An Immune Inspired Approach for Detecting Packet Drop Attacks in MANET

Deepak KR
Assistant Professor,
Bannari Amman Institute of Technology,
Sathyamangalam, Tamil Nadu.

T.V.P.Sundararajan,
Associate Professor,
Bannari Amman Institute of Technology,
Sathyamangalam, Tamil Nadu.

ABSTRACT
Security is one of the major issues in the case of wired and wireless networks. The rapid proliferations in the area of Mobile Adhoc Networks (MANETs) have changed the landscape of network security. MANETs are self organizing, infrastructure less, multi hop networks where the constituent nodes act as both hosts and routers simultaneously. Dynamic topological changes and constantly moving nodes in the network make MANETs more vulnerable to a variety of attacks than traditional networks. In this paper we deal with misbehavior nodes in MANETs that drop packets instead of forwarding them towards the destination. To defend against this attack we propose a novel intrusion detection system (IDS) that is motivated by the human immune system. Recently, IDS techniques that are inspired from the Immune System (IS) of human beings are gaining importance since immune systems are robust, accurate and highly adaptable in detecting any new intrusion. From the results it is shown that the proposed immune AODV provides better performance than the normal AODV in the presence of packet dropping nodes in the network.

Keywords
Security, Mobile Ad Hoc Networks (MANET), Intrusion detection Systems (IDS), Artificial Immune Systems (AIS), Immune system or Natural Immune System.

1. INTRODUCTION

1.1 Mobile ad hoc networks
Mobile Ad Hoc Network (MANET) is defined as a self-configuring, infrastructure less, multi-hop wireless network consisting of constantly moving nodes. Each mobile node in the MANET is free to move inside as well as in and out of the network without any restriction and hence it exhibits highly dynamic topological changes in the network. The network is an infrastructure less network since there is no centralized control or server to control the activities of constituent nodes. For this purpose, each node in the network performs all the functionalities of the network on its own without any centralized control and also each node is responsible for forwarding the data sent by some source node in the direction of the intended destination.

Fully self-organized MANETs [1] can be thought of as a group of strangers working towards accomplishing a common objective. These people are not related to each other and do not share any common keying material on their nodes. Therefore the network thus created has to be operated and managed by the nodes themselves. This increases the load on each and every node of the network and eventually the network operation becomes dependant on the co-operation and trusting between the nodes. The relative position of the nodes with respect to each other is constantly changing and hence the overall network topology is unpredictable. Hence routing protocols that are designed for MANETs need to consider such eccentric network topologies, self organizing nature and distributed operation of nodes. While viewing from a security perspective, distributing all the functionalities of the network to as many nodes as possible makes it hard to concentrate on a single point of attack. Hence special procedures and protocols need to be evolved to incorporate security mechanisms for ad hoc networks.

1.2 Need for intrusion detection systems
The rapid development in the area of wireless networks and mobile computing applications has changed the entire perspective towards network security. The mobile nature of nodes creates new threats and problems that do not exist in a fixed wired network, and as on date many of the successful security measures turn out to be ineffective. Therefore, the traditional method of securing networks with firewalls and encryption algorithms is no longer effective in the case of MANETs thereby creating the need for new architectures and mechanisms to protect the wireless networks. Intrusion prevention mechanisms such as encryption and authentication [2] can be used in ad-hoc networks to reduce intrusions, but one cannot completely eliminate the intrusions as there is no fixed point of attack in MANETs. Intrusion detection systems can be thought of as a "second wall of defense" and it is a necessity in any mobile adhoc environment which has inherent vulnerabilities due to mobility, medium access, security and so on. Therefore an Intrusion detection system [3] can be used as an added security layer or as a second wall to protect network systems. This is because once an intrusion is detected as in the case of early stage of a DDoS attack[4], a response mechanism can be put into place to minimize damages caused by the attack and also gather evidence for audit data, and even launch counter-attacks[5].

2. RELATED WORK

2.1 Traditional Intrusion Detection Approaches
Traditional intrusion detection or misbehavior detection approaches use the knowledge of already known intrusions or misbehavior patterns and detect them by searching for similar patterns in the network activity. Thus this type of intrusion detection is very proficient when that particular attack is known in advance. In [6] Buchegger and Le Boudec used a reputation system in order to detect misbehaviors in DSR. In the proposed technique, every node calculates the reputation factor for every other node through its own observations as well as observations made by other nodes. Depending upon the reputation of every node, decision is taken by the reputation manager whether or not to allow the node to participate in network activity and by this way co-operation

between nodes are stimulated in the network. The IDS as described by Suchitra et al [7] makes use of an association based approach that is applied on top of traditional AODV protocol. A trust value is calculated for each node in the network and this value represents its reliability level based on which the nodes in the network can be classified as either unknown or known or companion. The nodes only routes the data through the companion node or a known node thereby isolating unknown node which might be an attacker. Srinivasa Rao et al proposed an IDS architecture [8] for detecting routing anomaly in MANETs. In the proposed system, a detection agent is attached to each and every node present in the network. The Agent makes use of data collection module, detection engine, voting module and intrusion response module in order to detect routing anomalies. Traditional intrusion detection approaches as described in [9] does not have the ability to learn new misbehaviors and adapt to new responses in order to counter attack them. For the IDS to have a better performance all of the misbehaviors have to be guessed in advanced and elaborately addressed in the detection system. This is the major drive towards opting for using an AIS approach [10] which is based on replicating the behavior of the human immune system into the wireless networks.

2.2 AIS based intrusion detection systems

Hofmeyer and Forrest used an AIS for intrusion detection in wired local area networks [11] [12]. Their work is based on the negative selection part of the self-nonself model which is a part of the human immune system activity. In their system nodes employing transmission control protocol (TCP) connections as application, play the role of self and nonself cells. One TCP connection is represented by a set consisting of sender's destination address, the receiver's destination address, and the receiver's port number and it is analogous to the self set as in the case of natural immune system. A random set of data having the same length as that of the self set, is generated and compared with the self set using the "r-contiguous" matching rule. Those which match the self set are ignored and only those which do not match the self set are taken as detectors. Non-eliminated detectors have a finite lifetime and die unless they match a nonself triplet, as in the IS.

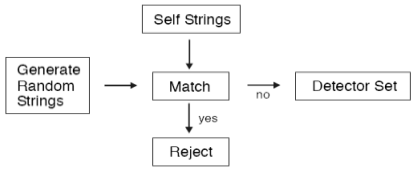

Figure 1: A flow chart representation of Negative Selection

Algorithm

The negative selection algorithm as proposed by S. Forrest et al can be summarized as follows:

- A self set S is created and is defined as the set of elements that corresponds to the normal operation of the network. The self set S is a subset of the universal set U which is a collection of all possible network activities.
- A random set of detectors R, is generated each of which fails to match any string in S. Those detector sets that match any element in the self set S are discarded and once those which are not in any way similar to that of self set are considered as elements of detector set R.
- The self set S is monitored repeatedly over some finite time and matched continuously with the detector set R. I any o the elements are found to have a match then it indicates that there is a change in the normal behavior of the network, since detector set is only formed with elements that are completely different from S.

Over the years many algorithms [13] [14] have been proposed for intrusion detection that are inspired from the negative selection algorithm as proposed by S.Forrest et al.

Lu Hong proposed a new hybrid learning algorithm [15] for the immune based detection mechanism. The modifications made were in the training phase where a real valued negative selection (RNSA) was used for matching along with a classification algorithm in order to generate detectors from the initial random set of values considered for detection generation. Each detector has an age associated with it and it is increased as the number of iteration increases, if it is inside the self-set. If the detector becomes old, i.e. if the age is above some threshold value, then it will be replaced by a new randomly generated detector. During the training stage, the input corresponds to the normal samples (feature vectors) that are used by the RNSA algorithm to generate abnormal samples. Subsequently, the normal and abnormal samples are used as input to a supervised algorithm that produces a classifier. This classifier corresponds to the anomaly detection function and is used during the testing phase to classify new samples as normal or abnormal.

S.Sarafijanovic et al [16] evaluated the way in which artificial immune systems are used in order to detect misbehavior in ad hoc networks. The concepts of natural immune system and biology were extended into MANET environments and also a better representation of the Self Set has been proposed by the authors. The definition of self-set is a major challenge while considering the case of artificial immune systems since it is not sure on the aptness of the parameters that can be used as self-set and also this eventually has a direct effect on the accuracy of the detection process. Also the proposed method gives an idea on how to map the complex immunological concepts into the computer networks. Also S.Sarafijanovic et al also proposed a method for representing the self-set with the help of the protocol events of the routing protocol such as RREP sent, RREQ received, RERR received, Data sent, Data received and so on. The framework thus enacts the possibility of applying immunological concepts into computer network terms and provides further scope towards developing a very accurate intrusion detection system [17] resembling the human immune system.

3. PROPOSED METHOD: *immune* AODV

The existing AODV routing protocol [18] is one of the most accepted and widely used on demand routing protocol. The routes are formed dynamically and only at times when there is a need to send data. When a source node has to send data to any destination node in the network it floods the Route Request (RREQ) packet in the network and sooner or later the destination node replies to the source node with the Route Reply (RREP) packet thereby forming an active route between source and destination for the data transfer. The RREQ and RREP packets of the routing protocol have the following six fields: Source ID, Destination ID, Source Sequence Number, Destination Sequence Number, Broadcast ID and TTL. AODV routing emphasizes on finding the shortest and latest path towards the destination thereby

making it inherently vulnerable to packet dropping attacks where the adversary node may easy gain access of the active path by advertising false routing information. Hence, in order to enhance AODV in terms of security a new protocol called the Immune AODV is proposed. The new protocol has the following modifications done over the normal AODV protocol and they are listed as follows

- Sequence Number Table (s-table)
- Path cache
- Gene List

Also the entire operation of immune AODV is divided into two phases called as the Learning Phase and Detection phase which are explained in sections 3.2.1 and 3.2.2.

3.1 Modifications

In order to make the AODV routing protocol immune towards the packet dropping attacks it is essential to add some features to it since there is no separate provision for security. The details of the three modifications made to immune AODV are explained in the following subsections.

3.1.1 S-table:

A sequence number table is maintained at each and every node and immune AODV checks the S-Table each and every time before forming an active route for data transfer. The S-Table at every node stores the sequence numbers of its one hop nodes situated around the node of interest and also it is exchanged between the neighbors periodically. This is mainly because of the fact that the adversary node carrying out the packet drop attack normally would generate a false RREP message to let the source node know that it holds the most recent and shortest path towards the destination. Hence the adversary node places a very high sequence number in the false RREP packet that it generates towards the source. Since AODV is hungry towards finding the shortest and latest path there is a huge possibility that the adversary node gaining access to the active path between source and destination. In order to reduce this chance, a table is maintained at every node and shared between the neighbors so that whenever a latest path or a very high sequence number is encountered in the RREP packet then there is a chance for verifying it by looking into the S-Tables of neighbor nodes before forming the path.

3.1.2 Path cache

A path cache is maintained at all the nodes in the network and the path cache entries are exchanged between the neighboring nodes in case of any suspicious behavior encountered during the path formation. The Path Cache stores only the reverse path information for the RREP packets that traverse over the network. This is mainly because of two reasons. One of the reasons is to have an option for cross checking the validity of the node that is generating the RREP packet i.e. either it has to be a valid intermediate node or the intended destination. The other reason for making the Path Cache to store only the reverse path information of the RREP message is to keep a check on the control overhead. This is because of the fact that the adversary node gaining access to the newly formed route by sending out a false RREP message.

3.1.3 Gene list

In order to successfully implement the immunological concepts like Negative Selection and Clonal Selection into the wireless ad hoc network operation it is important to define a self-set for the network very efficiently so that an intrusion detection mechanism that is as close to the robustness and adaptable nature of our human immune system can be realized. This Gene List is created at each and every node in the network and it is verified when there is a need to confirm the presence of any attacker/intruder in the network. Every now and then the gene list is created at each and every node in accordance with the protocol events associated with it at that instant of time and this is done to support the dynamic nature of MANET. The Gene List is created using the following protocol events that are recorded at each and every node in the network

- Number of RREPs received
- Time of reception of RREP packet
- Sequence Number indicated in the RREP packet
- Node ID

The S-table and Path cache at every node are made use for the purpose of creating the Gene lists. These Protocol events are grouped together and converted into 1s and 0s form at the nodes for carrying out further matching functions during the detection phase of immune AODV in order to detect the intrusion. Every node in the network should disclose its own Gene List before gaining access towards the active route of data transfer.

3.2 Operation

The operation of the entire intrusion detection mechanism based on immune AODV is divided into two phases namely, learning and detection phase.

3.2.1 Learning phase

The Learning Phase operation of immune AODV may be thought of as one analogous to the phase during which the T-cells are developed in the human body. The T-cells are created in the bone marrow and are allowed to mature in the thymus where the immature T-cells undergo Negative Selection Algorithm and come out of the thymus as matured T-cells that are ready for detecting the antigens or foreign bodies entering the human body. The bone marrow of the human body can be thought of as a protected environment where the possibility of the presence of any foreign body or non-self cell is very less. In the context of the proposed immune AODV, the learning phase is carried out in the absence of any misbehavior or attack. During the learning phase, the network is allowed to function in a normal way and free from any type of attack and the data is accumulated by means of S-Table and Path Cache. The collected data are then used for the creation of genes at the node sites as explained in section 3.1.3. Hence during the Learning phase the creation of a valid self-set may be considered done. And at the end of the Learning Phase, Negative Selection Algorithm is run on the Gene list that is created at each node and a set of detectors are created.

3.2.2 Detection phase

After the Learning phase is over, it can be thought of a scenario where the nodes are moving out of the protected environment and then the network may be exposed to packet dropping adversary nodes. When an adversary node tries to capture the route by sending out a falsified RREP which generally reaches the source node well ahead of the reply messages sent out by other legal nodes in the network, immune AODV does not grant access of the route to the adversary node unlike normal AODV routing protocol. As soon as the source node receives the RREP message then the S-Table and Path Cache are verified for any discrepancy. Then the detectors that are generated as a result of Negative

Selection Algorithm at the end of the Learning phase are used for verifying the gene list of the node that has generated the RREP message, either be it destination or any intermediate node that possess the route towards the destination.

Assuming the adversary node sending out a false RREP message towards the source with an intention of gaining access of the route towards the destination, the RREP contains a very high sequence number and also reaches the source very quickly so that the source may be lured into taking this route. By doing so, the adversary node would have generated a gene structure that would be different than the normal self-set that was created at the end of training set with respect to the normal operation of the network. As soon as the source receives the message it checks the entries in the S-Table and the reverse path information of the Path cache. The ID of the node which has generated the RREP message can be easily obtained by checking the reverse path information and the nodes that are sending out the reply messages are kept in the suspicious list initially. Now the detectors are used to perform matching functions with the gene list of the nodes originating the RREP messages and once the detectors identify the gene list of the particular node as different from that of the normal pattern then the node is declared as packet dropping node or misbehavior node and then it is isolated from the path of data transfer by denying the permission to participate in the active path between the source and destination.

4. SIMULATION RESULTS

4.1 Simulation setup

The simulation is implemented in Network Simulator-2 version 2.32 [19], one of the popular and open source simulators that support simulations involving MANET. The simulation is done for a total duration of 400 seconds of which the first 50 seconds constitute the learning phase and next 350 seconds are devoted for the detection phase operation of the proposed immune AODV. During the detection phase the network is slowly exposed to misbehavior nodes. The nodes in the network are made to follow the Random Way Point (RWP) mobility pattern where the movement of every node is independent of every other node present in the network. The key parameters that are implemented in the simulation are briefed in table 4.1.

Table 4.1 Simulation Parameters

Simulation Time	50+350 seconds {learning + detection phase}
Simulation Area	500 x 500 m
Total no. of nodes	50
Mobility model	RWP
Routing Protocol	AODV/ immune AODV
Application	CBR
Packet Size	512 bytes
% of misbehavior	5,10,15,20 %

The simulation area is set to 500 x 500 m with a total of 50 nodes in the network. The application used over the source node for data transfer is Constant Bit Rate (CBR). The packet size of a single CBR packet is 512 bytes and the packets are flowing in the network at a rate of 2 packets per second. The scenario used for the above explained simulation is shown in Figure 2. In the scenario, the misbehaving or packet drop nodes are shown in red color. Also the source node is indicated in blue color and the destination node is indicated in pink color.

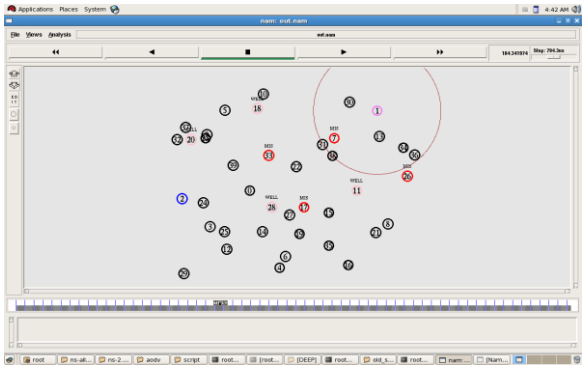

Figure 2: Snapshot of Simulation Scenario created using NS-2.

4.2 Results and discussion

As explained in section 4.1 the simulation setup is used for simulating the existing AODV protocol and that of the proposed immune AODV. Also the simulations are done by the percentage of misbehavior nodes in the network and results are obtained to evaluate the performance of both existing AODV and immune AODV in the presence of packet drop attack. The results obtained from the simulations are presented as follows.

Figure 3 shows the effect of malicious nodes on the packet delivery ratio in the simulation involving both existing AODV and the proposed immune AODV protocol. From the Figure 3, it is evident that there is a reduction in the packet delivery fraction of both immune AODV and existing AODV as the number of malicious nodes causing the packet drop attack is increased. However immune AODV sustain better PDF than the normal AODV. For example, the improvement of PDF in the case of the proposed immune AODV is 69.5 % with that of the existing AODV even in the presence of 15% of misbehaving nodes.

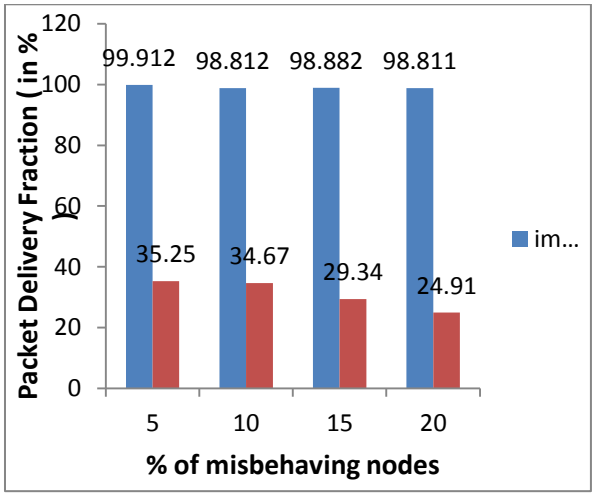

Figure 3: Effect of misbehaving nodes on PDF

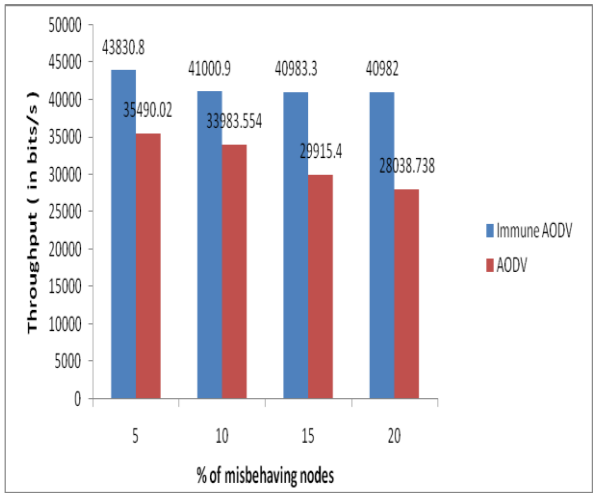

Figure 4: Effect of misbehaving nodes on Throughput

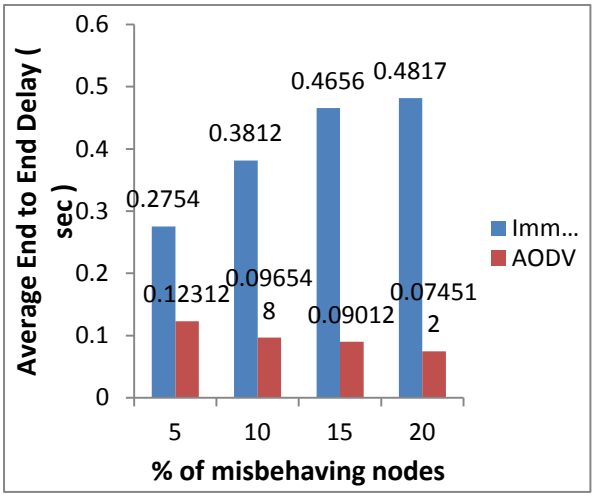

Figure 5: Effect of misbehaving nodes on Average End to End Delay

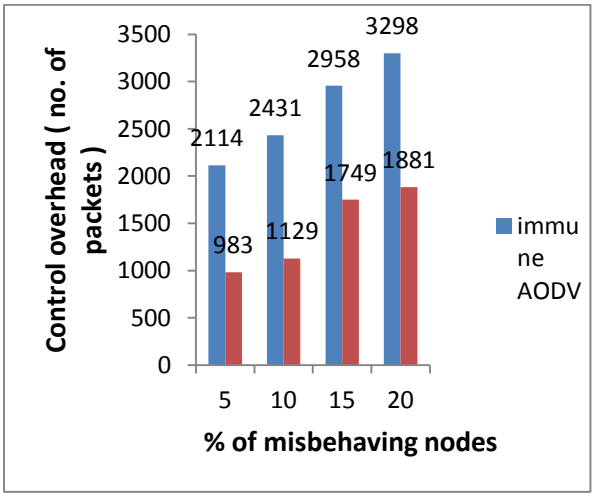

Figure 6: Effect of misbehaving nodes on Control Overhead

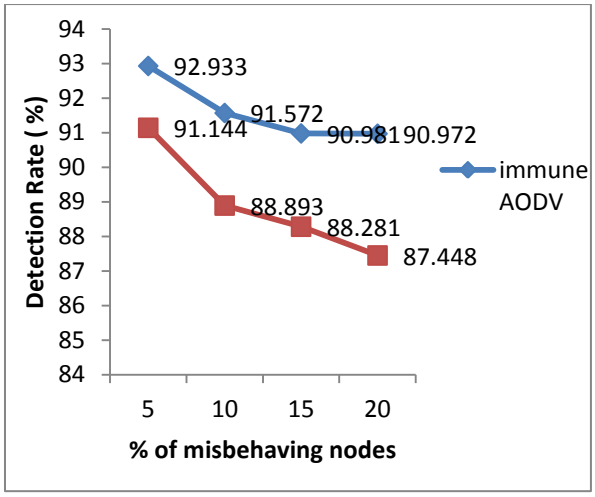

Figure 7: Detection rate

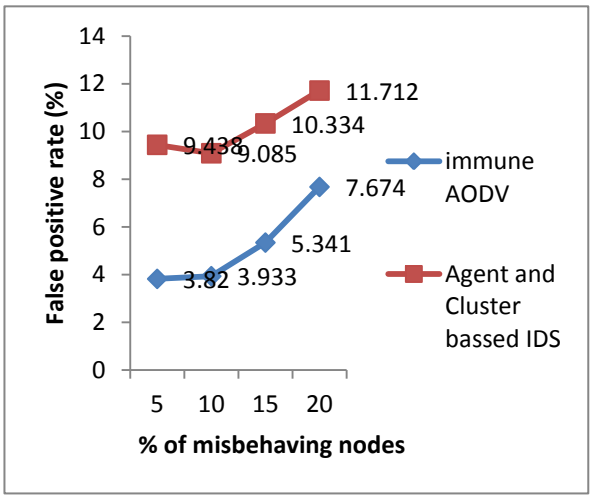

Figure 8: False Positive rate

From the Figure 4 the reduction in throughput of existing AODV under malicious nodes can be easily inferred when compared to that of throughput of immune AODV. Although there is a slight reduction throughput in immune AODV in the worst case scenario of 20% misbehaving nodes, immune AODV still presents a better performance as the throughput achieved in the case of existing AODV is much lower. Figure 5 shows the effect of malicious nodes on the average end to end delay in the simulations involving both existing AODV and immune AODV. The delay is comparatively very high for the proposed immune AODV protocol than the existing AODV and this is very obvious since packet drop node can easily get access to the route in existing AODV protocol by means of a fabricated RREP message. Also the additional security procedures added into the immune AODV reflects directly in the end to end delay of the network. Finally, the performance of existing AODV and immune AODV is analyzed in terms of control overhead. Figure 6 shows clearly that the number of control packets required for immune AODV is much higher than the existing AODV protocol. This phenomenon is normal since any intrusion detection mechanism is expected to increase the number of control packets as it responsible for mitigating all the type of misbehavior in the network.

Figure 7 and Figure 8 show the Detection Rate (DR) and False Positive Rate (FPR) for the proposed immune AODV algorithm. From Figure 7 it is clear that the proposed method is able to achieve a comparitively higher degree of detection rate than the existing Agent and Cluster based IDS (as explained in section 2.1) and at the same the false positive rate is sustained at a reasonably smaller value.

At 5% misbehaving nodes, the DR of immune AODV shows an increase of 1.8 % when compared to the IDS employed in Agent and Cluster based approach. Also in the worst case scenario of 20% misbehavior nodes, the DR of immune AODV is 3.5% greater than Agent and Cluster based IDS. Even though the FPR of immune AODV is lesser than that of Agent and Cluster based IDS, at 20% misbehaving nodes the FPR obtained through immune AODV is 7.67% which is still a slightly higher value.

5. CONCLUSIONS

In this paper an intrusion detection mechanism that is designed based on the human immune system is presented. Packet drop attacks in MANET are considered to be a very serious threat to the performance of the whole network which is evident from the results obtained from the simulations. From the graphs presented in section 5.2, it is clear that the existing AODV suffers heavily in the presence of packet drop attack in terms of important network performance parameters such as PDF, Throughput and Average End to End Delay. The proposed immune AODV provide an effective intrusion detection mechanism against packet drop attacks. The results prove the effectiveness of the proposed immune AODV over the existing AODV protocol with a 64% increase in PDF. Also there is moderate increase in the overall throughput of the network. Conventional AODV achieved a throughput of 21038 bits/s in the presence of worst case scenario of 20% misbehavior nodes whereas the proposed immune AODV achieved around 40982 bits/s which can thought of a 50% increase in the performance of the network. In terms of average end to end delay the proposed immune AODV shows a sharp increase when compared to existing AODV but this is acceptable for any intrusion detection mechanism when we consider the increase in performance of the network in terms of PDF and Throughput.

The DR of the proposed immune AODV is better than the existing Agent and Cluster based IDS as the % of misbehaving nodes is increased. However the FPR of immune AODV is slightly at a higher value at the worst case scenario of 20% misbehaving nodes. In our future work, we aim at reducing the false positive rate of the proposed immune AODV by varying the learning and detection phases accordingly.

6. REFERENCES

[1] C. Prehofer and C. Bettstetter, “Self-organization in communication networks: Principles and design paradigms,” IEEE Communications Magazine, 43:78–85, July 2005.

[2] Chaoqun Lin, Yang Zhou, Yunhua Xiao and Guang Sun, “Encryption Algorithm of RSH”, Information Technology Journal, 10(3):686-690, 2011.

[3] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), 9: 546- 556, 2003.

[4] S. Meenakshi and S.K. Srivatsa, “A Distributed Framework with less False Positive Rate against Distributed Denial of Service Attack”, Information Technology Journal, 6:1139-1147, 2007.

[5] A.Vani and D.Sreenivasa Rao, “Providing of Secure Routing against Attacks in MANETs”, Int. J. Computer Applications, 24: 16-25, June 2011.

[6] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the CONFIDANT protocol: Cooperation of nodes—Fairness in distributed ad hoc networks,” in Proc. IEEE/ACM Symposium on Mobile Ad hoc Networking and Computing (MobiHOC), Lausanne, Switzerland, pp. 80–91, 2002.

[7] Suchita Gupta and Ashish Chourey, “Performance Evaluation of AODV Protocol under Packet Drop Attacks in MANET”, in Int. J. Research in Computer Science, 2: 21-27, 2011.

[8] Srinivasa Rao D., Pandurang Vital T., Sriram T.V.S., “Detection of Routing Anomaly using IDS Architecture based on Agents and Clusters in MANETs”, Int. J. Computer Applications, 26: 36-40, July 2011.

[9] Z.Muda, W.Yassin, M.N.Sulaiman and N.I.Udzir, “A K-Means and Naïve Bayes Learning approach for better intrusion detection”, Information Technology Journal, 10(3):648-655, 2011.

[10] AISWeb - The Online Home of Artificial Immune Systems (http://www.artificial-immune-systems.org/).

[11] S. A. Hofmeyr and S. Forrest, “Architecture for an artificial immune system,” in proceeding of Evolutionary Computation., 7: 45–68, 2000.

[12] S. A. Hofmeyr, “An immunological model of distributed detection and its application to computer security,” Ph.D. dissertation, Dept. Computer. Science, Univ. New Mexico, Apr. 1999.

[13] Hu Zhengbing, Zhou Ji, Ma Ping, “A Novel Anomaly Detection Algorithm Based on Real-Valued Negative Selection System”, in proceedings of the IEEE workshop on Knowledge Acquisition and Modeling, pp. 499-502, 2008.

[14] Chen Jinyin, Yang Dongyong, “A Study of Detector Generation Algorithms Based on Artificial Immune in Intrusion Detection System”, in WSEAS Transactions on Biology and Biomedicine 4: 29-35, 2011.

[15] Lu Hong, “Artificial immune system for anomaly detection”, in proceedings of the IEEE workshop on Knowledge Acquisition and Modeling, pp. 340-343, 2008.

[16] S. Sarafijanovic, and J-Y. Le Boudec, “An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile ad hoc Networks”, in Proc. of IEEE Transactions On Neural Networks, September , 16: 1076-1087, 2005.

[17] Xianjin Fang, L.L., “An Improved Artificial Immune Approach To Network Intrusion Detection”, in proceedings of international conference on Advanced Computer Control, 2: 39-44, 2010.

[18] C. Perkins, E. Belding-Rover an S. Das, “RFC-3561: Ad Hoc On-Demand Distance Vector (AODV) Routing”. Available at: www.ietf.org/ref/ref3561.txt, July2003.

[19] Network Simulator-2, Available at: www.isi.edu/nsnam/ns.

AUTHOR'S PROFILE

Deepak KR received his B.Tech (Electronics and Communication Engineering) degree from SASTRA University, Thanjavur. He is currently pursuing his M.E. degree from Anna University, Coimbatore. His research interests lie in the field of wireless networking, especially ad hoc security. He has published 2 papers in national and international conferences.

T.V.P. Sundararajan received the BE Degree in Electronics and Communication from Kongu Engg. College, Perundurai in 1993 and the ME Degree in Applied Electronics from the Government college of technology, coimbatore in 1999. He is Associate Professor, working in Bannari Amman Institute of Technology, Sathyamangalam. He has published 12 articles in National and International journals and more than 25 papers in International and National conferences. He is doing a part time Ph.D research in Anna University, Chennai. His current research focuses on mobile ad hoc networks and wireless security. He is member of the IEEE, ISTE and the IEEE computer society.