process into two main phases described below.

3.1 Fault Detection and Damage Spread Stopping

Upon detection of an abnormal behavior by the detection agent, the response agent will execute the necessary actions to stop the intrusion(s). To finish this phase, it will trigger the self-healing process.

3.2 Self-healing or Fault-repair

In this phase, the healing agent will use the information collected by the detection agent about the detected intrusion(s) to measure the damage caused by the intruder(s). Then, building on the assessed level of damage, it will create and execute an appropriate list of actions to heal the network.

In fact, the healing agent will store information (a kind of backup information??) about network traffic regularly (during the detection phase). Once an abnormal behavior is detected by the detection agent, or a notification of a detected intrusion is received by the collaboration agent via the network, this will trigger the healing agent to start the healing or recovery process using both its backup data and data collected during the detection phase as illustrated in the example of Table 1.

Table 1. Example of IDS and healing data (case of a blackhole or grayhole attack).

Detection data	Healing data
- Node *I* is the intruder. - *x* packets were dropped by node *I* during *T* (*T* is the active detection interval of time). - Detection time.	- Active routes having node *I* as a member. - Source and destination nodes' IDs for each path (it knows the dropped packets were generated by node *S* and are destined to node *D*). - Copy of the packets sent during *T*.

The healing agent performs the following tasks:

i. The node, on which the healing agent resides, should keep a copy of every sent packet during every active detection interval of time (detection session T).
ii. Receive messages about anomalous events from the detection agent: if no message is received from detector during T, then the healing agent will purge the recovery base (i.e., it will delete the stored packets' copies from the recovery base at the end of the current detection session). Else, it will start the diagnosis and fault identification by using information contained in the received message (e.g., ID of the intruder, intrusion detection time, drop ratio, and so on).
iii. Repair the damage caused by the detected intrusive activities. This is a twofold task: the healing agent will first establish a new route, not including the intruder and the suspected nodes (if they exist), to replace the damaged route. Then, it will resend the stored packets to their destination via the newly established route.

4. Evaluation by Simulation

In order to evaluate the proposed approach, we carried out a series of simulation experiments using the network simulator *ns-2* [10]. The following subsections detail the simulation environment, metrics and a discussion of the obtained results.

4.1 Simulation Environment and Parameters

In order to evaluate our approach, we simulated a MANET using *ns-2*. It is an object oriented discrete event simulator, written in C++, with an OTcl (Object-oriented Tcl) interpreter as a frontend. It can simulate both wired and wireless network systems. Table 2 summarizes the different parameters related to our experiments.

Table 2.Simulation Parameters

Parameter	Value
Simulator	*ns-2* (version 2.34)
Simulation time	120 s
Number of nodes	50
R.P. for legitimate nodes	AODV
R.P. for blackhole nodes	blackholeAODV
R.P. for grayhole nodes	grayholeAODV
Traffic model	Constant Bit Rate (CBR)
Transport protocol	User Datagram Protocol (UDP)
Terrain area	1000 m × 1000 m
Maximum bandwidth	2 Mbps

4.2 Evaluation Metrics

To validate the efficiency of our approach, we consider the following metrics shown below.

4.2.1 Packet Delivery Ratio (PDR)

Packet delivery ratio designates the ratio between the number of packets originated by the application layer CBR (Constant Bit Rate) sources and the number of packets received by the final destination.

Packet delivery ratio is important as it describes the loss rate that will be seen by the transport protocols. This metric characterizes both the completeness and correctness of our protocol.

$$PDR = \frac{\sum received\ packets}{\sum sent\ packets}$$

4.2.2 Protocol Control Overhead (PCO)

PCO represents the ratio between the number of protocol control packets transmitted and the number of data packets received (or transmitted??).

A lower value of the PCO means a better performance of the studied protocol.

$$PCO = \frac{\sum \text{control packets}}{\sum \text{data packets}}$$

4.3 Results

In this subsection, we present and discuss the results of our study. As mentioned earlier, we used *ns-2* and simulated an ad-hoc network consisting of 50 mobile nodes. Each node in the network is assigned an initial position within a simulation area of (1000 × 1000) square meters and joins the network at random. The MAC layer used for the simulations is IEEE 802.11. The packets are generated using CBR with a rate of 4 packets per second. The simulation takes place for 120 seconds.

Figure 1 presents the evolution over time of the packet delivery ratio. In the presence of intrusions, PDR has notoriously increased through the use of MASID-R but a more considerable increase was achieved after the integration of the healing agent. This is due to the healing agent's ability to restore the damaged data in an adequate timely manner.

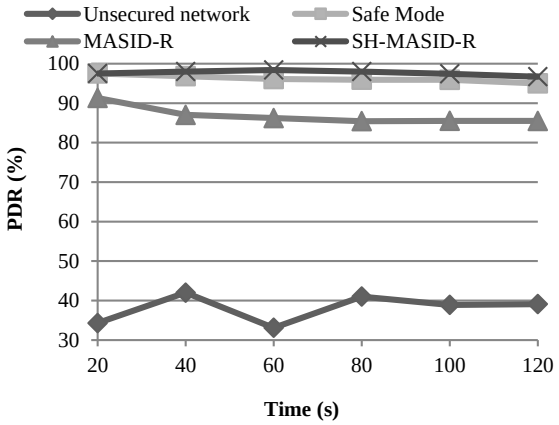

Figure 1. Packet delivery ratio vs. time

To achieve these rates, it was necessary to achieve a tradeoff between guaranteeing the delivery of packets and both the overall communication time and the generated control overhead. More specifically, the healing approach tends to increase the ratio of correctly delivered packets at the cost of an increased latency in the interrupted communication's delay resulting from the retransmission of the damaged packets.

In addition to the potential increase in the communications' delays, some traffic overhead may result due to the new route search as shown in Figure 2.

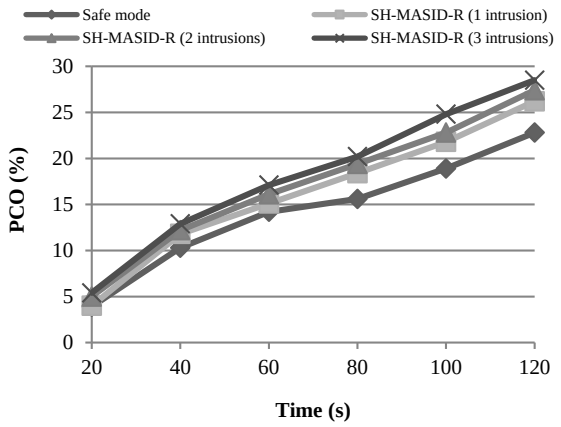

Figure 2. Protocol control overhead vs. time

Fortunately, this overhead is proportional to the number of intrusions and their distribution over time, i.e., it increases with the increase in the number of intrusions and decreases if the risk disappears.

5. Conclusion

In this paper, we presented a recovery oriented approach for a self-healing MANET. It is based on the ability of MASID-R to assess the damage caused by the detected intrusions and aimed at enabling the supervised network to heal itself of any damage or faults through the integration of the healing agent.

The network is now sufficiently survivable as it can provide its services correctly even in the presence of intrusions and faults. For instance, a very high packet delivery ratio was achieved in return of a small additional traffic overhead and proportional short delivery delays. Also, since recovery data is stored for limited short intervals of time, it will not overload the nodes on which it is stored. Moreover, the design of the recovery base in that flexible way greatly facilitates data manipulation (i.e., storage, extraction, and deletion), thereby minimizing both processing load and time.

As a future work, we plan to improve the healing ability of our intrusion detection system so as to heal the network of all kinds of damage and faults that can be caused by potential intrusions.

6. REFERENCES

1. Chen, J. and Wu, J. 2010.A survey on Cryptography Applied to Secure Mobile ad hoc networks and wireless sensor networks.Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, 262—289.
2. Abusalah, L., Khokhar, A. and Guizani, M. 2013. A survey of secure mobile ad hoc routing protocols. IEEE communications surveys & tutorials, vol. 10, no. 4, 78—93.
3. Patil,J. A. andSidnal, N. 2013.Survey - secure routing protocols of MANET. InternationalJournal of Applied Information Systems, vol. 5, no. 4, 8—15.
4. Mechtri, L., Djemili, F.T. and Ghanemi, S. 2014.Towards high reliability of a multi-agent system designed for intrusion detection in MANET. ICEECA'2014, Springer, In press.
5. Elsadig,M. and Abdullah, A. 2009. Biological inspired intrusion prevention and self-healing system for network security based on danger theory. International Journal of Video & Image Processing and Network Security, vol. 9, no. 9, 16—28.
6. Lee,C-H. and Suzuki, J. 2008. SWAT: a decentralized self-healing mechanism for wormhole attacks in wireless sensor networks. In: Xiao, Y., Chen, H., Li, F. Eds., Handbook on Sensor Networks, 2008 World Scientific Publishing, New Jersey, USA., 01—21.
7. Kong, J., Hong, X., Yi, Y., Park, J-S., Liu, J. andGerla, M. 2005. A secure adhoc routing approach using localized self healing communities. In proceedings of the Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05), USA, 254—265.
8. Jain, P., Singh, P. K. and Abraham, A. 2011. Intrusion detection and self healing model for network security. In proceedings of the 7th International Conference on Next Generation Web Services Practices, 320—325.
9. Ghosh, D., Sharman, R., Rao, H.R. and Upadhyaya S. 2007.Self-healing systems - survey and synthesis. Decision Support Systems 42, 2164—2185.
10. K. Fall, and K. Varadhan. 2010. The VINT Project: The ns manual. http://www.isi.edu/nsnam/ns/ns-documentation.