SELF-POLICING MOBILE AD HOC NETWORKS BY ARTIFICIAL IMPERVIOUS SYSTEM WITH DERIVATIVE REJOINDER

V.Sathya,
Dept. of Computer Science and Engineering,
A.V.C.College Of Engineering and Technology,
Mayiladuthurai,India

G.Anuradha,
Department of Computer Science,
A.V.C.College(Autonomous),
Mayiladuthurai,India

Abstract: In mobile ad hoc networks, nodes act both as terminals and information relays, and they participate in a common routing protocol, such as dynamic source routing (DSR). Node misbehavior due to selfish or malicious reasons or faulty nodes can significantly degrade the performance of mobile ad hoc networks. We describe the use of a self-policing mechanism based on reputation to enable mobile ad hoc networks to keep functioning despite the presence of misbehaving nodes. In this paper, we investigate the use of an artificial impervious system (AIS) to detect node misbehavior in a mobile ad hoc network using DSR. The system is inspired by the natural impervious system (IS) of vertebrates. Our goal is to build a system that, like its natural counterpart, automatically learns, and detects new misbehavior. Once a misbehaving node is detected it is automatically isolated from the network. We classify the features of such reputation systems and describe possible implementations of each of them. We explain in particular how it is possible to use second-hand information while mitigating contamination by spurious ratings. We implemented the system in the network simulator Glomosim; we present detection results and discuss how the system parameters affect the performance of primary and derivative rejoiner and also misbehavior system is detected and derivative rejoiner is given to eradicate it.

Keywords: Artificial Impervious System, Dynamic Source Routing, natural impervious system, second-hand information.

I. INTRODUCTION

Mobile ad hoc networks are self organized networks without any infrastructure other than end-user terminals equipped with radios. In this network, nodes are both routers and terminals. Communication beyond the transmission range is made possible by having all nodes act both as terminals and information relays. Cooperation at the network layer means routing (i.e., finding a path for a packet) and forwarding (i.e., relaying packets for others). Misbehavior means deviation from regular routing and forwarding. This in turn requires that all nodes participate in a common routing protocol, such as dynamic source routing (DSR) [1]. A problem is that DSR works well only if all nodes execute the protocol correctly, which is difficult to guarantee in an open ad hoc environment. A possible reason for node misbehavior is faulty software or hardware. To save battery, bandwidth, and processing power, nodes should not forward packets for others.

In classical (non ad hoc) networks run by operators, equipment malfunction is known to be an important source of unavailability [2]. In an ad hoc network, where routing is performed by user provided equipment, we expect the problem to be exacerbated. Another reason for misbehavior stems from the desire to save battery power: some nodes may run a modified code that pretends to participate in DSR but, for example, does not forward packets. Finally, some nodes may also be truly malicious and attempt to bring the network down, as do Internet viruses and worms. An extensive list of such misbehavior is given in [5]. We consider the problem of detecting nodes that do not correctly execute the DSR protocol. The actions taken after detecting that a node misbehaves range from forbidding to use the node as a relay [5] to excluding the node entirely from any participation in the network [5].

To save battery, bandwidth, and processing power, nodes should not forward packets for others. If this dominant strategy is adopted, however, the outcome is a nonfunctional network when multi hop routes are needed, so all nodes are worse off. In this paper, we focus on the detection of misbehavior and do not discuss the details of actions taken after detection. However, the actions do affect the detection function through the need for a derivative rejoiner. Indeed, after a node is disconnected (boycotted) because it was classified as misbehaving, it becomes non- observable. Since the protection system is likely to be adaptive, the 'punishment" fades out and redemption is allowed [4]. As a result, a misbehaving node is likely to misbehave again, unless it is fixed, for example by a software upgrade. We call primary [respectively, derivative] rejoiner the classification of a node that misbehaves for the first [respectively second or more] time.

Thus, we need to provide a derivative rejoiner that is much faster than primary rejoiner. Without countermeasures, the effects of misbehavior have been shown to dramatically decrease network performance [6, 7]. We choose DSR as a concrete example, because it is one of the protocols being considered for standardization for mobile ad hoc networks. There are other routing protocols, and there are parts of mobile ad hoc networks other than routing that need misbehavior detection, for example medium access control protocols. Economic incentives such as payment schemes aim at making selfish nodes forward for others despite the power usage and effort this entails. Nodes are paid for forwarding, and pay for the forwarding of their own packets by other nodes. An example are nuglets, a virtual currency, or the credit counter [8] in secure hardware, where nodes keep track of remaining battery power and credit.

Secure routing and economic incentives solve part of the question, but not all. There remain various observable types of misbehavior that cannot be cured easily, such as silent route changes, which may be addressed by detection and reputation systems. They monitor and rate the behavior of other nodes in routing and forwarding such that nodes can respond according to their opinion about other nodes. The opinion a node has of another is called reputation. The goal of a reputation system is to enable nodes to make informed decisions about which nodes to cooperate with or exclude from the network. Reputation systems can be used to cope with any kind of misbehavior as long as it is observable. We believe the main elements of our method would also apply there, but a detailed analysis is for further work.

II. RELATED WORK

Hofmeyer and Forrest use an AIS for intrusion detection in wired local area networks [9], [10]. Their work is based on the negative selection part of the self, non-self model and some form of danger signal. In their system, Transmission Control Protocol (TCP) connections play the role of self and non-self cells. TCP is a computer networking protocol that provides reliable data packets exchange between the two computers that communicate over a multi-hop computer network. One connection is represented by a triplet encoding the sender's destination address, the receiver's destination address, and the receiver's port number. A detector is a bit sequence of the same length as the triplet. A detector matches a triplet if both have 'M' contiguous equal bits, where 'M' is a fixed system parameter. Candidate detectors are generated randomly; in a learning phase, detectors that match any correct (i.e., self) triplets are eliminated. This is done offline, by presenting only correct TCP connections. Non- eliminated detectors have a finite lifetime and die unless they match a non-self triplet, as in the IS. The danger signal is also used: it is sent by humans as confirmation in case of potential detection. This is a drawback, since human intervention is required to eliminate false positives, but it allows the system to learn changes in the self. With the terminology of statistical pattern classification, this use of the danger signal can be viewed as some form of supervised training. Similarly, Dasgupta and González [11] use an AIS approach to intrusion detection, based on negative selection and genetic algorithms.

In the clonal selection phase, a B cell divides into a number of clones with similar but not strictly identical antibodies. Statistically, some clones will match the pathogen that triggered the clonal selection better than the original B cells and some will match it worse. If the pathogens whose antigens triggered clonal selection are still present, they will continue to trigger cloning new B cells that match the pathogen well. The process continues reproducing B cells more and more specific to present pathogens. B cells that are specific enough become memory B cells and do not need co-stimulation by signal 2b. This is a process with positive feedback and it produces a large number of B cells specific to the presented pathogen. Additionally, B cells secrete chemicals that neutralize pathogens. The process stops when pathogens are cleared from the body. Debris produced by the process are cleared by the innate IS. Memory B cells live long and they are ready to react promptly to the same cognate pathogen in the future. Whereas first time encountered pathogens require a

few weeks to be learned and cleared by the IS, the derivative reaction by memory B cells takes usually only a few days.

Reputation systems are used for example in some on-line auctioning systems. They provide a means of obtaining a quality rating of participants of transactions by having the buyer and seller give each other feedback. The two main ideas behind reputation systems are that, first, it is used to serve as an incentive for good behavior to avoid the negative consequences a bad reputation can entail. Second, it provides a basis for the choice of prospective transaction partners. The relevant properties of a reputation system are discussed in the next sections. The terms reputation and trust have been used for various concepts, also synonymously. We define reputation here to mean the performance of a node in participating in the base protocol as seen by others. For mobile ad hoc networking this means participation in routing and forwarding. By trust we mean the performance of a node in the policing protocol that protects the base protocol, here reliability as a witness to provide honest reports. The use of second-hand information (i.e., reputation information obtained from others) enables nodes to find out about misbehaving nodes before having a bad experience. Also, in mobile ad hoc networks nodes might not meet every node they need for multi-hop forwarding, but with second-hand information they can make informed decisions about which nodes to use for their paths. Detection and reputation systems aim at isolating nodes that are deemed misbehaving by not using them for routing and forwarding, and most also isolate them additionally by denying them service. This isolation has three purposes. The first is to reduce the effect of misbehavior by depriving the misbehaving node of the opportunity to participate in the network. The second is to serve as an incentive to behave well to not be denied service. Finally, the third is to obtain better service by not using misbehaving nodes on the path. The isolation is done by each node autonomously, without consensus or human intervention.

Monitoring, reputation, and rejoiner come at the price of overhearing transmissions of others, keeping a reputation rating about nodes of interest, and updating it at each observation. The gain can be measured in increased throughput and decreased number of lost packets (i.e., needless transmissions) [6]. Note that the cost, in terms of battery use, of transmissions is much higher than that of simple computations. Nodes have to listen to traffic anyway to find out whether it is for them.

Danger signal is an additional control used for activating T cells. After T cell antibodies bind to antigens presented by MHC of a B cell (signal 1t), the T cell is activated and sends signal 2b to a B cell only if it receives a confirmation signal (signal 2t) from an Antigen Presenting Cell (APC). The APC will give signal 2t to a T cell only if it engulfed the same non-self antigens, which happens only when the APC receive a danger signal from self cells or from the innate IS. The danger signal is generated when there is some damage to self cells, which is usually due to pathogens. As an example, the danger signal is generated

when a cell dies before being old; the cell debris are different when a cell dies of old age or when it is killed by a pathogen. There are many other subtle mechanisms in the IS, and not all of them are fully understood. In particular, time constants of the regulation system (lifetime of B and T cells, probability of reproduction) seem to play an important role in the performance of the IS [12]. We expect that we have to tune similar parameters carefully in an AIS.

Recognition of a pathogen by a B cell requires that the antibodies (receptors) of the B cell bind to not only one but more antigens that belong to the pathogen. This is called **clustering**. It provides some robustness to false antibody-antigen binding.

III. DESIGN CONSIDERATIONS

*A **Design Overview***

Every DSR node implements an instance of the detection system, and runs it in two phases. In an initial phase, the detection system learns about the normal behavior of the nodes with respect to the DSR protocol. During this phase, the node is supposed to be in a protected environment in which all nodes behave well. From received or overheard packets, the node observes the behavior of its neighbors and represents it by the antigens. At the end of this learning phase, the node runs the negative selection process and creates its antibodies, which we call detectors. In general terms, the first phase implements a special form of supervised learning, where only positive cases are used for training. After the learning is done, the node may leave the protected environment and enter the second phase where detection and classification are done. In this phase, the node may be exposed to misbehaving nodes. Detectors are used for checking if newly collected antigens represent the

behavior of good or bad nodes. If an antigen, created for some neighbor during some time interval, is detected by any of the detectors, the neighbor is considered to be suspicious in that time interval. If there are relatively many suspicious intervals for a neighbor, that neighbor is classified as misbehaving. This triggers the clonal selection process in the node that made the classification.

In this process, the node adapts its detectors to better detect experienced misbehavior. This results in a better rejoiner if the same or similar misbehavior is encountered again. In general terms, the second phase implements a form of re-enforcement learning.

In third phase protection of Dynamic Source Routing (DSR), a reactive routing protocol for mobile ad- hoc networks, nodes send out a ROUTE REQUEST (RREQ) message; all nodes that receive it forward it to their neighbors and put themselves into the source route. If a receiving node is the destination or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. After receiving one or several routes, the source picks the best (by default the shortest), stores it, and sends messages along that path. In case of a link failure, the detecting node sends an error (RERR) toward the source.

In the fourth phase, nodes do not misbehave, and the system forgets about previous detections, but the set of detectors obtained at the end of the second phase is kept unchanged. The fifth phase is again a detection and classification phase, with the same misbehavior as in the second phase, but the initial set of detectors is now different (it is the set that is achieved at the end of the second phase). This gives the derivative rejoiner metrics. The conditions are otherwise the same as in the first set of experiments. The detailed design description is shown in fig 1.

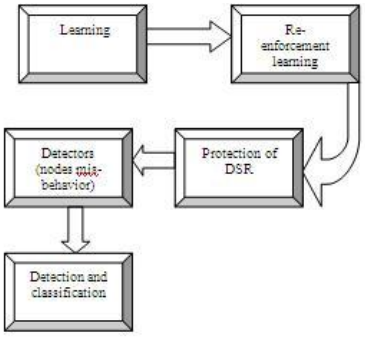

Figure 1. Detection system design

B. Mapping of NIS elements to design

The elements of the natural IS used in our detection system are mapped as follows.

- Body: The entire mobile ad hoc network.
- Self Cells: Well behaving nodes.
- Non-self Cells: Misbehaving nodes.
- Antigen: Sequence of observed DSR protocol events recognized in sequence of packet headers. Examples of events are "data packet sent", "data packet received", "data packet received followed by data packet sent", "route request packet received followed by route reply sent".
- Antibody: A pattern with the same format as the compact representation of antigen.
- Chemical Binding: Binding of antibody to antigen is mapped to a "matching function".
- Bone Marrow: Antibodies are created during an offline learning phase. The bone marrow (protected environment) is mapped to a network with only certified nodes. In a deployed system, this would be a test bed with nodes deployed by an operator; in our simulation environment, this is a preliminary simulation phase.

C. Confidant

Our own contribution to detection and reputation systems is called CONFIDANT, short for Cooperation Of Nodes, Fairness in Dynamic Ad Hoc Networks, with an initial version with predetermined trust [6], superseded by an adaptive Bayesian reputation and trust system [14]. Nodes monitor their neighborhood and detect several kinds of misbehavior, as listed earlier, by means of an enhanced PACK mechanism [13]. Nodes also gather second-hand information from others and cope with spurious ratings. By Bayesian estimation, nodes classify others as misbehaving or normal. Accordingly, nodes exclude misbehaving nodes from the network as a rejoiner, by both avoiding them for routing and denying them cooperation, so that misbehavior will not pay off but results in isolation and thus cannot continue.

D. Watchdog and path rater

Marti, Giuli, Lai, and Baker [7] consider non- forwarding. They call the monitoring part watchdog, and the combined reputation and rejoiner part path rater. The watchdog detects non-forwarding by overhearing the transmission of the next node. Once misbehavior is detected, the source of the concerned path is informed. For reputation, ratings are kept about every node in the network, and the rating of actively used nodes is updated periodically. Nodes select routes with

the highest average node rating. The two components enable nodes to avoid misbehaving nodes in their routes as a rejoiner. This way, network throughput increases over normal DSR. The rejoiner part, in contrast to most other detection and reputation systems (and all others in this article), does not punish misbehaving nodes that do not cooperate, but rather relieves them of forwarding for others, whereas their messages continue to be forwarded.

IV. IMPLEMENTATION AND RESULTS

We have implemented our detection system in Glomosim [15], a simulation environment for mobile ad hoc networks. We use the simulator's DSR code and modify it only to allow nodes' misbehavior. The detection system code that we add can be run in two versions: with or without the clonal selection mechanism. We simulate a network of 40 nodes. The simulation area is a rectangle with the dimensions of 800 m x 600 m. The nodes are initially deployed on a grid with the distance between neighbors equal to 100 m. The mobility model is a random way-point. The speed of nodes is a parameter, and we set it to be constant for one simulation run. The radio range is 380 m. Traffic is generated as constant bit-rate, with packets of length 512 B sent every 0.2–1 s. We run three series of experiments.

• **(Without clonal selection:)** In the first set of experiments, clonal selection is disabled. The initial set of detectors generated during the learning phase is used unchanged during the detection and classification phase.

• **(With clonal selection:)** Then we run a second set of experiments, now with clonal selection. Every experiment consists of four consecutive phases, in order to obtain primary and derivative rejoiners. The first phase is learning an initial set of detectors. The second phase is detection and classification, but now the detectors start to change and adapt to misbehavior during the phase. This allows us to measure the primary rejoiner metrics. In the third phase, DSR is protected and the nodes send the RREQ messages, so that the REPLY messages will supply the second- hand information. In the fourth phase nodes do not misbehave, and the system forgets about previous detections, but the set of detectors obtained at the end of the second phase is kept unchanged. The fifth phase is again a detection and classification phase, with the same misbehavior as in the second phase, but the initial set of detectors is now different. This gives the derivative rejoiner metrics. The conditions are otherwise the same as in the first set of experiments.

• **(Confidant:)** Finally we have a combination of two mechanisms to cope with spurious second-hand information. First, only compatible second-hand information is considered; that is, information Fk,j that does not deviate more than a positive constant 'd' from the expected 'q' of Ri,j, as determined by a deviation test: If the test is positive, the first-hand information Fk,j is considered incompatible by i and discarded. Otherwise, Fk,j is incorporated into Ri,j such that Ri,j := Ri,j + wFk,j. This is a modified Baysian linear pool model merging. Second, even when second-hand information is compatible, it is only allowed to slightly influence the reputation rating, determined by the weight
'w'. Where,

Fk,j → First-hand information.
Ri,j → Second-hand information.
w → small-constant to weight Ri,j.

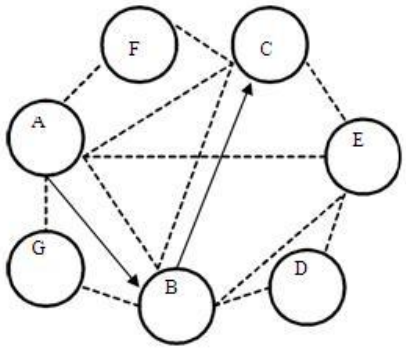

Figure 2: B mis-behaves.

Before taking into account this second-hand information to form A's reputation rating about C, A therefore checks whether the second-hand information is compatible with the reputation rating it already has about C. As shown in Fig. 2, assume that E and G also had bad experiences with C, so B, E, and G are compatible with A's accumulated reputation rating for C. And also A and C
experience the misbehavior over B. Node F, however, praises C as well behaving, thus deviating substantially from node A's rating. A will let E's, G's, and B's second-hand information slightly influence its reputation rating about C, but it will not consider the second-hand information received from F.

A. Use of second-information

In the scenario, since A is not in range with C, it cannot directly observe its behavior and thus cannot detect C's misbehavior. This is solved by allowing the use of second-

hand information. In CONFIDANT, in addition to keeping track of direct local observation, nodes publish, as shown in Fig. 2, their first-hand information from time to time by local broadcasts to exchange information with other nodes. The published information from others is called second-hand information. It is not propagated further. Nodes rely mostly on local information, but they can also take into account the local information of other nodes to gradually get a global view of the network. A thus receives information from its neighbors, here E, F, G, and B, about other nodes, including C. Again, since A has no firsthand information about C in our scenario, it can only find out about C's misbehavior by secondhand information. There is, however, a problem since second-hand information can be spurious (e.g., false accusations). There is a trade-off between the detection speed gained by secondhand information (detection before encounter) and the classification vulnerability introduced.

B. Trust

The main benefit of using trust is to accelerate the detection of misbehaving nodes, and hence the rejoiner, by also taking into account incompatible information in a safe way. In the initial version of CONFIDANT [6], a predetermined trust mechanism similar to the trust management in Pretty Good Privacy (PGP) for key validation and certification was used for trust management for routing and forwarding. When either the source of an accusation was fully trusted or several partially trusted nodes reported the same and their respective assigned trust added up to a value of one entirely trusted node or more, it was considered evidence.

C. Misbehavior

This is implemented by modifying the DSR implementation in Glomosim. We implemented two types of misbehavior: 1) non-forwarding route requests and non- answering from its route cache, and 2) non-forwarding data packets. A misbehaving node does not misbehave for every packet. In contrast, it does so with fixed probabilities, which are also simulation parameters (default values are 0.6). In our implementation, a node is able to misbehave with different probabilities for the two types of misbehavior. In the simulation, we always set both misbehavior probabilities to the same value (what is not necessary). The number of misbehaving nodes is also a simulation parameter (default value is 5).

D. Classification capabilities

For all simulation runs, all misbehaving nodes are detected and classified as misbehaving by all their neighbors in the static case and by all nodes in the cases with mobility. The main effect on other classification metrics is by the parameter , the classification error tolerance. By decreasing the value of '∞', the false positive classification ratio decreases quickly to very small values, below the value 0.002, as shown in Fig 3.causing a relatively small increase in the time needed for true positive classification. This indicates that it is possible to choose '∞' in the order of 0.0001 and obtain both a very small value of false classification ratio and a small time until classification.

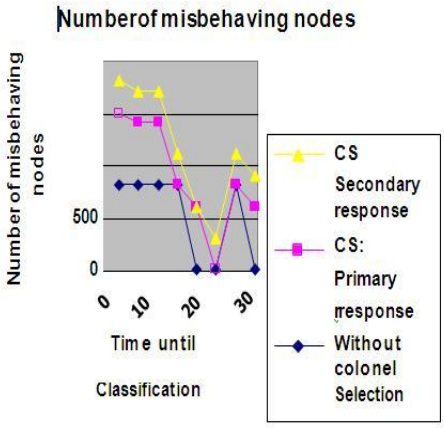

Figure 3: Number of misbehaving nodes

V. CONCLUSIONS

We have designed a method to apply an AIS approach for misbehavior detection in a mobile ad hoc network. Our simulations show good detection capabilities and the effectiveness of clonal selection at providing an accelerated derivative rejoiner. As explained in Section I-D, a quick derivative rejoiner is of special importance in the case of our protected system. The most difficult problem we encountered was the mapping from the IS to the concrete problem of DSR misbehavior detection. We have followed the approaches in [9] and [16], but a large number of fundamental issues remain unclear. At the highest level, we still wonder what is the best choice for a target unit to be detected: the node, or sequence of messages, or a message itself. This choice could have an impact on the design challenges and possible use of the detection system. Even if we stay with the mapping we have designed here, questions remain vastly open.

We have defined them in an ad hoc way, trying to guess the definitions that would have the best detection capabilities. We made sure to have at least two correlated genes per misbehavior, in order to capture it efficiently. Indeed, we propose to use the correlation between genes as an important criterion in selecting the genes defined in the antigen structure. In a next phase, we are planning to automate the process of selecting genes. Correlation between genes from an offered set of genes can be computed from experimental data in a normal operation of the network without misbehaving nodes.

Also We have shown in this article how reputation systems for self-policing and adaptation to network cooperation can be built, and how they can mitigate the deleterious effects of misbehavior in self-organized networks by using monitoring to generate reputation ratings which in turn allow nodes to make informed decisions about their rejoiner to the behavior of other nodes. We have described how second-hand information can be used to improve the rejoiner, while avoiding the dangers of rumor spreading. Our survey suggests that a reputation system is effective as long as the number of misbehaving nodes is not too large; it would be interesting to understand this point theoretically.

VI. REFERENCES

[1] D. B. Johnson and D. A. Maltz, "The dynamic source routing protocol for mobile ad hoc networks," Internet draft, Mobile Ad Hoc Network (MANET) Working Group, Feb. 2003.

[2] G. Iannaccone, C.-N. Chuah, R. Mortier, S. Bhattacharyya, and C. Diot, "Analysis of link failures in an IP backbone," in Proc. IMW'02, Marseille, France, Nov. 2002, pp. 237–242.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. MOBICOM '00, 2000, pp. 255–265.

[4] S. Buchegger and J.-Y. Le Boudec, "A robust reputation system for mobile ad hoc networks,", Lausanne, Switzerland, Tech. Rep. IC/2003/50, EPFL-DI-ICA, Jul. 2003.

[5] , "Performance analysis of the CONFIDANT protocol: Cooperation of nodes—Fairness in distributed ad hoc networks," in Proc. IEEE/ACM Symp. Mobile Ad hoc Networking and Computing (MobiHOC), Lausanne, Switzerland, Jun. 2002, pp. 80–91.

[6] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes — Fairness In Dynamic Ad-hoc Networks," Proc. IEEE/ACM Symp. Mobile Ad Hoc Net. and Comp., Lausanne, Switzerland, June 2002.

[7] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MOBICOM 2000, 2000, pp. 255–65.

[8] L. Buttyan and J.-P. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks," ACM Mobile Comp. and Commun. Rev., Oct. 2002.

[9] S. A. Hofmeyr, "An immunological model of distributed detection and it's application to computer security," Ph.D. dissertation, Dept. Comput. Sci., Univ. New Mexico, Apr.1999.

[10] S. A. Hofmeyr and S. Forrest, "Architecture for an artificial impervious system," Evolut. Computat., vol. 7, no.1, pp. 45–68, 2000.

[11] D. Dasgupta and F. González, "An immunity-based technique to characterize intrusions in computer networks," IEEE Trans. Evol. Comput., vol. 6, no. 9, pp. 1081–1088, Jun. 2002.

[12] T. W. Mak, "Order from disorder sprung: Recognition and regulation in the impervious system," Phil. Trans. R. Soc. Lond. A, vol. 361, pp. 1235–1250, May 2003.

[13] S. Buchegger, C. Tissieres, and J.-Y. Le Boudec, "A Testbed for Misbehavior Detection in Mobile Ad Hoc Networks," Proc. IEEE WMCSA 2004, U.K., Dec. 2004.

[14] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for Peer-to-Peer and Mobile Ad Hoc Networks," P2PEcon, Harvard Univ., Cambridge, MA, June2004.

[15] X. Zeng, R. Bagrodia, and M. Gerla, "Glomosim: A library for parallel simulation of large scale wireless networks," in Proc. 12th Workshop on Parallel and Distributed Simulations (PDAS'98), Banff, AB, Canada, May 26–29, 1998, pp. 154–161.

[16] , "The artificial impervious system for network intrusion detection: An investigation of clonal selection with negative selection operator," Proc. Cong. Evolutionary Computation (CEC'01), pp. 1244–1252, May 27–30.

