J. Basic. Appl. Sci. Res., 3(1s)160-164, 2013
© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Application of Artifical Immune System for Detection of Misbehaviour Nodes in Mobile Ad Hoc Network

Behzad Mahdavi[1], Bahram Najafpour [2], Saeid Nejhad Hoseini[3], Mahmoud Sardarpour[4], Narges Latifi Navid[5]

[1]Department of Computer Engineering, Science and Research branch, Islamic Azad University, Ardabil, Iran
[2]Sama technical and vocational training college, Islamic Azad University, Ardabil Branch, Ardabil, Iran
[3]Department of Computer Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran
[4]Department of Computer Engineering, Science and Research branch, Islamic Azad University, Ardabil, Iran
[5]Department of Computer Engineering, Germi Branch, Islamic Azad University, Germi, Iran

Received: June 10 2013
Accepted: July 11 2013

ABSTRACT

The absence of a centralized management of a standardized infrastructure for mobile networks is important. Since this kind of networks are centrally managed, and also dynamic topology and have limited power, Thus providing a secure environment for MANET routing is very difficult. Artificial immune system is presented a paradigm relatively new and promising for solving the problem of security in Ad hoc mobile networks. Artificial immune system maintained network security by determine unsafe nodes and removing all network unreliable nodes. The purpose of this study, applications of artificial immune system for detecting attacks on Ad hoc mobile networks routing protocols.

KEYWORDS: artificial immune systems, misbehavior nodes, MANET, danger theory, attacks.

1. INTRODUCTION

Ad hoc mobile networks [1], are the self-organized networks without infrastructure and centralized management. Having all nodes as terminals requires that all nodes participate in a common routing protocol. Routing will work properly only when all nodes run, routing protocol. MANET does not have fixed infrastructure, so in Compared to the fixed-infrastructure networks, are more vulnerable to security threats. These threats can cause Misbehavior network nodes.

A possible reason for the Misbehavior of nodes, is inappropriate software or hardware. Another reason of misbehavior is due to a desire to save battery. Some nodes to run a fake ID, and then participate in routing. For example, the packages are no forward. Some nodes may actually be damaging their efforts to bring down the network performance. Internet viruses and worms such as this are malicious. If the misbehavior of a node can be detected from its neighbors and the neighbors can remove the node from the network. Well behaved node saves resources and improve the communication quality. Otherwise, the network may lose its structure and its navigation is disrupted.

Thus the nodes recognize Misbehavior and create an extensive list of Misbehavior and improve these anomalies in the network can be provided. The human immune system (HIS) to protect against viruses, bacteria and other pathogens that cause harm to the body, is very successful. MANET as a mobile, decentralized, limited energy and limited capacity of wireless networks, Need to provide your environment using the system stronger, more self-finding and self-understanding algorithms, such as artificial immune systems. Because of this we need to have a biologically inspired approach to MANET is essential to the human immune system [2] [3].

Artificial Immune building concept to dynamically detect and adapt to new threats. When a cell is damaged, danger signals are produced in the immune response should be issued [4] [5]. In this paper, we studied applications of artificial immune system for detecting attacks in MANET and the security issues in MANET investigated and studied artificial immune system and attempt to evaluate the overall concept inspired from the human immune system and its mapping to the MANET.

2. Attacks under the MANET

MANET is a group of wireless nodes that form a temporary network and concentrated without central management, with each other and there is no trust between nodes. This feature leads to the conclusion that this network model, compared to most other types of networks are under attack. MANET can be attacked by using several techniques. Therefore it is necessary to classify security attacks take place within the MANET. This classification is shown in Figure 1 below.

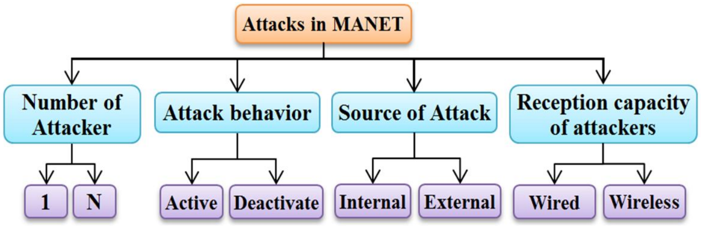

Fig. 1. Classification of attacks in MANET

Corresponding author: Department of Computer Engineering, Science and Research branch, Islamic Azad University, Ardabil, Iran. Email address: Behzad.M966@yahoo.com;Mobile:0098-9399520366

Basically Routing protocols are faced with two types of security threats internal attacks and external attacks. External attacker could inject false information into the network as enemy and cause to prevent the routing is functioning properly. Internal attacker is a node that may supply false information.

3. Malicious and selfish nodes in MANETs

Malicious nodes can disrupt proper operation of routing protocols by changing routing information [6]. This nodes do with false routing information and impersonate other nodes. On the other hand selfish nodes by simply refusing to participate can be reduced the operation of the network performance. Finest types of active attacks is create a tunnel [7] in the network between Malicious node that is via it to make a private connection and circumvention network. This type of attack allows a node to short- circuit the normal flow of routing messages constructing a virtual vertex cut in the network. Malicious nodes can modify protocols in order to subvert traffic carried attacks can easily be integrated. There for an attacker can cause reduction in network traffic, and Direct to different parts or a long path to a destination be elected, which increases the communication delay.

4. Natural Immune System

The body has many defense mechanisms. Among of them skin, Membrane of hollow organs and vessels of the adaptive immune system. adaptive immune response represents a specific foreign substance and illness (antigen). This adaptive immune reaction is made to better recognition for the detection of antigen encounter and a memory. The high-speed memory and improve the adaptive immune response for exposure with the future is antigen. Defensive reactions are divided into three types: non-specific defensive reactions, defensive reactions to certain immune responses inherited, defensive reaction. Adaptive immune system is part of a specific immune response. In natural systems, the antigen is a substance that can cause an immune response. Reaction of the immune is response to antigens.

Antigens can be either bacteria, fungi, parasites and viruses. Antigen is known as foreign (non-self). Immune reaction by secreting proteins called antibodies takes place. All body cells, with the end of his life during a natural process called apoptosis, which die of any other mode of cell death, called necrosis or unnatural death. In this case chemicals are released into the surrounding cells and propagation of this material may damage other cells and cause their death is unnatural. Any connection between the two cells, called induced signal. Signal (token) is sent and received by direct contact two cells or through the release of chemicals being transported. Signal reception, creates interact in the cell. Intracellular signals may be combined to define and meet their new signal.

Therefore signals create complex relationships between body cells which are difficult to analyze [8].All body cells are produced in the bone marrow. Some of these cells are large cells and particles of white blood cells known as phagocytes. Phagocytes including, macrophages and neutrophils. Macrophages are versatile cells that secrete chemicals have an important role in T cell activation. Other cells in small white cells are known lymphocytes. There are two types of lymphocytes: B cells and T cells, both of them are made in the bone marrow. B and T cells have receptors on their surface that recognize patterns and external signals they receive from their cells to be enabled. B and T cell s be active by observation of unknown antigen and receiving chemical signals from environment, Some of immune cells Such as B cells and dendritic cells (DC) can swallow Anonymous antigens And after analyzing and processing them, Using a set called MHC- II exists only in these cells, Bring to the surface and called to offer. Cells that are able to perform this task, are called antigen presenting cells (APC). Therefore cells capable of APC, have a primary diagnosis of the situation and recognize the symptoms as they migrate to the lymph nodes. There, the cells with the findings to other immune cells and persuade them to initiate an immune response against pathogens are widespread [9] [10].

5. Mapping Security Architecture to the Biological Immune System

Mapping of biological immune systems for MANET Mobile Ad hoc range is mapped with the human body. Represented mobile nodes in MANET similar to lymph nodes in the human body is intended. In MANETs there is trusted nodes and compromised nodes. Compromised node is also called malicious nodes that can route the packet loss. But leads trusted nodes to forward packets to the destination and at the right time. Compromised nodes can lead to forward data to the wrong and data can also lead to a nodes that is not the destination. Antigens have been drawn with the sequence of normal observed patterns. Biological immune system with MANET, for guarantee Ad hoc mobile network is mapped malicious attacks. System for secure Ad hoc mobile networks by biological immune system called artificial immune systems in the human body, Presented. As shown in Table 1 can be mapped to the human immune system with Ad hoc mobile networks. Mobile nodes play the same role that lymphocytes it plays in the body.

Table 1. Mapping immune system to security architecture

Natural immune	Security approach
Body	Mobile nodes
Lymph nodes	Mobile nodes
Self	Normal behavior
Antigens	Sequence of normal observed patterns
Detectors	Special patterns
Antibodies	A pattern with the same format as representation of antigen

6. Artificial Immune System

MANET security in artificial immune system is suitable for use in MANET security. Decentralization and volatility in the MANET nodes are the key features. Same scalable system that can be characterized by a centralized system, would affected. Numbers of artificial immune system have been made for a wide range of applications such as document classification, fraud detection and host-based intrusion detection. For protect the security, immune agent is created by using artificial immune system, Agent residing on basic nodes in domain, and a copy of these Artificial immune to other node inputs will be sent during new connection.

6.1. Related work in artificial immune system

In [11] [12] Using Artificial Immune Systems (AIS) for intrusion detection in wired networks is local. Work they is that based on part of the negative selection model - non-self and others is a danger signal. TCP connections a role Self and non-self-cells play. A connection by a triple encoding the sender address, recipient address and port number of the caller is shown. In [13] Use of an artificial immune system approach for intrusion detection based on negative selection and genetic algorithms. In [14] shown between immune system (HIS) and Intrusion Detection system (IDS) research on the immune system's methods for intrusion detection. The study presented in this paper will focus on an overview of IDS For AIS researchers to identify the appropriate research issues. Artificial immune system for detecting mistreating Ad hoc mobile networks with both innate, adaptive systems and the danger signals is presented [15]. In this paper [16], Comparative between Ad hoc Mobile Network Security in routing layer through watermarking and shows the artificial immune system. also analysis Security framework is proposed to provide security Bee Ad hoc protocol. The results obtained in this paper indicate that the artificial immune system based on safety, cost power consumption is very low compared to cryptographic systems.

7. Build the Immune System for Misbehavior Nodes

The human immune system (HIS) to protect against viruses, bacteria and other pathogens that cause damage to the body, is very successful. The body immune system produce immune cells and identifies training injuries. There are many Algorithmic and Conceptually models who are trying to explain Mode of action the human immune system (HIS). Methods of Artificial Immune system (AIS) used these concepts and algorithms (HIS) to solve similar problems in artificial systems. Using an artificial immune system method to overcome the limitations of traditional methods of detecting Misbehavior. Map the concepts and algorithms of the human immune system to a mobile ad hoc network and distributed artificial immune system to detect Misbehavior in DSR. Each node detection algorithm runs based on their observations. Signals are exchanged among the nodes. Figure 2 shows this issue [17].

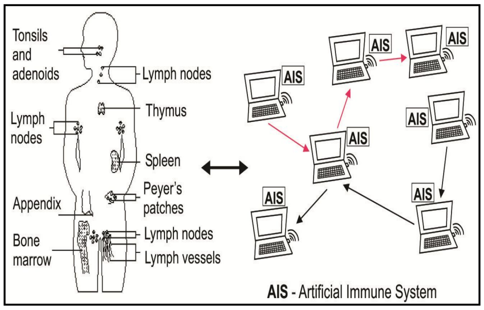

Fig. 2. Create the routing for misbehavior node

8. Misbehavior Node Detect in MANET routing

Dynamic Source Routing (DSR) [18] is one of the communication protocols between node can be terminal and the mobile phone network, is used. a mobile ad hoc network consists Number terminal node, each with a device radio communication Terminal nodes are added to the network. There is no infrastructure between nodes. Thus, the nodes are not only function of terminal but also as a Relay (Repeater) function to send data on the network. this type of network topology need to a routing protocol such as DSR is common. Therefore, the proper implementation of DSR protocol by Ad hoc network nodes is very important. Sometimes misconduct is a node in the network. This misbehavior can be have nodes in the standby mode (Standby) are in effect. Hardware failure and malicious software (eg viruses) in nodes can lead to the network be toppled. A danger theory inspired artificial immune system is proposed in [19], [20] to detect malicious nodes in Ad hoc mobile networks. Each node in the network consists is a example of this algorithm inspired by observations made by the node on which it is applied.

Themeselves as a network With Normal traffic and without packet loss is defined. Namely dynamic is defined as a node in the network is invisible and without packet loss will generate new traffic. For example, dynamic self. each node in the network, traffic Neighbor nodes monitor / sees a. this observations are buffered For a time buffering. Available detectors have detected the its own models is removed and replaced with new detectors have. Negative selection is used to generate the detectors. Observations will provide a buffer to the Available detectors. If the detector is consistent with the observations, it is awarded a positive score, otherwise it has a negative rating. When a detector is consistent with the observation that if observed is risk associated with the signal. Detectors are clustered according to the scores obtained. If a source node the Experience of packet loss (misbehavior node) to be the source node starts to generate a danger signal, along with the observed the package is missing. Action taken by neighboring nodes is that observation is the buffer the observation of the signal associated with danger (as observed) is. This prevents the generation of non-self-detector is observed.

9. DCA uses to detect attacks

Many properties are shared between the MANET and the innate immune system. One important issue is that the two environments are open and encounter with outside or inside attacks. All this subscriptions cause using the capabilities of ASI Ad hoc mobile networks are better in detecting attacks. Dendritic cells is one of the innate immune cells that inspired the danger intrusion detection algorithm based on the DCA called ASI. The body 's natural immune system, dendritic cells, the antigen presenting professional cells that have play a key role in the initiation and maintenance of primary and secondary T cell responses play. DCA inspired by immunological studies In the biological role of dendritic cells and their quality can be used as mobile anomaly detector [21]. According to the biological model based on DCA, each DC input signals at inputs and a set of antigens available in four main groups are as follows:

1- Pathogen associated molecular pattern signal (PAMP)
2- danger signals
3- signals Secure
4- inflammatory signals.

10. Danger Theory

Danger theory to explain the immune response extensively was studied and this theory as a more complete model of science of immunology to design efficient artificial immune systems, it seems quite reasonable and accurate. Danger theory states that Cells, consistent with Immune system, are unable to attack to own host, because every cell is able to do this during the removal process maturity. Immune reaction Danger theory (DT) as a reaction to a stimulus is harmful to the body, not just a simple response that is none intended. In danger theory Foreign and allow immune cells to be together and this is the photo of artificial immune system [22].

Danger theory is a hypothesis that abnormal cells dying and Or anxious may be a release danger signal to cover a small area around the cells, Antigen reagent cells (APCs received) this signal and, in turn, stimulates the immune system cells. Theory Danger structure is shown In Figure 5. Because Danger signals activated the programs (APCs), B and T cells in turn stimulate the rules are as follows: Signal 1 (sig 1) immune cells to pattern of anti- genetic or a piece of antigens presented by the program connects. Signal 2 (sig 2) or T helper cells help to activate the signal given by a B cell or a signal for activation of T cells stimulated by the plans. In a word, the theory suggests that the adaptive immune system can signal Danger insider Danger from outsiders to detect. Immune reaction causes the Danger signals are produced by damaged cells. Figure 3 shows the architecture using the idea of immune Danger theory, that developed by Danger theory. Kaiser [23] proposed danger theory of artificial immune system to solve in identification problem. Thymus [24] used Danger theory to improve the dynamic data clustering algorithm in Self-organizing device security management capacities (SOSDM) was applied in 2003.

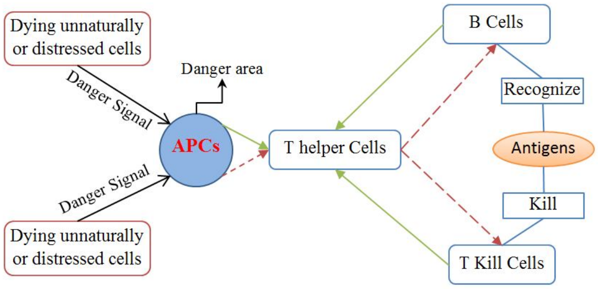

Fig. 3. The structure of the danger theory

11. Discussion

MANETs is a collection of mobile nodes each of which acts as a router. MANET nodes are responsible for forwarding traffic from the source node to the destination node through intermediate nodes. Lack of focus and Instability node is key features of MANET. There are two types of attacks in MANET internal attacks and external attacks. In internal attack, the nodes in the network Can be fall in danger and other nodes be misled and false nodes can redirect the packages. MANET nodes can also join the group or range without Need to leave, generally not to be trusted markers. Foreign invaders packages from wrong path to the node false lead. Ad hoc mobile networks are weak in the security attacks, and has already done a lot of research on Ad hoc Network Security in terms of confidentiality, integrity, authentication, availability and justice focus. Routing protocol design for mobile Ad hoc networks are very difficult.

There are many techniques for mobile Ad hoc networks safety, such as watermarking. Watermarking is an efficient mechanism for providing secure, but it has a huge overhead. Therefore, an approach using similar system biology immune system is the body that is known as artificial immune systems. Reason for using of artificial immune system is that the body's immune system, the body against damage caused by excessive bacteria, viruses, parasites, and fungi that protect the pathogen is known. Therefore doing such action without prior knowledge of pathogen structure is difficult and long. Artificial immune system by specifying a non-trusted nodes and Removing all nodes and unreliable networks, network security is maintained.

12. Conclusion

To achieve Secure routing protocol is important work that the unique characteristics of Ad hoc wireless networks a challenging. In recent years the use of the natural human immune system in computing systems caused to artificial immune system by the different applications. Most of these systems are designed based on the model of insiders and outsiders. The importance study Application of danger theory as the full model, the artificial immune system is felt and Need to this model for Use in the detection and prevention of attacks in MANET can be very helpful. In this paper an overview of the different security objectives, security threats and detection Misbehavior nodes on DSR routing protocol did display. Also advantage of theory danger the AIS-based intrusion detection algorithms, called DCA, For identifying attacks in mobile ad hoc networks examined and We expressed That dendritic cell use algorithm can be very useful in detecting various attacks in MANET networks.

REFERENCES

[1] Giordano, S., Mobile ad hoc networks. Hand book of wireless networks and mobile computing. P. 325–346.

[2] Le Boudec, J.Y. and j.s. Sarafi, An artificial immune system approach to misbehavior detection in mobile ad hoc networks, Biologically Inspired Approaches to Advanced Information Technology, 2004. P. 396-411.

[3] Sarafijanovic, S. and J.Y. Le Boudec, An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks, Neural Networks2005, IEEE Transactions on, 16(5):1076–1087.

[4] Uwe, A. and C. Steve, The Danger Theory and Its Application to Artificial Immune Systems, Information Infrastructure Laboratory HP Laboratories Bristol, 2002.

[5] Carvalho, M., R. Ford, A. William and M. Gerald, Securing MANETs with BITSI: Danger Theory and Mission Continuity, 2008 .Proc. of SPIE Vol. 6973 69730D-1.

[6] Kargl, F., S. Schlott, M. Weber, A. Klenk and A. Geiß, Securing Ad hoc Routing Protocols, in Proceedings of 30th Euromicro Conference 2004, Rennes, France.

[7] Hu, Y.C., A. Perrig and D.B. Johnson, Packet leashes: adefense against wormhole attacks in wireless networks, In INFOCOM. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003. volume 3: 1976–1986.

[8] Andries, P., computational intelligence, university of Pretoria south. Africa, WILEY, 2003.

[9] Goldsby, R. A., T.J. Kindt, B.A. Osborne and J. Kuby, Immunology, 5th Ed., W. H. Freeman & Co, 2002.

[10] Meyer, B.J., H.S. Meij, S.V. Grey and A.C. Meyer, Fisiologievan diemens -Biochemiese, fisiese en fisiologie \sebegrippe. KagisoTersier - Cape Town, first edition, 1996.

[11] Hofmeyr, S.A., An Immunological Model of Distributed Detection and it's Appli cation to Computer Security. PhD thesis, Department of Computer Sciences, University of New Mexico, 1999.

[12] Hofmeyr, S.A. and S. Forrest, Architecture for an Artificial Immune System. Evolutionary Computation, 2000. 7(1): 45-68.

[13] Dipankar, D. and G. Fabio, An Immunity-Based Technique to Characterize Intrusions in Computer Networks., IEEE Trans, 2002. (6)9: 1081.1088.

[14] Jungwon, K.E., Immune system approaches to Intrusion Detection- A Review, 2006.

[15] Slavi, S.j. and Y.L.B. Jean, An Artificial Immune System for Misbehavior Detection in Mobile Ad Hoc Networks with both Innate, Adaptive Subsystems and with Danger Signal, Proceedings of AISB 2004 Symposium on The Immune System and Cognition, Leeds, 2004. UK: 45-46.

[16] Nauman, M., Energy Efficient Security in MANETs: A Comparison of Cryptographic and Artificial Immune Systems, Pak. J. Engg. & Appl, 2010. Vol. 7, Jul: 71-94.

[17] SlavisaSara, j. and Y.L.B. Jean, An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors, Springer, 2004. P. 342–356.

[18] David, B. J. and A.M. David, Dynamic source routing in ad hoc wireless networks, in Mobile computin, 1996. ch.5.

[19] Abdelhaq, M., R. Hassan and M. Ismail, Detecting Sleep Deprivation Attack over MANET Using a Danger Theory-Based Algorithm, IJNCAA, The Society of Digital Information and Wireless Communications, 2011. P. 534-541.

[20] Feixian, S., Artificial Immune Danger Theory Based Model for Network Security Evaluation, journal of networks 2011. vol. 6, no. 2.

[21] Julie, G., A. Uwe and C. Steve, Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection, ICARIS, 2005.

[22] Aickelin, U. and S. Cayzer, The Danger Theory and Its Application to Artificial Immune Systems, Information Infrastructure Laboratory HP Laboratories Bristol, 2002.

[23] Aickelin, U. and S. Cayzer, The danger theory and its application to artificial immune systems, Proc. of the 1st International Conference on Artificial Immune Systems, 2002. P. 141-148.

[24] Thymus, Conference on Artificial Immune Systems, 2003. Springer LNCS 2787: 194-203.