International Journal of Computer and Communication Technology

Volume 5 | Issue 3 Article 1

July 2014

# Preemptive Routing & Intrusion Detection for MANETs

N. Sandeep Chaitanya
*JNTU, Hyderabad, India,*, n.sandeepchaitanya@gmail.com

V. Ramesh
*Sathyabama University ,Chennai, India*, v2ramesh634@yahoo.co.in

K. Vijaya Kumar
*Department of CSE, CMRCET*, kvijayakumar@gmail.com

S. Siva Skandha
*Department of CSE, CMRCET.*, ssivaskandha@gmail.com

G. Ravi Kumar
*5Department of CSE, CMRCET*, gravikumar@gmail.com

Follow this and additional works at: https://www.interscience.in/ijcct

## Recommended Citation

Chaitanya, N. Sandeep; Ramesh, V.; Kumar, K. Vijaya; Skandha, S. Siva; and Kumar, G. Ravi (2014) "Preemptive Routing & Intrusion Detection for MANETs," *International Journal of Computer and Communication Technology*: Vol. 5 : Iss. 3 , Article 1.
DOI: 10.47893/IJCCT.2014.1236
Available at: https://www.interscience.in/ijcct/vol5/iss3/1

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Computer and Communication Technology by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

# Preemptive Routing & Intrusion Detection for MANETs

N. Sandeep Chaitanya [1], V.Ramesh[2], K. Vijaya Kumar [3], S.Siva Skandha [4] & G. Ravi Kumar [5]
[1] JNTU, Hyderabad, India, [2]Sathyabama University ,Chennai, India
[3,4&5]Department of CSE, CMRCET.
E-mail : n.sandeepchaitanya@gmail.com[1], v2ramesh634@yahoo.co.in[2]

***Abstract*** **-** An ad-hoc network will often change rapidly in topology, this courses for routes in the network to often disappear and new to arise. The Ad-hoc On-Demand Distance Vector Routing Protocol(AODV), is based on the principle of discover routes as needed. In this paper we will extend the definition of AODV with the ability to discover multiple routes to a host and switch between them, if an active route is becoming weak and there is a risk that it will disappear. We will refer to it as "pre-emptive AOMDV". We will show that the performance of pre-emptive AOMDV do handle changes in topology better than AODV it self. To show the effect of extending AODV, the suggested protocol is implemented in a simulator. Performance enhancements will be presented from different scenarios, to compare pre-emptive AOMDV with the ordinary AODV. In this paper we also focus on intrusion detection based on Finite State Machine and cache memory in ad hoc networks. Security is one of the most important issues in current networks. The most common cases of attacks in mobile Ad hoc networks can be drop of routing packets and changes in the incoming packets which aims at disrupting the network routing and overall network reduce performance. The presented approach based on FSM focuses at recognizing the malicious nodes within the network in a fast and accurate way, then it deals with rapid introduction of the malicious nodes to other nodes in the network to prevent sending multiple packets and drop and packet change. Finally, we will show the significant improvement in comparison with others, we simulated our methods by NS2 software.

***Key words*** **-** *AODV, AOMDV, Preemptive Region, Multi Path Route Discovery Intrusion Detection Technique.*

## I. INTRODUCTION

Currently, great demands for self-organizing, fast deployable wireless Mobile Ad Hoc NETworks (MANETs) come along with the advances in wireless portable technologies. Unlike the conventional cellular wireless mobile networks that rely on extensive infrastructure to support mobility, a MANET does not need expensive base stations or wired infrastructure. This feature is important in battlefields or disaster rescue sites where fixed base stations are undesirable or unavailable. For commercial applications such as convention centers, electronic classrooms, and conferences, a rapid deployment of all-on-air networks provides users with more flexible and cheaper ways to share information.

The absence of a fixed infrastructure, however, requires every mobile user to cooperate together for message transmission. Since radio transmission range is limited for each host, a source host must depend on several intermediate hosts to send its message to a host far away. Finding a path from the source to the destination, or routing, is fundamental for providing other advanced services. Routing, however, is very challenging in MANETs due to frequent network topology changes and power and bandwidth constraints.[1][2]

The Routing Protocols in MANET fall into two categories:

1. Reactive
2. Pro-active

Re-active routing protocol does not take initiative for finding routes. It establishes routes “on demand” by flooding a query.

Some pros and cons of reactive routing protocols are:

- It does not use bandwidth except when needed.
- Much network overhead is present in the flooding process when querying for routes.
- There is initial delay in the traffic.

On the other hand pro-active routing protocols set up routes based on continuous control traffic. All routes are maintained all the time.[1][2]

Some pros and cons of these protocols are:

- Constant overhead is created by control traffic.

- Routes are always available.

The idea of this paper is to demonstrate how pre-emptive routing and multipath routing can be added to the AODV protocol and how it will improve performance in a network with a low overhead.

## II. AODV

The AODV protocol, is designed for mobile nodes in ad-hoc networking, where there often are changes in topology. The AODV protocol is based on on-demand route discovery. Because of that every node have different and limited local knowledge of the network. The fact that a node seeks information about the network, only when needed, is causing low overhead since nodes does not have to maintaining unnecessary route information.

To handle router information AODV uses 3 different kinds of messages Route request (RREQ), Route Reply (RREP) and Route Error RERR. AODV is using ring expansion when discovering new routes to limit flooding of the network and there by reducing overhead. The protocol is ideal for discovering neighbour nodes. If a node needs a route to a node in the other end of the network1 the protocol will course a reasonable flooding of the network. Expansion ring search is a better strategy than doing a full scale search for the node. Likely some other node in the network has a valid route to the destination, and will send a RREP to source, and there by reducing overhead. By every RREQ a node sends, a sequence number is increased, this is used by the protocol to guarantee loop-freedom in paths found.

## III. PREEMPTIVE ROUTING

The idea behind pre-emptive routing is to look for a new route to a host that the node already could have a active route to, before the basic AODV protocol initiates a route discovery. There could be a lot of reasons to do this, we will use it to minimize end-to- end delay in a transfer between two nodes, before the link that they are using disappears. A link can disappear for multiple reasons, but we will look into the case where mobility of nodes is the reason. To be able to see that a node is moving and a route is about to break, we relay on the fact that communication is based on electronic signals. Because of that it is possible to measure the quality of the signal and based on that guess if the link is about to break. Based on this we will discuss how to handle route breaks, with in the AODV routing protocol. Figure 1 is showing how it could look, in a network when a node (X) is moving away from another node and enters its pre-emptive zone.

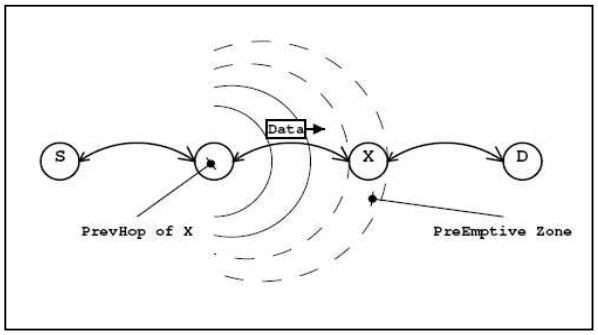



Fig. 1 : Preemptive Zone

## IV. MULTI PATH ROUTE DISCOVERY

The multipath route discovery will not be explained in depth in this rapport, we will just give a overview of the idea and refer to [3] for deeper discussion.

The basic idea behind multipath route discovery is finding multiple node-/link disjoint paths to a destination node. This can be done with a low overhead, because flooding RREQ's through the network is being done already by AODV. Due to AODV already flooding the network, it is easy to see that a change in behaviour when a node receives a RREQ can result in multiple routes to the same destination. The destination node must be allowed to send more RREP's, one for each path.

Figure 2 shows two node disjoint paths from a source to a destination. In article [3] its proved how link-/node disjoint paths are discovered, and how it is implemented. We will in the rest of the rapport assume the availability of multipath routing.

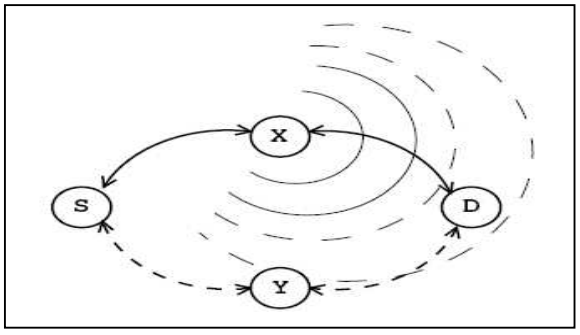



Fig. 2: Two Paths

This section will describe how to extend the AOMDV routing protocol [3], to handle pre-emptive routing as presented and describe how the different approaches can cooperate to create a more efficient algorithm. Using multipath route discovery with pre-emptive routing, will hopefully cause a smaller end-to-end delay and a larger throughput to a host. The RERR message in AODV, needs to be changed to contain

information about the error type. This can be done by altering the definition of the reserved field. Some bits in the reserved field could indicate what kind of error, that the sending node wants to report. We are using the last bit to represent the type of error, table 1 shows how the different errors are represented. To differ between the two RERR messages, it is enough to use 1 bit, since we are only interested in whether the error is send to indicate a dead link or a weakened link.

| | |
|---|---|
| Link broke | 0 |
| Link possibly going to break | 1 |

Table 1: Representation of RERR Messages

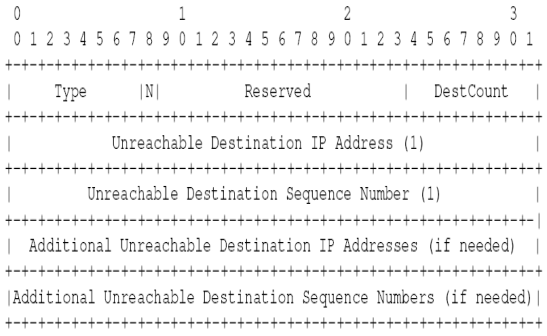



Fig. 3(i): AODV RERR Message Format

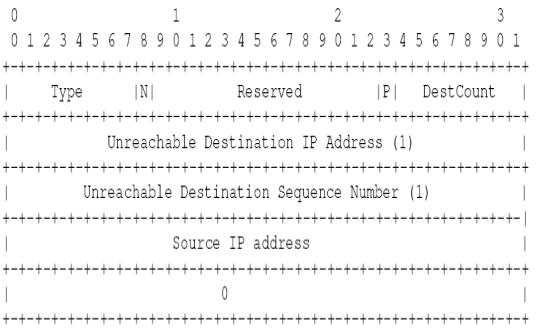



Fig. 3(ii) : AOMDV RERR Message Format

The error messages will be used in the following way:

*Link broke :* When a link is broke the last bit of the reserved is set to 0. This will indicate that the sending node have to find another route to the destination and that the current route does not exist any more.

*Link possibly going to break :* When the routing node, believes that the link will break within a short period of time. This means that the sending node, should find another way to the destination, as soon as possible.

To avoid flooding when sending a RERR we choose to send it to the original source. The "Additional Unreachable Destination IP Addresses" from the AODV RERR message is altered with the source IP address. Each intermediate node will forward the RERR to source.

## V. ALGORITHM FOR AOMDV WITH PREEMPTIVE ROUTING

*Algorithm 1:*

```
Data : IP packet
if ReceivingNode.isInPreemptiveZone then
    send RERR to source of IP packet
end
```

*Algorithm 2 :*

```
if Receive(RERR) then
    if Destination == this.NodeIP then
        if existRouteInMultipath then
            Change default route to destination;
        else
            Initiate a new route discovery to destination, while
            continuing using the weak link.
        end
    else
        send via next_hop to destination
    end
end
```

Algorithm 1 is showing when a node must send a RERR message, to notify a sending node of a route being weak, this is based on the assumption that a lower network layer is able to indicate when a IP packet is received from a node in a pre-emptive zone.

Algorithm 2 shows how a node must behave when it receives a RERR. The first case is handling the RERR if the receiving node is the destination of the RERR. This could course two kinds of actions, either the node could choose another route found using multipath or it could initiate a new route discovery. The second case is if the receiving node is not the destination, then it needs to forward the RERR to the destination using its own default_route, to the destination.

By using the algorithms 1 and 2 we ensure that a RERR message is sent when a active node is entering a pre-emptive zone, as described in the previous sections and if a node receives a RERR, it either initiate a new

route discovery or uses a route found using multipath, in the previous route discovery.

When using the algorithm in a real network, it is the strength of the signal with which a packet is received that indicates the link condition. It is important to notice that the reception of a packet that determines if a node is in pre-emptive zone. This have the consequence that a node entering pre-emptive zone can look in the packet to see where to send the RERR message. This assures that when a source receives a RERR then the default_route to destination is weak.

Pre-emptive AOMDV always find three paths to destination, and only paths with traffic will enter pre-emptive zones and shortly after move out of range. This creates the best results in our protocol.

## VI. INTRUSION DETECTION SYSTEMS

Intrusion detection systems in the Ad Hoc networks are generally divided into several categories from different viewpoints. The most important ones of the mentioned systems are as following: host based intrusion detection and network based intrusion detection. The rest of the paper expresses some of their features and functionality [5, 6].

A. Host based intrusion detection system (HIDS):

In these systems a technique is presented to detect intrusion. Also the intrusion detection technique is saved by each node and runs independently. Each decision about the suspicious network nodes will be made based on data collected only by the corresponding node and no cooperation between network nodes will exist for this matter [7, 8]. So no any kind of control and security information between network nodes will be sent. According to the structure of the intrusion detection systems and the method for identifying them, it'll be much

B. Network based intrusion detection system (NIDS):

In this system, detecting attacks and malicious actions are done by a group of neighboring nodes by their cooperation between each other. Usually clustering techniques are used to implement existing models in this category such that a node will be selected as the inter cluster supervisor. The supervisor monitors the performance of existing nodes in the cluster and detects the malicious nodes of the cluster by using received information from the nodes existing in its area. Thus, suspected nodes within other cluster nodes will be found. In addition, the supervisor node is in charge of sending attack warning message to other clusters by communicating with other supervisor nodes of adjacent clusters [9, 10].a combination of the HIDS and NIDS can be used to discover attacks at the ad hoc network. This combination is a powerful and distributed intrusion detection system. In this system, the exchanged packets in the network and also data collected from the network nodes are considered as a basis for intrusion detection.

Each of intrusion detection systems use the following techniques to detect attacks at Ad hoc network [4, 5]:

Rather than benefits of Ad hoc networks, these networks have some limitations and weaknesses. That are more about security issues these networks. Because of the specific characteristics and nature of network communication media, the variety and number of attacks is very high in such networks. Tiny drop route request packets with the aim of disrupting the routing, Tiny drop data packets to interfere with submitting information to the destination And creating delays in it, Changing the content of routing packages to change the optimized rout. And other types of network attacks that aim to lower the overall performance and network resource consumption. Alongside these wide attacks, the various intrusion detection methods are designed That they have sometimes some bugs. Including the ability of discovering just one or two attacks. Or to detect malicious nodes from control packets and exchange them into large networks. This makes overhead for network. Some other methods require heavy computation with complex algorithms to detect malicious nodes. Due to the limitations of Ad hoc networks in processing, the mentioned methods don't have very high performance will [2, 3, 10]. In this paper a method is discussed to detect three types of attacks at the same time.

In this paper we present a new intrusion detection method based on FSM and cache memory. Eavesdropping the sent data by neighbor nodes is the basic idea of this method. This method which is placed Between Data link layer and physical layer can detect three types of attacks simultaneous: strike drop data packets, routing packets drop and changes in the incoming packet. This method operates as follows. First, the network nodes are clustered by a certain clustering method and a cluster head node is determined for the cluster, periodically and dynamically. The task of cluster head is final diagnosis of malicious nodes within the cluster and informing the adjacent cluster heads. Then each node in the cluster produces a FSM for each neighbor by sending a path request packet to each one of them and also produces a FSM for each output data packet. Then based on the type of packet sent from the node which can be data packet or routing packet, one of the following two scenarios will be estimated: Scenario 1:

Evaluating the neighbor nodes during the route request packet receiving: A node when receives a route request packet will have two different modes (whether the node is destination or not), that show in Figure 4:

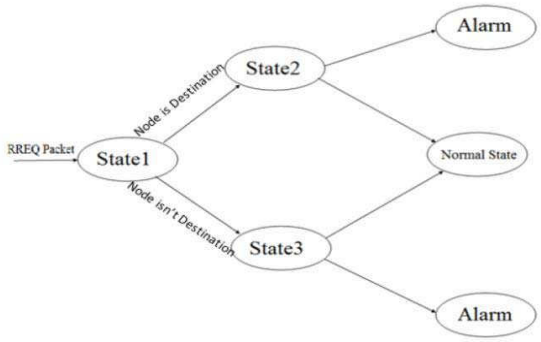



Fig. 4 : FSM to route request packet

State 2 : Receiving node is the destination node, In this case, if the node sends a Reply then the FSM of the node switches to normal mode, otherwise it switches to the Alarm mode.

State3 : Receiving node isn't the destination node, In this case, if the node sends Reply (there is a route to destination) or a Broadcast (there isn't any route to destination) then the FSM of the node switches to normal mode, otherwise it switches to the Alarm mode.

Scenario 2: Evaluating the neighboring nodes performance during receiving data package: When a node receives a data packet it'll have two different modes (whether the node is destination or not), that show in Figure 5:

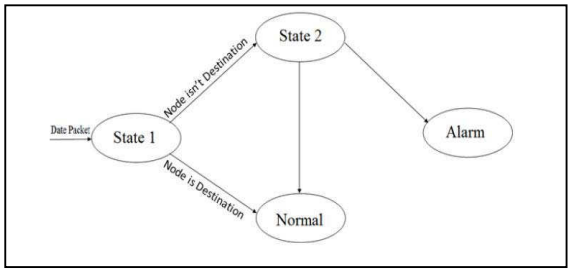



Fig. 5 : FSM to data packet

Normal State : in this case the node who receives data packet also is the destination node. In this situation the FSM of the node will go to normal mode.

State2 : when the node which receives data packet isn't the destination node. In this case if the node sends the data package to the next node then the FSM of the node switches to normal mode, otherwise it will go to Alarm mode. In addition, to detect changes in the incoming packets, the source node stores the packet1 with a FSM in its memory and sends the packet to the intermediate node then it compares the packet outputting from the intermediate node with the sent packet (Packet1 and Packet2) and based on the responses of this comparison, the necessary changes to the FSM will be satisfied. The Figure 6 shows detecting the changes of incoming packet.

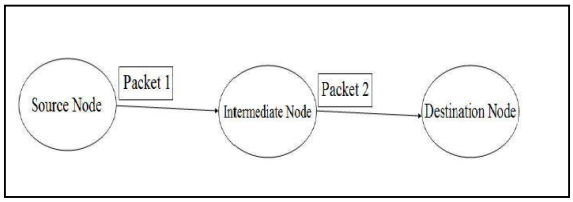



Fig. 6 : Detecting the changes of incoming packet

## VI. RESULTS

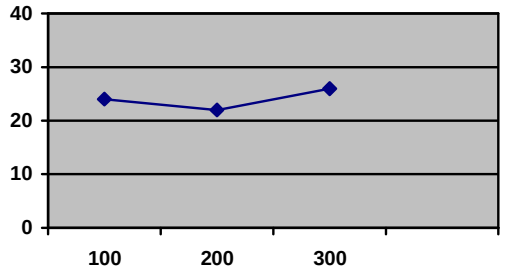
We simulated our method by NS2 software. Our simulation conditions are as follows: In our simulation, ad hoc routing protocol is PAOMDV. In these simulations of 32 hosts used randomly within an 1000 × 1000 m2 area. Each node has a radio propagation range of 100 m and the channel capacity was 1 Mbps. The minimum and maximum speed is set to 1 and 10 m/s, respectively. Intrusion detection engine for 10 malicious nodes. The malicious behavior is carried between 100 and 300 sec. malicious nodes drop all data packet they receives. 10 traffic generators were developed to send constant bit rate datagram to 10 destination nodes. The mean size of the data payload was 256 bytes. Figure 4 shows packet delivery rate relative to Time when there are 10 selfish nodes in the network. As it has been shown, packet delivery ratio Passing the time and starting destructive function selfish nodes, it was almost constant and don't decrease

The results shows that using pre-emptive AOMDV instead of AODV in our limited scenarios is an improvement.

| | AODV | | Pre-emptive AOMDV | |
|---|---|---|---|---|
| | AODV messages | packets received | AODV messages | packets received |
| 10 Packets/sec,512bytes | 153 | 75 | 81 | 79 |
| 4 Packets/sec, 512bytes | 152 | 30 | 79 | 32 |

Table 2 : The table show that traffic is increased by approximately % and AODV-messages are reduced by around 47%.

Delivery(%) Y axis




Time(s) X axis

Figure 4 Packet delivery ratio changing with regard to Time for a 10-selfish nodes network

Figure 5 shows True and False Positives in term of selfish nodes inside the network. As can be seen, increasing time inside the network, increases True Positive. Also, it is clear that many times, amount of False Positive is zero or it's very little.

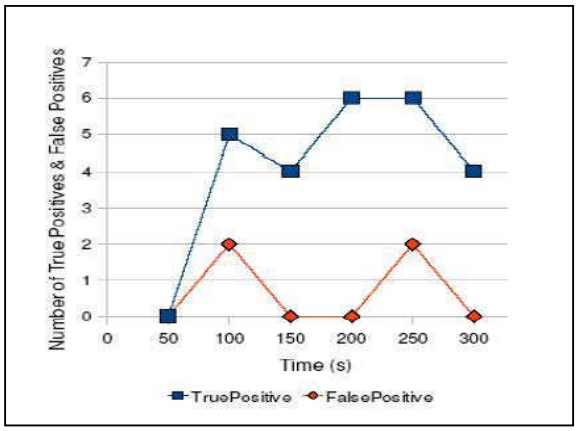



Fig. 5 : True and false positives changes regarding to Time

## VII. CONCLUSION

By reducing the number of AODV-messages, the overhead on the network is also reduced, which gives more network bandwidth to ordinary traffic. Since we are getting 6% more traffic through from source to destination, we conclude that nodes spend less time to find alternative routes to destination. This means that the end-to-end delay also is reduced. on FSM focuses at recognizing the malicious nodes within the network in a fast and accurate way, then it deals with rapid introduction of the malicious nodes to other nodes in the network to prevent sending multiple packets, that Our method is able to identify three type of the attacks (Data packet Drop, Drop of route request packets and changes in the incoming packet) at the same time in the network. Our method doesn't need heavy computation and also its speed and accuracy in detecting suspicious nodes are great

## REFERENCES

[1] YUAN Peiyan, LI Layuan, "Performance Evaluation and Simulations of Routing Protocols in Ad Hoc Networks", ACM 2006.

[2] C. Siva Ram Murthy, B.S, Manoj, "Routing Protocols for Ad Hoc wireless Networks," in Ad Hoc wireless networks: Architectures and Protocols, Chapter 7. Pearson Publication.

[3] Mahesh K. Marina & Samir R. Das, On-demand Multipath Distance Vector Routing in Ad Hoc Networks, http://www.nmsl.cs.ucsb.edu/ksarac/icnp/2001/papers/2001-2.pdf.

[4] Muhammad Sulleman Memon, Manzoor Hashmani and Niaz A. Memon, 2008, A review for uniqueness and variations in throughput due to performance parameters of simulators on MANETs routing protocols, presented in 7th International Conference on EHAC'08, University of Cambridge, UK Cambridge, 20-22 Feb, 2008, PP: 202-208.

[5] Dhanant Subhadrabandhu and Saswati Sarkar Farooq Anjum, " Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols," IEEE VTC, 2004

◈◈◈