AN ARCHITECTURE FOR INTRUSION DETECTION AND ACTIVE RESPONSE USING AUTONOMOUS AGENTS IN MOBILE AD HOC NETWORKS

Ping yi, Shiyong Zhang, Yiping Zhong
Department of Computing and Information Technology, Fudan University, Shanghai, 200433, China

Keywords: Immune system, Intrusion detection, Mobile agent, Mobile ad hoc network, Network security

Abstract: This paper focuses on investigating immunological principles in designing the multi-agent security architecture for intrusion detection and response in mobile ad hoc networks. In this approach, the immunity-based agents monitor the situation in the network. These agents can take appropriate actions according to the underlying security policies. Specifically, their activities are coordinated in a hierarchical fashion while sensing, communicating, decision and generating responses. Such an agent can learn and adapt to its environment dynamically and can detect both known and unknown intrusions. The proposed intrusion detection architecture is designed to be flexible, extendible, and adaptable that can perform real-time monitoring. This paper provides the conceptual view and a general framework of the proposed system. In the end, the architecture is illustrated by an example to show it can prevent the attack efficiently.

1 INTRODUCTION

A mobile ad hoc network consists of a group of mobile nodes that communicate with each other via wireless Radio Frequency(RF) links without help of a fixed infrastructure. The mobile ad hoc network have several salient characteristics: dynamic topologies, bandwidth-constrained, variable capacity links, energy-constrained operation, limited physical security(S. Corson, 1999). Wireless ad hoc networks have applications in military tactical operations, emergency scenarios, law enforcement and rescue missions, due to easier deploying. Many of these applications are security-sensitive. But traditional security systems can not do well in mobile ad hoc networks for above properties.

The immune system is to protect the body from threats posed by toxic substances and pathogens, and to do so in a way that minimizes harm to the body and ensures its continued functioning. The immune system is highly complicated and appears to be precisely tuned to the problem of detecting and eliminating infections. The immune system has some features. Firstly, it is distributed, consisting of many components that interact locally to provide global protection, so there is no central control and hence no single point of failure. Secondly it is dynamic, i.e. individual components are continually created, destroyed, and circulated throughout the body, which increases the temporal and spatial diversity of the immune system allowing it to discard components that are useless or dangerous and improve on existing components. Thirdly it is adaptable, i.e. it can learn to recognize and respond to new microbes, and retain a memory of those microbes to facilitate future responses and so on. We believe that it also provides a compelling example of a distributed information-processing system, one which we can study for the purpose of designing a robust distributed adaptive security system for mobile ad hoc networks.

In the paper, the authors propose the security architecture, based on the framework of the immune system, which is capable of detecting and identifying an attack, elaborating a specialized response measure to isolate the invader, and recovering form the attack. In addition, the proposed model has the same learning and adaptive capability of the human immune system, and so it is able to react to unknown attacks and to improve the response under subsequent exposures to the same attack.

The rest of the paper is organized as follows. Section 2 gives the related work. The proposed architecture is described in section 3. In section 4, we describe how our architecture detects intrusion and responds by an example. We address some

yi P., Zhang S. and Zhong Y. (2005).
AN ARCHITECTURE FOR INTRUSION DETECTION AND ACTIVE RESPONSE USING AUTONOMOUS AGENTS IN MOBILE AD HOC NETWORKS.
In *Proceedings of the Seventh International Conference on Enterprise Information Systems - DISI*, pages 220-226

features of the security architecture in section 5. Finally, we conclude the paper and elaborate on how we exploit it in the future.

2 RELATED WORK

The papers of mobile ad hoc networks security can be classified in three categories: Key management, secure network routing, and intrusion detection.

Capkun, Buttyan and Hubaux propose a fully self-organized public key management system that can be used to support security of ad hoc network routing protocols(Srdjan Capkun, 2003). Zhou and Hass first proposed to use threshold cryptography to securely distribute the Certificate Authority (CA) private key over multiple nodes to form a collective CA service(Lidong Zhou,1999). Routing security has been most noted by its absence early in the discussion and research on ad hoc routing protocols. Since then several ad hoc routing protocols that include some security services have been proposed: SRP(P.Papadimitratos,2002), Ariadne(Yih-Chun Hu, 2002), ARAN(Kimaya Sanzgiri, 2002), SEAD(Yih-Chun Hu, 2002). SRP assumes the existence of shared secrets between all pairs of communicating nodes and leverages this for MAC authentication, such that fake route requests are not accepted at the destination and routes set in route replies cannot be modified. In Ariadne, end-to-end authentications are got by one-way hash chain and MAC(Message Authentication Code) authentication. ARAN relies on public key certificates to retain hop-by-hop authentications. SEAD uses elements from a one-way hash chain to provide authentication for both the sequence number and the metric in each entry. Yongguang Zhang developed an intrusion detection architecture and evaluated a key mechanism in this architecture, anomaly detection for mobile ad-hoc networks(Yongguang Zhang, 2003). These above security systems have not any idea of immune system.

S. Forrest, S. Hofmeyr, and A. Somayaji(S. Forrest, 1997) and Hofmeyr and Forrest(S.Hofmeyr , 1999)(S. Hofmeyr, 2000) have been pursuing the problem of developing an artificial immune system that is distributed, robust, dynamic, diverse and adaptive, with applications to computer network security. In their system, the several immune system cells and molecules were simplified by the definition of a basic type of detector that combined useful properties from these elements. The detector cell had several different possible states, roughly corresponding to lymphocytes, naive B-lymphocytes and memory B-lymphocytes. The detectors were represented by bit strings of a given length, and a small amount of state. Detection was performed by a string match process that took into account the number of r-contiguous bits between two strings. The definition of self was performed by the negative selection algorithm described in Forrest, *et al*. The maturation of naive detectors into memory detectors, together with the negative selection, is responsible for the learning part of the system. The authors used permutation masks to achieve diversity of detectors.

Kim and Bentley(J.Kim, 1999) are working on the development of a network intrusion detection system inspired in the immune system. The authors proposed a Negative Selection Algorithm(NSA) with niching for network intrusion detection. They also suggested that an overall artificial immune model for network intrusion detection would be comprised by three distinct evolutionary stages: (1) Negative selection, (2) clonal selection; and (3) gene library evolution.

Dasgupta(Dipankar Dasgupta, 1999) proposed an agent-based system for intrusion/anomaly detection and response in networked computers. In his approach, the immunity-based agents roamed around the nodes and routers monitoring the situation of the network. The most appealing properties of this system were: Mobility, adaptability and collaboration. The immune agents were able to interact freely and dynamically with the environment and each other.

3 SYSTEM ARCHITECTURE

3.1 Overview

The immune system is a complex system composed by all kind Lymphocytes, such as B-cell, T-cell. An agent is a small intelligent active object which is able to carry out activities continuously and autonomously in a particular environment. Agent is autonomous, lightweight, adaptive, mobile. Multi-agent can communicate and cooperate with each other. These qualities make agent a choice for security architecture in bandwidth and computation-sensitive mobile ad hoc networks.

Fig.1 shows the three essential components of the architecture: Monitor agent, decision agent and killer agent. Monitor agent resides on each node and monitors the neighbor nodes by collecting all packets with its communication range. Monitor agent codes behavior information of its neighbor nodes and sends them to decision agent. Decision agents collect the information from the monitor agent, and make a judgment by security policies and its immune memory. If the decision agent can judge that some node is invader, it will produce killer agent to surround the invader and isolate it in the end. Three agents may view as T-cell, B-cell and antibody. When T-cell finds an invader, it activates B-cell to produce a lot of antibodies. These antibodies will bind the invader.

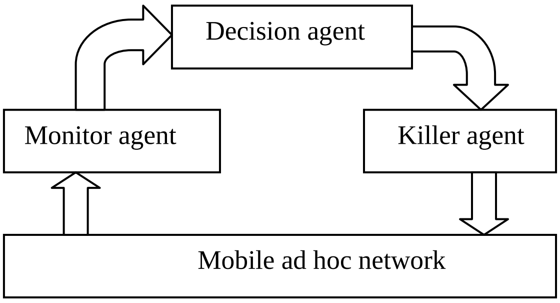

Figure 1: System agent architecture

3.2 Monitor agent

Monitor agent may be regarded as T-cell and resides on each node in mobile ad hoc networks. It monitor neighbor node and sends these information to decision agent. There are four components in monitor agent which are communication, coding, filter, collection. Fig.2 shows the components of monitor agent.

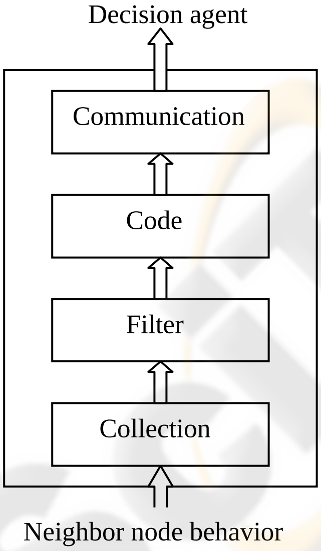

Figure 2: Components of monitor agent

The collection component is responsible for collecting information of its neighbor node behavior and hand in filter component. The information of neighbor node may be too many to send decision agent. Firstly, in order to reduce the amount of information, filter component filters unnecessary information, such as the routine packet to keep alive between neighbors. Secondly, the code component analyzes the information and codes them by number. For example, we may represent node behavior by the following number.

1—Route Request sent 2—Route Request received
3—Route Reply sent 4—Route Reply received
5—Route Error sent 6—Route Error received
7—data packet sent 8—data packet received

A monitor agent listen its neighbor A, B, C and store the dataset: A—21214343, B—87878787, C—2244688. Communication component passes theses messages to the decision agent.

3.3 Decision agent

The core of the security architecture is decision agent. It collects the information from monitor agents. Then it finds the invader through the information. Finally, decision agent may produce a lot of killer agents to isolate the invader. To save network resource, decision agents do not reside on all nodes in mobile ad hoc networks, they are only distributed over the whole network. Just as B-cell circulates in the body, they move in the network with the node moving or they move by themselves. Every agent monitors the nodes in a zone by monitor agents. Fig.3 shows its components of decision agent. There are three function components which are communication, analysis and response components and two databases which are security policy and immune memory databases.

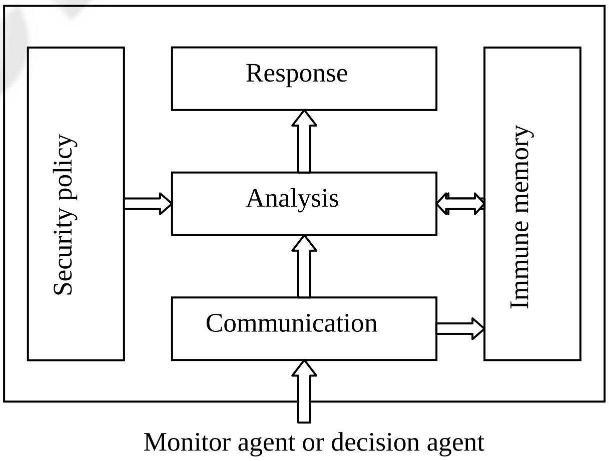

Figure 3: Components of decision agent

The communication component of decision agent collects information from the monitor agents. When two decision agents move closely, they can exchange their immune memory by communication component. The analyze component firstly compare information from monitor agents with the immune memory. The memory of previously seen invader allows the decision agent to mount much faster secondary responses. Secondly, it compares information with protocol form security policy database. It mainly depends on routing protocol. For example, when it receives a data packet, a node should forward it soon. In above subsection, the information of B's behavior is "87878787". It implies that node B can forward packets when it received packets. And node C's behavior is "2244688", which infers that node C only receives packets, but it does not forward data. If a node sometimes violates normal behavior, there may be some link errors. But if the number of abnormal behavior is over the threshold, the node can be an invader, just as a lymphocyte will only be activated when the number of receptors bound exceeds some threshold. Finally, when an invader is found, response component produces killer agents to surround the invader. The features of the node behavior will be save the immune memory and it will accelerate the process of intrusion detection when the same intrusion takes place next time. The process is show in Fig.4.

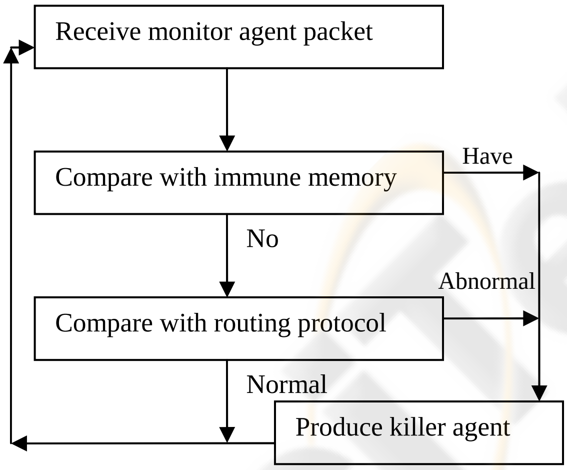
Receive monitor agent packet
Compare with immune memory
Have
No
Abnormal
Compare with routing protocol
Normal
Produce killer agent

Figure 4: The process of decision agent

Because of dynamic topology of mobile ad hoc networks, it is difficult to keep up the relationship between monitor agent and decision agent. And monitor agent can not flood the massages all over the networks for the limited wireless channel. Instead, we present a query-and-answer way. Decision agent broadcasts the query packet periodically. Monitor agents can send massages to decision agent until it receives a query packet. The decision agent in some zone may lose because the node which has decision agent moves out of the zone or the other reasons. If monitor agents in the zone have not received the query packet for a long time, they will select a new node to resident the decision agent. The approach to select a node may be competitive or negotiated.

3.4 Killer agent

When pathogen enters the body, the lymphocytes produce a lot of cells to bind and the efficient elimination of these pathogens while minimizing harm to the body. Killer agent is responsible for eliminating the invader.

A node has to depend on neighbor node's relay in mobile ad hoc network, if it joins in the network. Killer agents can get to the neighbor node of the invader and surround the invader. Killer agents may cut off the routing request of the invader and drop packets form the invader. At that time, the invader is in the network, but it has been isolated form the other nodes. As a result, the invader can not do some damage on the network any more, just as antibodies block binding between pathogens and self cells.

When a B-cell is activated, it migrates to a lymph node. In the lymph node, the B-cell produces many short-lived clones through cell division. The new B-cell clones have the opportunity to bind to pathogen captured within the lymph node. If they do not bind, they will die after a short time. If they succeed in binding, they will leave the lymph node and differentiate into plasma or memory B-cells. Similarly, when a invader is found, decision agent go into killing mode. It produces a lot of killer agents which have limited lived period. These killers try to move and surround the invader. Those agents who succeed in get to the neighbor node of the invader will live for long until the invader die. The agents who can not bind with the invader will die out after a short time.

There are four components in killer agent which are move, locate, isolate, suicide. Fig.5 shows its components of killer agent. The invader is near to decision agent, when decision agent produces killer agents. But the invader may not adjoin to killer agent. Therefore, the killer agents have to move to the neighbor of the invader. Locating components search the location of the invader and tell moving component how to move. When killer agent get to the neighbor of the invader, isolating component takes action to drop all packets from the invader. When killer agent can not get to the neighbor of the invader within a period of time or the invader die, killer agent will commit suicide by suicide component. The suicide component prevent killer agent from occupying a lot of resource.

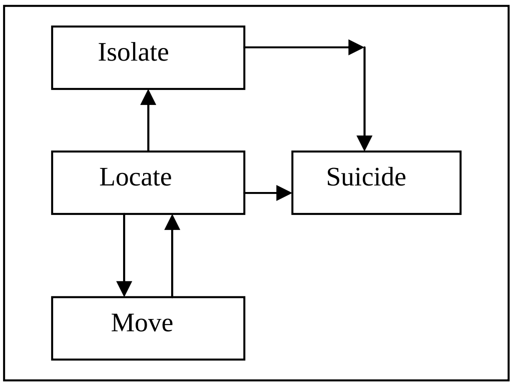

Figure 5: Components of killer agent

3.5 Mapping the immune system to security architecture

We compare mobile ad hoc networks to body and carry out the function of all kinds of lymphocytes by the special agent. Tab.1 shows the map between the immune system and the security architecture.

Table 1: The map between immune system and architecture

Immune system	Security architecture
Body	Mobile ad hoc networks
Self-cells	Normal nodes
Pathogen	Invader
Lymphocytes	Mobile agents
Antibody	Killer agent
B-cell	Decision agent
T-cell	Monitor agent
Bind	Killer agents surround and isolate the invader
Memory cell	Immune memory database

4 EXAMPLE

In order to discuss how to work in the security architecture further, we bring forward an example to explain the process of intrusion detection and intrusion response. Fig.6 is the topology structure of mobile ad hoc networks. There are 15 nodes in the networks and the neighbor nodes communicate by bi-direction link. There are three decision agents who reside on nodes C, L, O respectively and each node has monitor agent which monitors its neighbor node's behavior. Node H is the intruder.

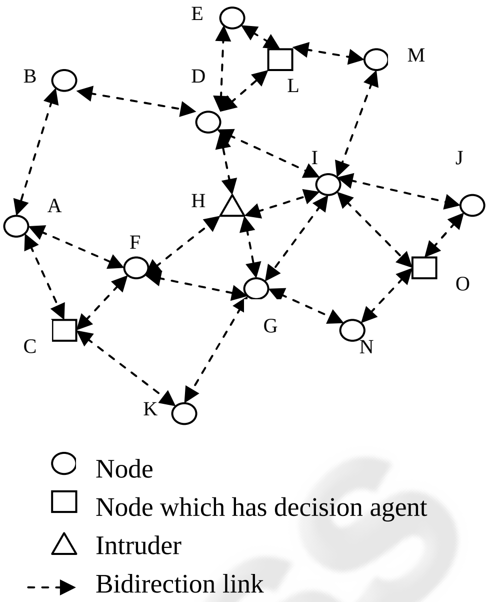

Figure 6: the topology of ad hoc networks

Fig.7 shows how the intruder attacks the mobile ad hoc networks. The node H broadcast a lot of useless packets by the neighbor nodes. The packets flood all over the networks and consume most of network's resource so that the other nodes can not send and receive the packet normally.

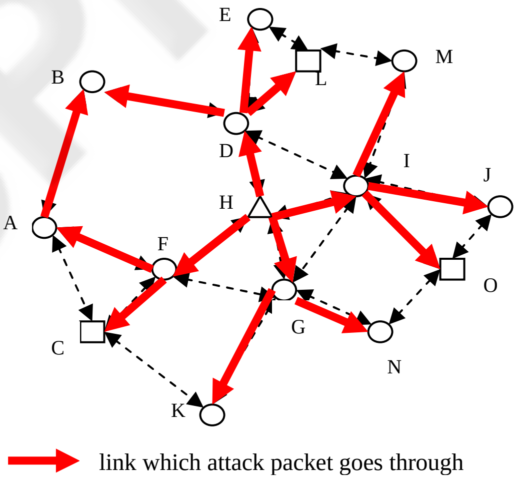

Figure 7: The attack of the intruder

Fig.8 shows the process which killer agents surround and isolate the intruder. The process of response may be composed of intrusion detection and intrusion response when the intruder attacks the networks. Firstly, the intruder must be found and located. When node H floods a lot of useless packets, the monitor agents in the neighbor node of H will monitor node H and code the behavior of H. If node H broadcasts Route Request packets, its behavior will be coded as “666666” according to the rule of Section Ⅲ. The monitor agent in node F sends the message to the decision agent in node C. The monitor agent in node D sends the message to the decision agent in node L. The monitor data in node I, G will be sent to node O. When decision agent receives these monitor data, it matches the data with immune memory. If the kind of attack has been recognized once and its signature has been stored in immune memory database, the decision agent will recognize the attack by immune memory at once. Otherwise, decision agent will make a judge by security policy. By the above way, the attack is recognized and the intruder is identified. Then the decision agent produces killer agents to isolate the intruder. The kill agent, who is produced by decision agent in node C, gets to node F by link CF and then breaks the link FH. Likewise, killer agents from node L, O get to the other neighbor node of H and meantime break the links DH, IH, GH. In the end, the intruder is surrounded by the killer agents in neighbor node and isolated because all links is broken. Just as Fig.8, the killer agents surround the intruder and construct a mobile firewall. The mobile firewall can isolate the intruder and moves with the intruder.

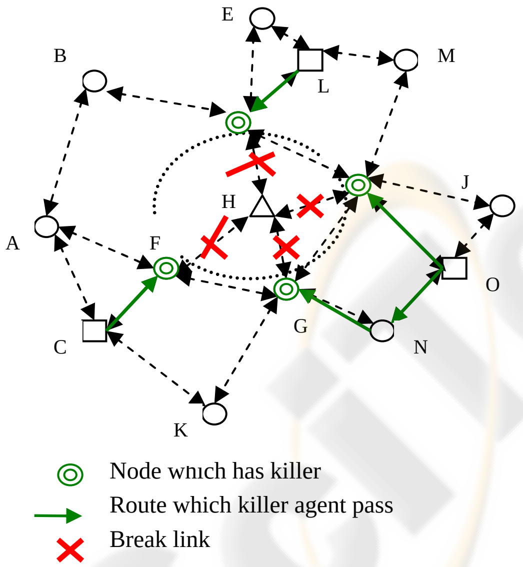

Figure 8: Killer agents surround and isolate intruder

5 PROPERTIES OF SECURITY ARCHITECTURE

As a consequence of the immune analogy, there are many important properties that our architecture exhibits.

5.1 Distributability

Lymphocytes in immune system are able to determine locally the presence of an infection. No central coordination takes place, which means there is no single point of failure. Mobile agents regard as lymphocytes in our architecture. Monitor agent can collect information independently; Decision agent can independently analyze, judge and respond. And killer agent can move and surround the invader independently. They all can work without central management. This may be a distinct feature between our security architecture and the traditional security system.

5.2 Autonomy

The immune system does not require outside management or maintenance. It autonomously classifies and eliminates pathogens. Our decision agents also make a judge who is an invader by it collected information and its policies without outside intervention.

5.3 Adaptability

The immune system learns to detect new pathogens, and retains the ability to recognize previously seen pathogens through immune memory. In our architecture, if a new invader is found, its behavior signatures are extracted. These signatures will store into immune memory database for secondary response. When two decision agents move closely, they can exchange their data in immune memory database. By the way, the signature of the kind of invaders will spread over the whole network, wherever the invader goes, it will be found at once.

5.4 Identity via behavior

In many security systems, the node is differentiated by ID, such as IP address. As a result, an invader may change its ID and become a well behavior node. Our security architecture, in contrast, does depend on ID. Instead, we identify an invader by its behavior without its ID. Therefore, whatever it changes its ID into. it will be found as long as it does not change its behavior.

5.5 Scalability

Our architecture is scalable in that adding more nodes will not increase the computational requirements of any existing node, because detection and response is local and distributed. Monitor agent only communicate with local decision agent and each decision agent can make a judge independently. This is desirable because the system should be scalable to very large networks.

6 CONCLUSIONS AND FUTURE DIRECTIONS

We propose the immunity-based security architecture for mobile ad hoc networks. Inspired by immune system, we compare mobile ad hoc networks to body and invaders as pathogens. Mobile agents corresponded to lymphocytes detect and isolate the invader. Just as immune system, our architecture owns some advantages, such as distributability, autonomy, adaptability and so on.

In future, we will develop the architecture in two directions. Firstly, we have designed an efficient algorithm to find the invader behaviour(Ping Yi, 2005). Secondly when an invader is found, killer agents want to surround and isolated it. How killer agents quickly move to the neighbour node of the invader and surround it is also our further work.

REFERENCES

S. Corson, J. Macker, 1999, Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations, RFC 2501, January 1999

Srdjan Capkun, Levente Nuttyan, Jean-Pierre Hubaux, 2003, Self-organized public-key management for mobile ad hoc networks, IEEE Transactions on Mobile Computing, 2(2003)1, 52-64

Lidong Zhou, Zygmunt J. Haas, 1999, Securing ad hoc networks, IEEE Networks Special Issue on Network Security, 13(1999)6, 24-30

P.Papadimitratos, Z.Haas, 2002, Secure routing for mobile ad hoc networks, in Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, January 27-31,2002

Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2002, Ariadne: A secure on-demand routing protocol for ad hoc networks, in Proceedings of the MobiCom 2002, Atlanta, Georgia, USA, September 23-28, 2002, 12-23

Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, 2002, A secure routing protocol for ad hoc networks, in Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), Paris, France, November 12-15, 2002, 78-86

Yih-Chun Hu, David B. Johnson, and Adrian Perrig, 2002, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), Calicoon, NY, June 2002, 3-13

Yongguang Zhang, Wenke Lee, 2003, Intrusion Detection Techniques for Mobile Wireless Networks, Wireless Networks, 9(2003)5, 545-556

S. Forrest, S. Hofmeyr, and A. Somayaji, 1997, Computer Immunology, Communications of the ACM, 40(1997)10, 88-96

S.Hofmeyr , S.Forrest , 1999, Immunity by design: An artificial immune system, In Proceedings of the Genetic and Evolutionary Computation Conference (GECCO), Morgan-Kaufmann, San Francisco, CA, 1999, 1289-1296

S. Hofmeyr, S. Forrest, 2000, Architecture for an artificial immune system, Evolutionary Computation Journal 8(2000)4, 443-473

S. Forrest, A.S. Perelson, L. Allen, R. Cherukuri, 1994, Self-nonself discrimination in a computer, In Proceedings of the 1994 IEEE Symposium on Security and Privacy, Oakland, CA, May 16 - 18, 1994, 202-214

J.Kim, P. J.Bentley, 1999, Negative selection and niching by an artificial immune system for network intrusion detection, Genetic and Evolutionary Computation Conference (GECCO '99), Orlando, Florida, July 13-17,1999,149-158

Dipankar Dasgupta, 1999, Immunity-based intrusion detection systems: A general framework, In the proceedings of the 22nd National Information Systems Security Conference (NISSC), Arlington, Virginia, USA, October 18-21, 1999,147-160

Ping Yi, Yichuan Jiang , Yiping Zhong, Shiyong Zhang, 2005, Distributed Intrusion Detection for mobile ad hoc networks, The 2005 International Symposium on Applications and the Internet (SAINT2005), Trento, Italy, January 31 - February 4, 2005