# A Dynamic Approach for Anomaly Detection in AODV

P.VIGNESHWARAN[1] and Dr. R. DHANASEKARAN[2]

[1]Research Scholar, Anna University of Technology, Coimbatore, Tamilnadu, India,
vigneshwaran05@gmail.com
[2]Director, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India,
rdhanashekar@yahoo.com

***ABSTRACT***

*Mobile ad hoc networks (MANETs) are relatively vulnerable to malicious network attacks, and therefore, security is a more significant issue than infrastructure-based wire-less networks. In MANETs, it is difficult to identify malicious hosts as the topology of the network dynamically changes. A malicious host can easily interrupt a route for which it is one of the forming nodes in the communication path. Since the topology of a MANET dynamically changes, the mere use of a static baseline profile is not efficient. We proposed a new anomaly-detection scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals. Our dynamic learning process involves calculating the projection distances based on multidimensional statistics using weighted coefficients and a forgetting curve.*

***KEYWORDS***

*Attack, Detection, Learning, MANET, Security, Feature Set, Anomaly, Malicious*

## 1. Introduction

Mobile ad-hoc networks (MANETs) are a collection of mobile nodes without any infrastructure due to this the mobile nodes in the network dynamically establish routing paths between themselves. These nodes act as both node and also router. MANETs may also be composed of different types of devices, which have different transmission ranges, this situation results in various problems. Due to differing transmission ranges of intermediate nodes, a path from the source to the destination might not be valid for the destination to the source since one node might not be able to transmit to its preceding node in the route. The major problem in MANET is its routing.

Despite the problems of MANETs, MANETs have a tremendous potential to be used in various real-world situations such as battle field scenarios, rescue operations and vehicular networks, where setting up a traditional network infrastructure would be implausible. Hence there is a need to develop special routing algorithms to meet these challenges. Swarm intelligence, a bio-inspired technique, has been applied to the MANET routing problem. Path quality is the key factor which affects the performance of the MANET.

DOI : 10.5121/ijasuc.2011.2408 

A MANET routing algorithm should be adaptive, in terms of state of the nodes, load conditions of the network and state of the environment. Since connections are less effective in delivering the QoS that is required in the rapidly changing MANET environment and impose additional overhead on the network. Hence the majority of MANETs are connectionless in nature. In MANETs the packet transmission relies on other nodes as they are multi-hop in nature. Thus MANETs require that traditional algorithms be redefined to accommodate these additional requirements.

Every MANET routing algorithm has three essential mechanisms: A route discovery a route error correction, and a route maintenance. Secure routing protocols in which key-based cryptographic technologies are applied have been suggested to meet the increasing demands for MANET security. However, besides the topology issue, these methods cannot protect the network from attacks by a malicious node that has managed to acquire the network key. Therefore, other security methods that can detect attacks from malicious hosts are required. If a well-known attack in the TCP/IP protocol stack is launched in a MANET, then it is possible to protect the network by using conventional security techniques. The techniques for detecting the malicious attacks are divided into two categories, namely, misuse detection and anomaly detection. In misuse detection, the method of using a signature-based analysis is widely implemented. In this method, the attacks are identified by comparing the input traffic signature with the signatures extracted from the known attacks at the network routers.

An anomaly detection is a technique that quantitatively define the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. It is rather easy to detect an attack, the traffic signature of which is identifiable by using misuse detection. However, for those attacks, the type or traffic signatures of which are hard to identify by misuse detection, the method is rather inadequate. In such cases, those attacks can only be detected by using anomaly detection methods. In anomaly detection, even when the traffic signature is unknown, if the baseline profile of a network is delineated a priori, then the abnormality can be recognized. Since the network conditions are likely to change, the pre-extracted network state may not correctly represent the state of the current network. The problem is indeed the accuracy of anomaly detection method. Due to the fact that the MANET environment dynamically keeps evolving, envisioning a robust anomaly detection method becomes imperative to thwart the malicious attacks against it. In this paper, we propose a new anomaly detection scheme based on a dynamic learning method which is based on a statistical decision theory that calculates the multidimensional projection distance between the current and normal states of the targeted host.

## 2. Related Works

Ruby et al [1] proposed that the embodied Secure AODV that reinforced security mechanism by using two additional control messages (IREQ, IREP). Kamaljit et al [2] proposed mechanism which uses symmetric key cryptography and generates very less overhead of calculations and saves power consumption of nodes significantly which is most important and attractive feature. Lai et all [3] proposed that AODV-BR performs better in light loads and decreases in heavy traffic situation because of the increase in packet collisions when there are more and more traffic. Zeyad et al [4] proposed a three heuristics have been developed to fortify the dominating set process against loss by reintroducing some redundancy using a least-first set cover rather than a greedy set cover.

Huang et al [8] proposed report of our progress in developing Intrusion Detection (ID) capabilities for MANET. Building on the prior work on anomaly detection, they investigated how to improve anomaly detection approach to provide more details on attack types and sources.

Zhang et al [9] proposed a novel anomaly detection scheme, called RADAR, to detect anomalous mesh node in WMNs. The development is based on a cooperative anomaly detection scheme by fully exploring the Spatio-temporal properties of mesh node behavior. The current scheme is specified and implemented with a reactive routing protocol, aiming at detecting malicious mesh nodes which intentionally violate normal routing mechanisms.

Huang at al [10] proposed techniques that deals with automatic construction of anomaly detection models, capable of detecting new (or unknown) attacks and also introduced a new data mining method that uses "Cross – feature analysis" to capture the inter-feature correlation patterns in normal traffic. These patterns can be used as normal profiles to detect deviation (or anomalies) caused by attacks.

Rajaram et al [11] proposed a trust based security protocol based MAC layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, a trust based packet forwarding scheme is used for detecting and isolating the malicious node using the routing layer information. It used trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by increasing or decreasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the second phase of the protocol, the link layer security using the CBC-X mode of authentication and encryption.

Li Zhao and Jose G. Delgado – Frias [12] have proposed a scheme MARS and its enhancements E-MARS to detect misbehavior and mitigate adverse effect in ad hoc networks. Madhavi and Tai Hoon Kim [13] have proposed a MIDS (Mobile Intrusion Detection System) suitable for multi-hop ad hoc wireless networks, which has detected nodes misbehavior, anomalies in packet forwarding, such intermediate nodes dropping or delaying packets.

T.V.P.Sundararajan, and Dr. A. Shanmugam [14] have proposed a behavior based anomaly detection techniques inspired by the biological immune system to enhance the performance of AMNET to operate despite the presence of misbehaving nodes. The system uses intelligent machine learning techniques that learns and detects each node by false alarm and negative selection approach.

The number of received RREP messages includes two types: The current system cannot be detected in early stage and during data transmission. The first type is a packet, both source and destination addresses of which exist in the training data. All of the other packets are classified as the second type (with either one or no matching features). As an example, when a node is under attack by the "Malicious flooding," it receives a tremendous amount of RREQ messages, and therefore, the number of received RREQ messages increases. This indicates the presence of anomaly in the network.

# 3. Present Work

In the proceeding section we illustrate the proposed concept with a complete conceptual representation. In this section we give an overview of the proposed system which revolves around the concept of using four different algorithms and how these algorithms supports AODV to detect dynamically the anomaly node.

## 3.1. Proposed system:

The proposed system is on the analysis of number of nodes involved in the data transmission, route discovery and maintenance in mobile ad hoc network. . In our paper, a dynamic learning

method is implemented in AODV protocol for detecting anomaly node. The proposed system finds the abnormal behaviors in the network path very early stage. The following algorithms are used

- Ant net algorithm
- Destination sequenced distance vector
- Probabilistic routing
- Q-routing

The possible data transmission with shortest path can be identified with help of AODV protocol. The early detection can be done with the help of ant net algorithm with DSDV routing protocol. The q-routing and probabilistic routing are sequence based data transmission strategies in the network path. The performance analysis is done with the comparison of throughput, instantaneous packet delay and average packet delay of all the four algorithms. The path finding features comprises of 1) Number of received RREQ messages 2) Number of forwarded RREQ messages 3) Number of outbound RREQ messages 4) Number of outbound RREP messages 5) Number of received RREP messages. A normal state needs to be defined by using the data reflecting the trend of the current situation, and this leads to the idea of updating the learning process within a time interval. By repeated so, the attack detection can adaptively be conducted even in a changing network scenario. The advantage of proposed system is to find abnormal behaviors in the network path at very early stage

### 3.1.1. Nodes creation in AODV:

The data transmission in which a node can receive packets that are neither broadcasted nor addressed to itself. Source Node determines routes dynamically and only as needed .Source Node that wants to send a packet must check its route cache. . The node sends the packet if there is a possibility of data transmission.

### Route discovery and maintenance:

**Route discovery:** It is the mechanism used only when source node sends a packet to destination and does not already know the route.

**Route maintenance**: It is the mechanism which indicates when a source route is broken, it can attempt to use any other route it happens to know route to destination or can invoke route discovery again to find a new route. Route Maintenance is used only between source and destination.

### 3.1.2. Dynamic anomaly detection:

An anomaly detection mechanism is interrelation between features. Moreover, they constructed an extended finite-state automaton (EFSA) according to the specification of the AODV routing protocol, envisioned nor- mal condition modeling, and detected attacks with both specification-based and anomaly-based detection schemes. In specification-based detection, the attacks were detected as deviant packets from the conditions by EFSA. In addition, in anomaly detection, the normal conditions are defined as the baseline with which the condition of EFSA and also the amounts of transition statistics are compared. The deviations from those conditions are then used to detect the potential attacks. For determining the baseline profiles, in both methods, the training data are extracted beforehand from the same net- work environment where the test data are applied. However, we note that the MANET topology can rather easily be changed, and the differences in network states grow larger with time. Furthermore, these methods

cannot be applied to a network where the learning phase has been conducted in another network. When the nodes in the current MANET differ from those in the training data, the defined baseline profile cannot express the current network state. As a result, these methods are rendered inadequate and considered difficult in a MANET environment. To solve this problem, a normal state needs to be defined by using the data reflecting the trend of the current situation, and this leads to the idea of updating the learning process within a time interval.

### 3.1.3. Ant colony optimization:

A set of computational concurrent and asynchronous agents (a colony of ants) moves through states of the problem corresponding to partial solutions of the problem to solve. They move by applying a stochastic local decision policy based on two parameters, called *trails and attractiveness. By moving, each* ant incrementally constructs a solution to the problem. When an ant completes a solution, or during the construction phase, the ant evaluates the solution and modifies the trail value on the components used in its solution. This information will direct the search of the future ants.

### 3.1.4. Destination-Sequenced Distance-Vector Routing

The main contribution of the algorithm was to solve the Routing Loop problem. Each entry in the routing table contains a Sequence number, the sequence numbers are generally even if a link is present; else, a number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently.

## 4. Implementation:

The AODV routing daemon to function it must determine when to trigger AODV protocol events. Since the IP stack was designed for static networks where link disconnections are infrequent and packet losses are unreported, most of these triggers are not readily available. Therefore, these events must be extrapolated and communicated to the routing daemon via other means. The events that must be determined are:

(i) **When to initiate a route request:**

This is indicated by a locally generated packet that needs to be sent to a destination for which a valid route is not known.

(ii) **When and how to buffer packets during route discovery:**

During route discovery packets destined for the unknown destination should be queued. If a route is found the packets are be sent.

(iii) **When to update the lifetime of an active route:**

This is indicated by a packet being received from, sent to or forwarded to a known destination.

(iv) **When to generate a RERR if a valid route does not exist:**

If a data packet is received from another host and there is no known route to the destination, the node must send a RERR so that the previous hops and the source halts transmitting data packets along this invalid route.

(v) **When to generate a RERR during daemon restart:**

After the AODV routing protocol restarts, it must send a RERR message to other nodes attempting to use it as a router. This behavior is required in order to ensure no routing loops occur.

### 4.1. Determining Local Connectivity:

To avoid wasting bandwidth and energy, it is beneficial for the sender of a data packet to have assurance that the next hop is within transmission range and is likely to receive the packet. In order to verify that the next hop is receiving data packets, local connectivity must be monitored. Notification of the inability to send data packets to a neighbor is needed to promptly notify the source that a path is broken; otherwise, the source continues to send data packets, wasting resources. The AODV routing protocol uses RERR Messages to notify the source and all nodes on the route to the source of the broken link. Because other solutions are not currently available, all current implementations utilize Hello messages.

## 5. Simulation of Attacks:

The malicious nodes can misuse the AODV by forging source IP addresses, destination IP addresses, RREQ IDs, hop counts, Destination Sequence numbers (Dst_Seqs), Source Sequence numbers (Src_Seqs), and also by flooding the network with routing packets. 1) Routing Disruption Attacks: These attacks interrupt the establishment of a route or destroy an existing route. The most common attacks of this type are the modification of RREP and the modification of RREQ. 2) Resource Consumption Attack: This attack wastes resources of a specific node and the network as a whole. The most common attack of this type is malicious flooding.

## 6. Experimentation and Results:

We have used Network Simulator 2 [5] and bounded for 75 nodes. The dimension of the area is fixed as 1200 X 700. Node movement is traced as random way point method.

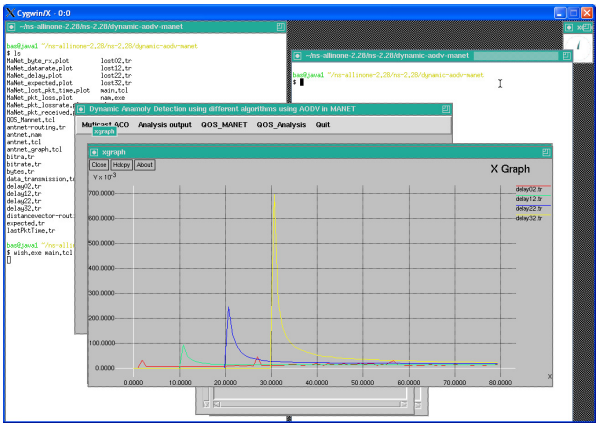


Fig 1. The algorithm performance analysis

Fig 1. Shows the comparison of the performance of antnet, probabilistic routing, and q-routing implemented on AODV protocol and DSDV protocol. From the graph it shows clearly that the antnet algorithm implemented on AODV protocol gives the better performance than the other three. The probabilistic routing gives the performance similar to that of the antnet but the rest gives the poor performance. This performance analysis is based on the throughput.

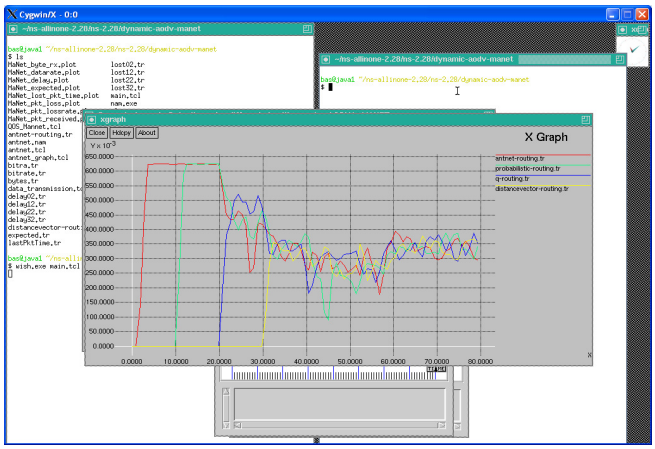


Fig 2. Packet Delay rate

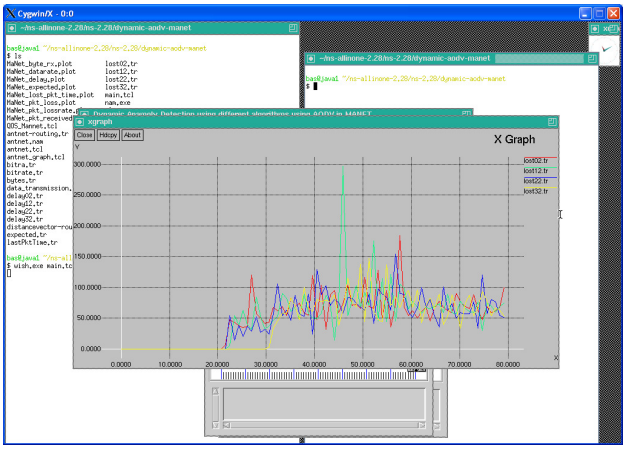


Fig 3. Delay Report

Fig 2 and 3 shows the comparison of the instantaneous delay and the average delay of antnet, probabilistic routing, and q-routing implemented on AODV protocol and DSDV protocol. The delay consumed by the antnet algorithm implemented on the AODV protocol is very less when compared to other three. The probabilistic routing gives somewhat better delay but the rest gives increased delay.

## 7. CONCLUSION

A new dynamic anomaly detection system for MANETs has been proposed. For enhancing the security in MANETs, which are vulnerable to attacks, mathematical based sequence methods

used for early detection in the network path. The ant colony optimization techniques used in the anomaly detection to prevent up normal behavior in between the path during data transmission.

AODV is a major routing protocol in MANETs, new protocols are emerging, e.g., dynamic MANET on-demand protocol (DYMO). It will evaluate these protocols and give an analysis for the additional types of attacks to further improve the accuracy of the overall system. Moreover, *reported* an interesting scheme with the context of studies on the intrusion detection system (IDS). The proposed IDS autonomic event analysis system that is represented by description logics allows inferring the attack scenarios and enabling the attack knowledge semantic queries. To cite a case, first, using proposed system to detect attacks and then rigorously applying these IDS to analyze these attacks may bring about a reliable approach.

## ACKNOWLEDGMENTS

We convey our profound thanks for constant encouragement from Dr. T. Srinivasan, Director, Rajalaskhmi Institute of Technology, Chennai. Also we extend our sincere thanks to Dr. E.N.Ganesh, Principal, Rajalskhmi Institute of Technology, Chennai.

## *REFERENCES*

[1] "A route stability-based optimized AODV protocol" by E.D.Kanmani Ruby, Assistant Professor, S.Rajasurya , K.Swarnam. Conference Proceedings. RTCSP'09.

[2] "Securing AODV for MANETs using Message Digest with Secret Key "by Mr. Kamaljit Lakhtaria, Prof. Bhaskar N. Patel, Mr. Satish G. Prajapati, Dr. N. N. Jani. International Journal of Network Security & Its Applications (IJNSA), Vol.1, No.3, October 2009.

[3] "Adaptive backup routing for ad-hoc networks" by Wei Kuang Lai, Sheng-Yu Hsiao, Yuh-Chung Lin. Computer Communications 30 (2007) 453–464.

[4] "Utilization of AODV in Wireless Ad Hoc Networks" by Zeyad M. Alfawaer, GuiWei Hua, and Nidal Abu Hamdeh. Journal of Computer Science 3 (4): 218-222, 2007.

[5] VINT Group, UCB/LBNL/VINT Network Simulator ns-2. [Online]. Available: http://www.isi.edu/nsnam/

[6] C.E. Perkins and E.M. Royer, "RFC3561: Ad hoc on-demand distance vector (AODV) routing", Internet RFCs, RFCs, Jul. 2003.

[7] IVAN STOJMENOVIC, "Handbook of Wireless Networks and Mobile Computing", wiley Edition, 2008.

[8] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection system for Ad Hoc Network," (SASN'03) Proceedings of the 1st ACM workshop on security of Ad hoc and Sensor Networks.

[9] Zonghuz Zhang, Farid Nait-Abdesselam, Pin-Han Ho, Xiaodong Lin, "RADAR: a ReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks", IEEE Wirless Communications and Networking Conference, 2008. (WCNC 2008).

[10] Yi-an Huang, WeiFan, Wenke Lee, Philip S. Yu, "Cross – Feature Analysis for Detecting Ad-Hoc Rouitng Anomalies," T.J. Watson Research Center, IBM, 2002.

[11] A. Rajaram, Dr.S. Palaniswami, "Malicious Node Detection System for Mobile Ad hoc Networks," International Journal of Computer Science and Information Technologies, Vol .1 (2), 2010.

[12] Li Zhao and Jose G. Delgado – Frias, "MARS: Misbehavior Detection in Ad Hoc Networks, " in proceedings of IEEE conference on Global Telecommunications Conference, Nivember 2007.

[13] S. MAdhavi and Dr. Tai Hoon Kim, " AN INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORKS", International Journal of Security and its applications, Vol. 2, No.3, July 2008.

[14] T.V.P. Sundararajan, Dr. A. Shanmugam, "Behavior based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET," International Journal of Computer Science and Security (IJCSS) Volume (3): Issue (2).

## Authors

He is doing Ph.D in Anna University of Technology, Coimbatore, Tamilnadu, India. He completed his M.E. in Computer Science and Engineering and B.E. in Computer Science Engineering from Anna University and Madurai Kamraj University. He published several papers in National and International Conferences and Journals respectively. He is having 10 years teaching experience. He is currently working as Assistant Professor, Department of Information Technology, Rajalskshmi Institute of Technology, Kuthambakkam, Chennai. His area of interest includes Communications, Mobile Networks, Routing protocols design, Security, and Operating systems.

He received Ph.D in Anna University, Chennai, Tamilnadu, India. He completed M.E. in Power Electronics & Drives from College of Engineering, Guindy, Anna University, Chennai and B.E. in Electrical and Electronics Engineering from Bharathiyar University. He published several papers in National and International Journals and Conferences. He is having 1 5 years of teaching and 5 Years of research experience. Presently he is working as. Professor and Director, Research and Development, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India. His area of interest is Power Electronics, Signal Processing, Advanced Drives and Networks.